FOR509 | ENTERPRISE CLOUD FORENSICS AND INCIDENT RESPONSE

Workbook



https://t.me/learningnets

Copyright © 2021 Pierre Lidome, David Cowen, and Josh Lemon. All rights reserved to Pierre Lidome, David Cowen, and Josh Lemon and/or SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

https://t.me/learningnets

Welcome to the FOR509 Electronic Workbook

E-Workbook Overview

This electronic workbook contains all lab materials for SANS FOR509, Enterprise Cloud Forensics and Incident Response. Each lab is designed to address a hands-on application of concepts covered in the corresponding courseware and help students achieve the learning objectives the course and lab authors have established.

Some of the key features of this electronic workbook include the following:

- Convenient copy-to-clipboard buttons at the right side of code blocks
- Inline drop-down solutions, command lines, and results for easy validation and reference
- Integrated keyword searching across the entire site at the top of each page
- Full-workbook navigation is displayed on the left and per-page navigation is on the right of each page
- Many images can be clicked to enlarge when necessary

Enjoy!

Authors:

- David Cowen | dlcowen@gmail.com | @hecfblog
- Pierre Lidome | plidome@sans.org | @Texaquila
- Josh Lemon | josh@joshlemon.com.au | @joshlemon

Using the E-Workbook

You can access the SANS FOR509 workbook from your host system by connecting to the IP address of your VM. Run `ip a` in the SOF-ELK console to get the IP address of your VM (also shown on the console screen). Next, in a browser on your host machine, connect to the URL using that IP address (i.e. `http://<%VM-IP-ADDRESS%>`).

We hope you enjoy the SANS FOR509 class and workbook! To get the most out of your lab time in class, we recommend following the guidance in How to Approach the Labs.

Trademarks

- The content of this workbook is bound by the SANS Courseware Licensing Agreement (CLA), available in its entirety here.
- ©2021 David Cowen, Pierre Lidome and Josh Lemon. All rights reserved.
- SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. All rights reserved.

https://t.me/learningnets

Syntax Used in This Course

The FOR509 course documentation uses consistent syntax styles with which you should become familiar. This section helps you to make sense of what the material conveys, so you can focus more on course material than styling.

Syntax Descriptions and Examples

> **Note**
>
> The commands listed in this section of the lab are just for reference, so you can become familiar with text styles used in the course materials. *No need to actually run them in your SIFT Workstation VMware Image*!

1. Text blocks that appear in the format shown below contain commands that you would run in the SOF-ELK VM. These code blocks include an icon to the far right that allows you to copy the contents of the block, suitable for pasting into the shell in your class VMs.

   List the contents of the `/tmp/` directory

   ```
   cd /tmp/
   ls -l
   ```

   The results are shown in the box below.

   Results

   ```
   total 2836
   -rw------- 1 sansforensics sansforensics       0 Apr  3 17:39 config-err-S09tBf
   -rw------- 1 sansforensics sansforensics       0 Jul 21 18:39 config-err-zVMGjJ
   -rw-r--r-- 1 root          root                0 May 10 07:45 fileK8YYJh
   -rw-r--r-- 1 root          root                0 Jun 11 07:45 fileVAP3BY
   -rw-r--r-- 1 root          root                0 Jul 11 07:45 fileVeFMlj
   drwxrwxr-x 3 sansforensics sansforensics    4096 Jul  6 18:03 npm-57783-5d61223f
   drwxrwxr-x 3 sansforensics sansforensics    4096 Jul  6 18:04 npm-57819-3bc1b3dc
   ...
   ```

2. Direct questions are reflected in the material as shown below.

   Who does the `admin@pymtechlabs.com` UPN belong to?

   Hank Pym

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Select a field to add to your existing table

The field is `user_name.keyword`

Expected results

Top values of user_principal_name.keyword	Top values of user_name.keyword	Count of records
admin@pymtechlabs.com	Hank Pym	1,036
jvandyne@pymtechlabs.com	Janet Van Dyne	627
slang@pymtechlabs.com	Scott Lang	279
luis@pymtechlabs.com	Luis	82
675be0f4-2486-4443-bef6-d37d9043ae99	675be0f4-2486-4443-bef6-d37d9043ae99	21
dcross@pymtechlabs.com	Darren Cross	12
f2830485-572c-4311-8ae1-08d355887e97	f2830485-572c-4311-8ae1-08d355887e97	1

3. When referring to literal strings inline with narrative text, the strings will be in depicted in Courier New font. For example, a search string of `not result_type: (0 OR 50074 OR 50140)` might be noted in the material inline, or via a call-out box as shown below:

```
not result_type: (0 OR 50074 OR 50140)
```

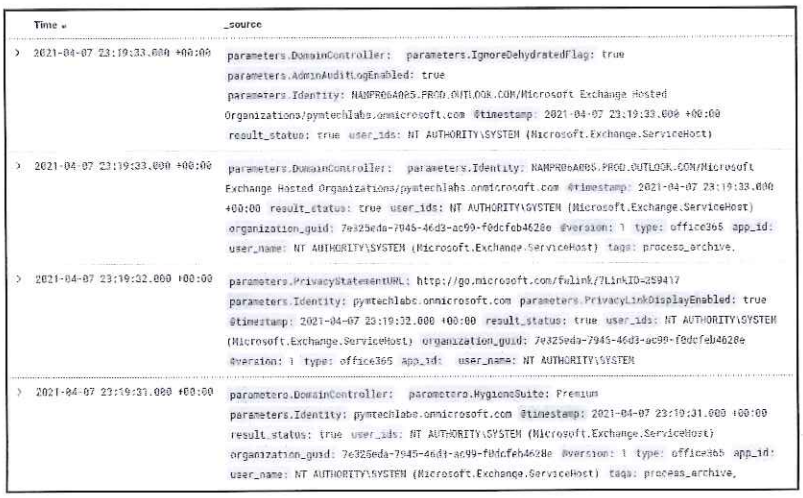
4. Some commands follow a "template" format, in which you will replace a part of the template with relevant information. These template command lines will include placeholders surrounded by the `<%` and `%>` enclosures with uppercase letters between them. This is an indication that you must alter the template command accordingly. For example, in the following command, you'd replace the `<%IP_ADDRESS%>` with the IP address of your SOF-ELK VM as an example.

```
ssh <%IP_ADDRESS%>
```

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

5. It is generally unadvisable to use the `root` administrative account for normal activities. We will follow best practices and use the `sudo` utility to perform administrative actions within the SOF-ELK VM environment wherever needed. The `elk_user` user has full `sudo` access to provide a reasonable balance between best practices and a practical classroom-based lab environment.

6. In the electronic workbook, some images are clickable, resulting in an enlarged version. This can be helpful when examining a detailed diagram or screenshot. An example of this is below.



Time ▾	_source
2021-04-07 23:19:33.000 +00:00	parameters.DomainController: parameters.IgnoreDehydratedFlag: true parameters.AdminAuditLogEnabled: true parameters.Identity: NAMPR06A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/pymtechlabs.onmicrosoft.com @timestamp: 2021-04-07 23:19:33.000 +00:00 result_status: true user_ids: NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost)
2021-04-07 23:19:33.000 +00:00	parameters.DomainController: parameters.Identity: NAMPR06A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/pymtechlabs.onmicrosoft.com @timestamp: 2021-04-07 23:19:33.000 +00:00 result_status: true user_ids: NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost) organization_guid: 7e325eda-7945-46d3-ac99-f0dcfeb4628e @version: 1 type: office365 app_id: user_name: NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost) tags: process_archive,
2021-04-07 23:19:32.000 +00:00	parameters.PrivacyStatementURL: http://go.microsoft.com/fwlink/?LinkID=259417 parameters.Identity: pymtechlabs.onmicrosoft.com parameters.PrivacyLinkDisplayEnabled: true @timestamp: 2021-04-07 23:19:32.000 +00:00 result_status: true user_ids: NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost) organization_guid: 7e325eda-7945-46d3-ac99-f0dcfeb4628e @version: 1 type: office365 app_id: user_name: NT AUTHORITY\SYSTEM
2021-04-07 23:19:31.000 +00:00	parameters.DomainController: parameters.HygieneSuite: Premium parameters.Identity: pymtechlabs.onmicrosoft.com @timestamp: 2021-04-07 23:19:31.000 +00:00 result_status: true user_ids: NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost) organization_guid: 7e325eda-7945-46d3-ac99-f0dcfeb4628e @version: 1 type: office365 app_id: user_name: NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost) tags: process_archive,

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Helpful Hints for Labs

To get the most out of each lab, we will step you through the different portions of the workbook. The workbook is specifically designed to enable students from a variety of backgrounds and with different skill levels to get the most out of each lab.

Important Note

The labs in this workbook require the specific version of the SOF-ELK VM made for FOR509. The public SOF-ELK distributions will not work for these labs!

Warning

- SOF-ELK is pre-configured to use the UTC time zone. *Do NOT change this setting*. In general, UTC is strongly preferred for forensic analysis. Using this single time zone ensures a consistent point of reference for evidence that may have originated in many different physical locales. All labs in this class have been engineered with UTC as a point of reference.
- Feel free to *increase* the CPUs and/or memory allocated to SOF-ELK. Do NOT decrease the allocated resources, or the labs may be extremley slow.
- *Do NOT upgrade packages in the image*
- *Do NOT upgrade VMware Tools*. This is known to cause problems, notably a complete lack of VMware's "Shared Folders" functionality.

Live Lab Updates

This electronic workbook can be refreshed with updates when available. To do so, simply run the following command from a shell prompt:

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Command lines

```
workbook-update
```

Expected results (when updates are available)

```
Updating workbook files
```

Expected results (when no updates are available)

```
No workbook updates available
```

When updates are available, they will be available in the browser on your local system. Note that a page refresh may be required if the updates are to content that is currently displayed.

Exercise Objectives

This section is designed to help students understand the larger picture of what the objectives of the lab are meant to show or teach. In some cases, we might be demonstrating an analytical technique or where to find specific information in a log. We strongly recommend that students quickly look over these objectives when beginning the lab.

Exercise Preparation

This section outlines the specific system, the condition of that system, or the capabilities that must be enabled before moving into the actual lab. Skipping over this step could mean that your system might not be ready for analysis. As many of our labs require the use of Kibana, make sure that you have the correct timeframe and index selected.

Questions without Explanations and Questions with Step-by-Step Instructions

For most labs, we try to get you to focus on the core concepts and analytical techniques instead of just blindly duplicating our steps. The most important part of this course, especially if you are new, is to focus on the analytic techniques.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

> **Note**
>
> In the printed workbook, the step-by-step instructions and explanations are provided right after the questions. In the electronic workbook, the step-by-step instructions and explanations are provided immediately following each question using a drop-down box such as this (click the box to see the solution):
>
> > **Solution**
> >
> > Here's where an answer would go. There will be a drop-down box such as this following each individual question.

Takeaways

For every lab, the takeaway section highlights important information we found in the logs.

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

SANS Courseware Licensing Agreement

Copyright ©2021, David Cowen, Pierre Lidome and Josh Lemon. All rights reserved to David Cowen, Pierre Lidome, Josh Lemon, and/or SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND THE SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, the SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by the SANS Institute to the User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO THE SANS INSTITUTE, AND THAT THE SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND), SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to the SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of the SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of the SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

https://t.me/learningnets

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Lab 0: Install SOF-ELK® VM

Objectives

- Install the SOF-ELK® virtual machine (VM) on your Windows workstation
- Configure and start the SOF-ELK® VM
- Load MaxMind's GeoIP database
- ***Update the SOF-ELK VM & Workbook***
- Access Kibana via your host's web browser

Background

Logs can be viewed within each cloud's console. However, most companies prefer the "single pane of glass" approach and combine all logs in a Security Information and Event Management (SIEM) system. For the our class, we chose ELK as our SIEM. We specifically selected the SOF-ELK distribution as it's maintained by SANS instructor Phil Hagen and includes numerous parsers that we need to ingest cloud logs.

Preparation

To prepare:

1. Install VMware Workstation or VMware Player from vmware.com
   - https://www.vmware.com/products/workstation
   - https://www.vmware.com/prodcuts/player
2. ***Be sure to install version 15.x or later. Earlier versions will not work correctly on Windows 10***
3. Make sure you have at least 40GB of available disk space
4. SOF-ELK is based on CentOS:
   - ***Do not change your regional or time settings inside the VM***
     The VM is preconfigured for the UTC time zone which is best practice for forensic investigations.
   - ***Do not update the operating system***
     The labs have been tested based on the exact version of SOF-ELK provided to you. Any changes may alter the results and impact your educational experience.
   - Feel free to give your VM additional CPU and/or RAM
5. SSD storage is highly preferable if available on your laptop.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Install Steps

1. Install 7-Zip on your workstation

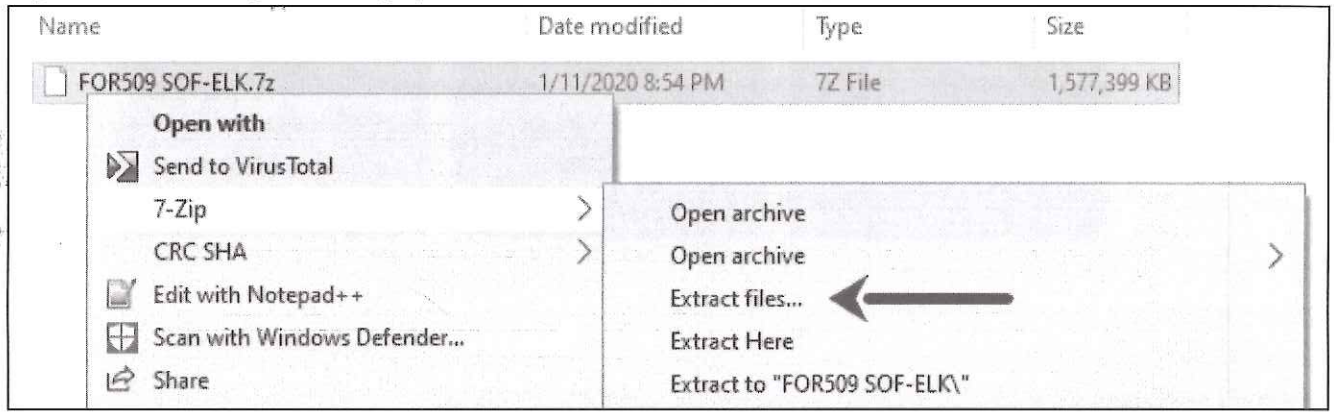
   The SOF-ELK VM will be provided to you in a compressed format and require the 7-Zip utility to decompress.

   - https://www.7-zip.org/

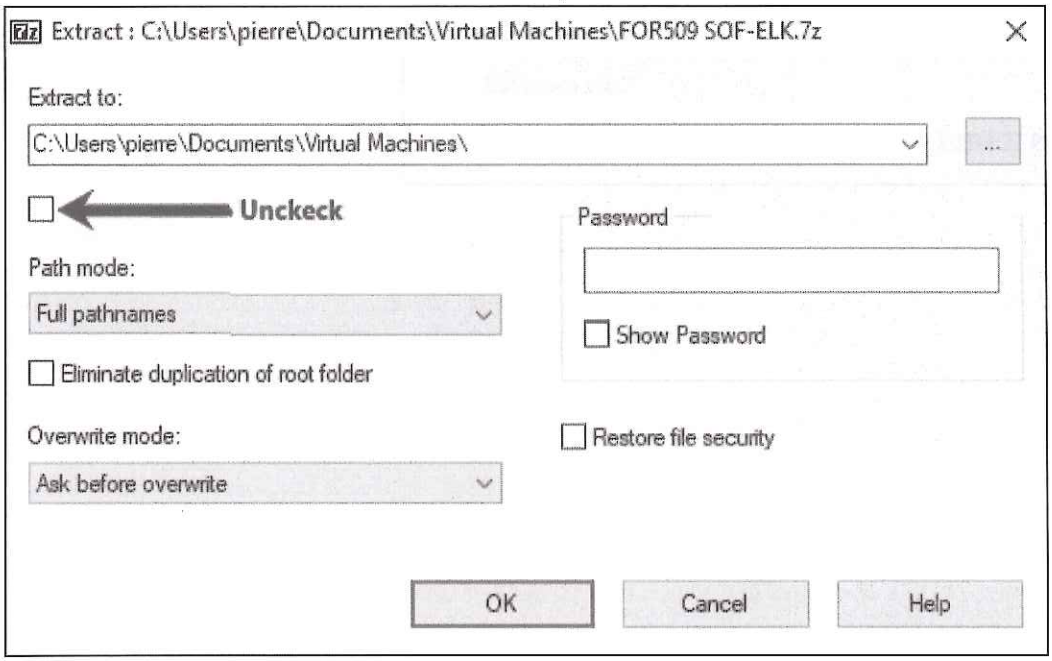
2. Unzip the SOF-ELK VM

   The VM may be provided to you either on a USB drive or as a download link in your SANS portal depending on your class modality. You will need to unzip the `FOR509 SOF-ELK.7z` file to your `Virtual Machines` folder on your host:

   - Right-click the file to get the 7-Zip options and select `Extract Files...`



   - Select a folder on your system to extract the files to
     - Recommend `c:\Users\<Username>\Documents\Virtual Machines`
   - Uncheck the checkbox below the `Extract to:` path

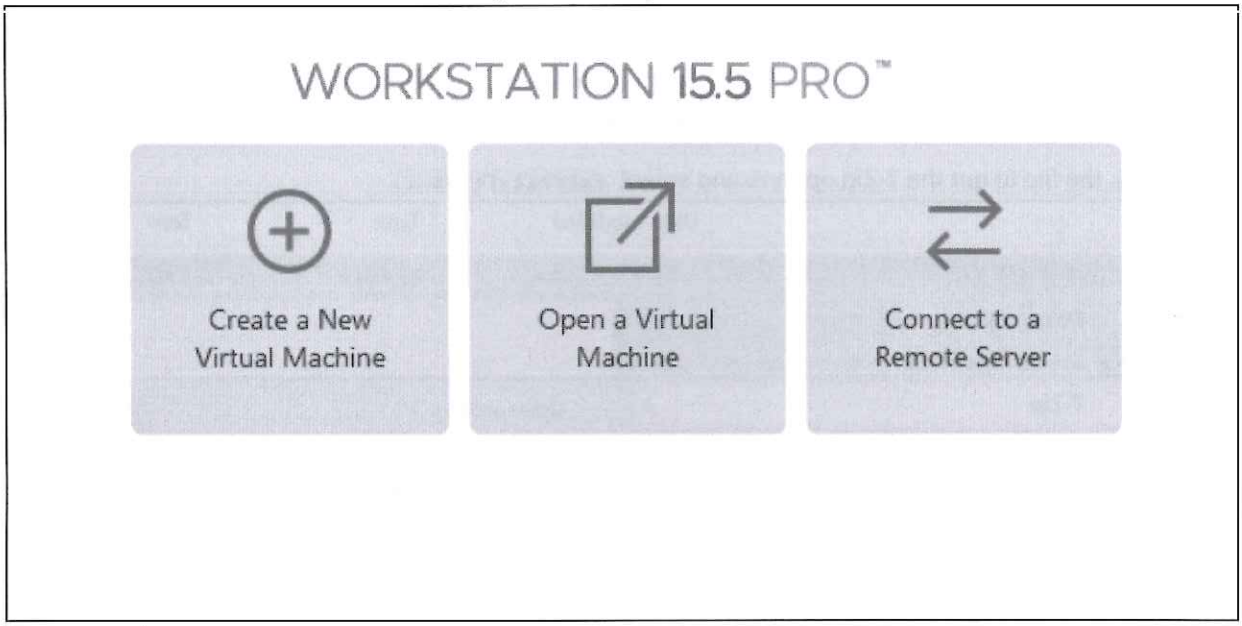


© 2021 Pierre Lidome, David Cowen, and Josh Lemon

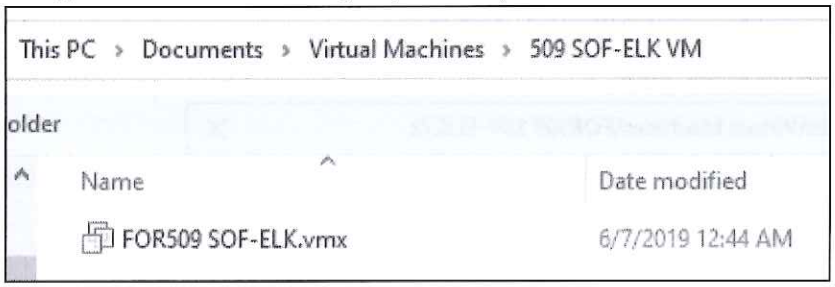
- Depending on whever you have an SSD drive or not, the extraction process can take between 5 and 20 minutes. Once completed, you will have a folder called `c:\Users\<Username>\Documents\Virtual Machines\509 SOF-ELK VM`

3. Configure VM Hardware Settings

- Start VMWare Workstation or VMWare Player. Select `Open a Virtual Machine`

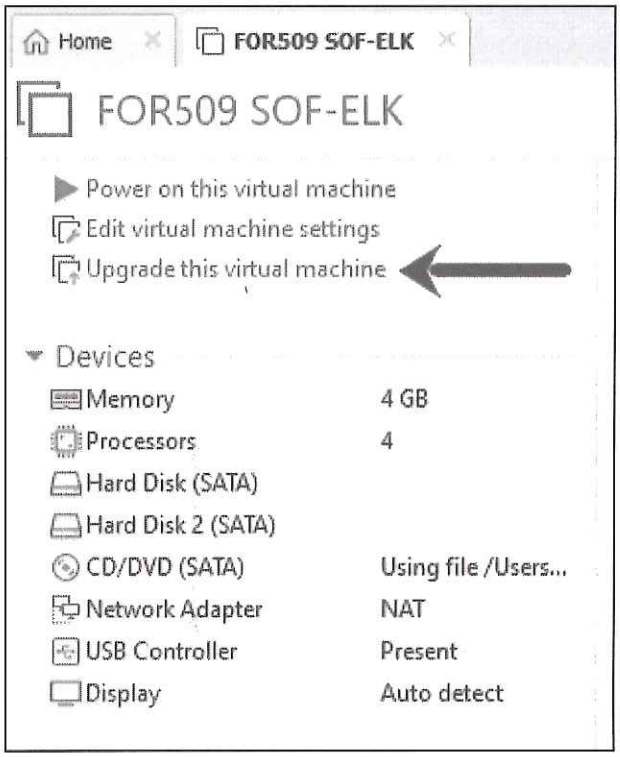


- Navigate to the folder where you previously extracted the files and select `FOR509 SOF-ELK.vmx`

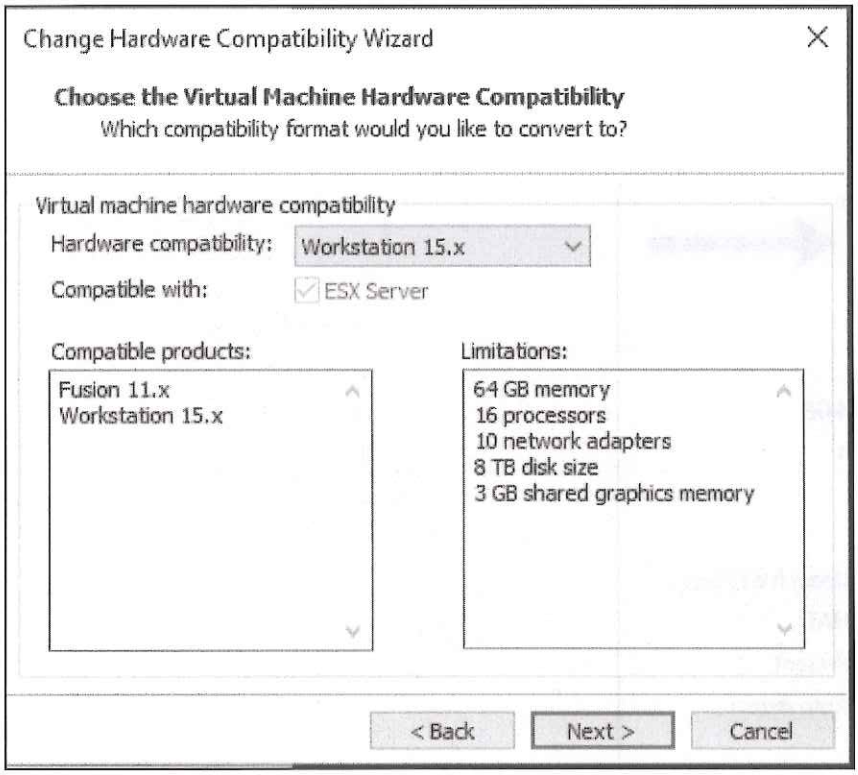


© 2021 Pierre Lidome, David Cowen, and Josh Lemon

- The FOR509 SOF-ELK virtual machine will open up and you should select `Upgrade this virtual machine`

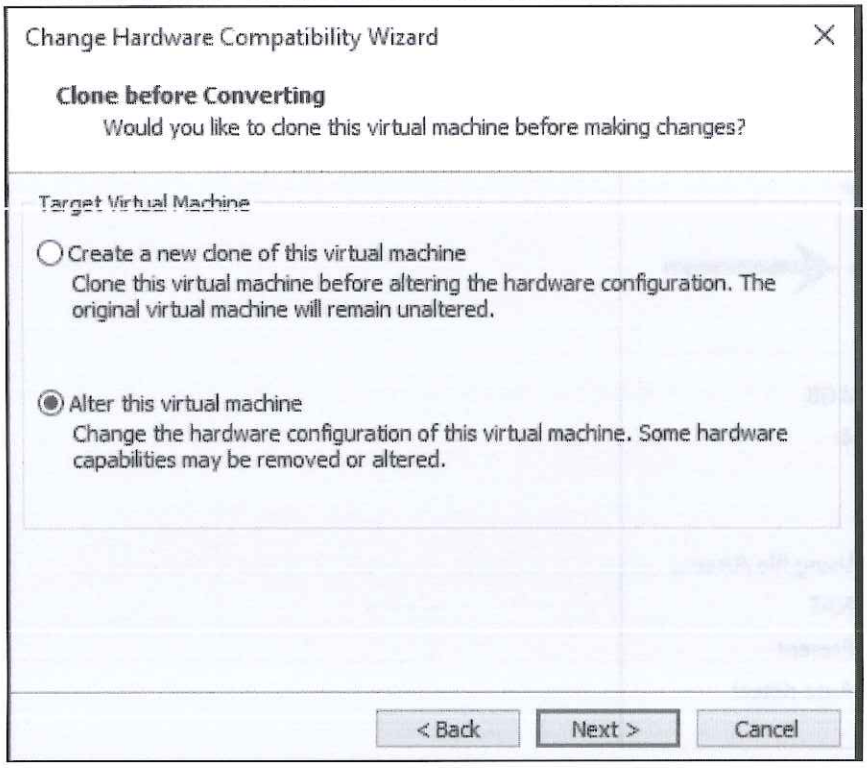


- Select the highest version available under "Hardware compatibility" and click Next

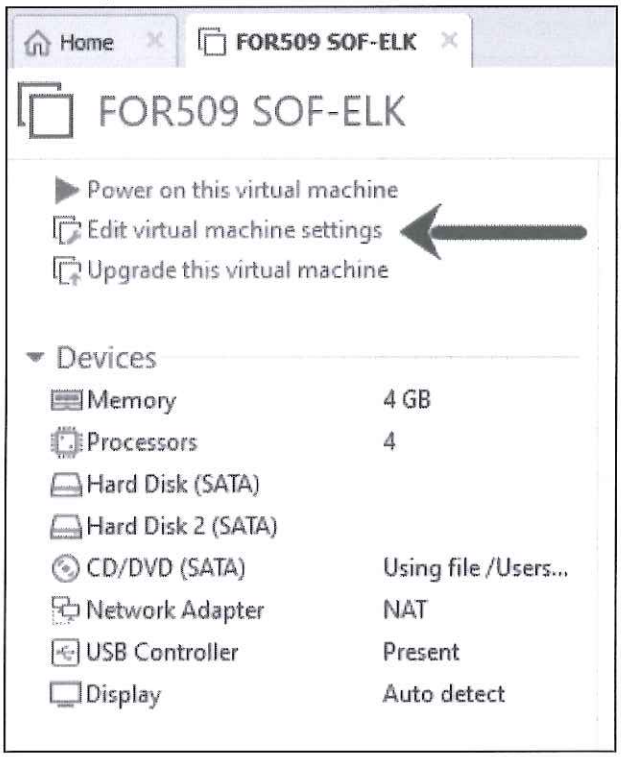


 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

- Select `Alter this virtual machine` and click Next. Click Finish on the next screen

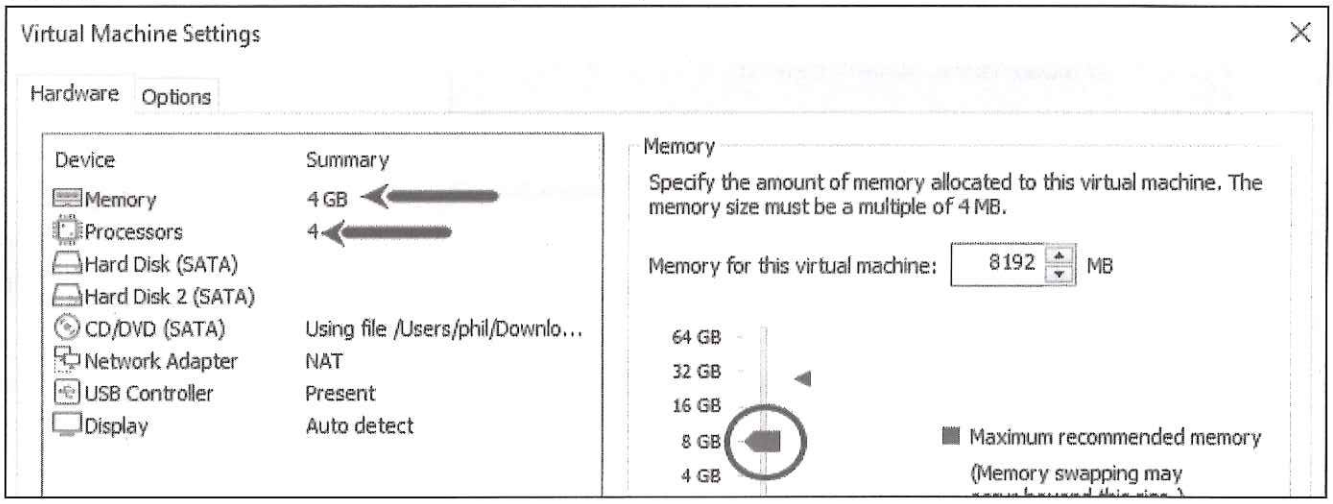


- Next step is to edit the settings

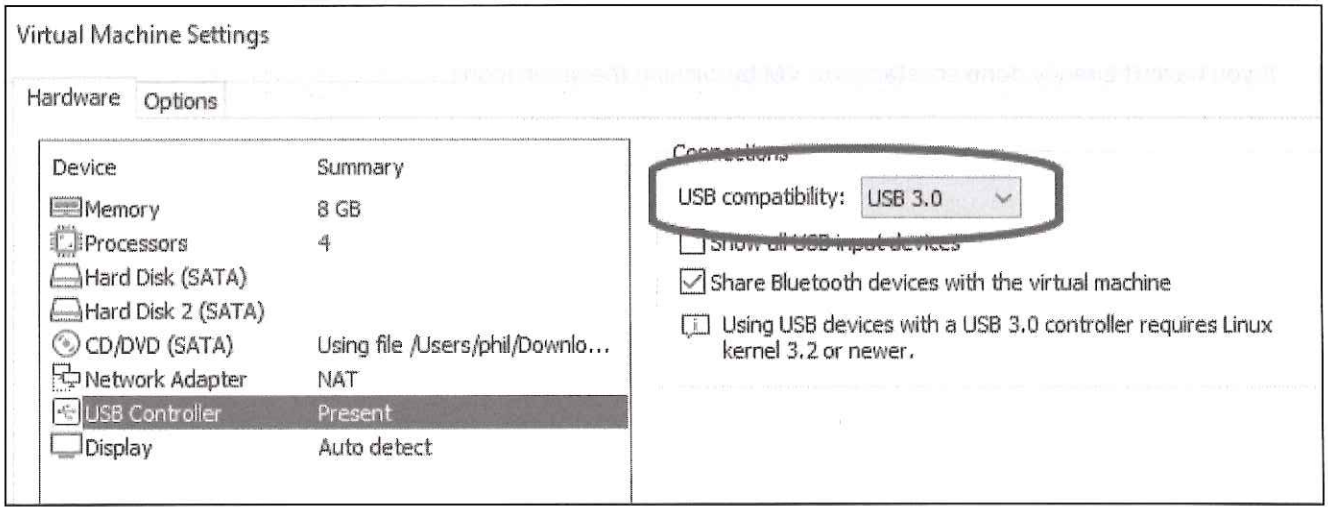


https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

- The ***509 SOF-ELK VM*** requires at least 4GB of RAM. If your host system has more than 8GB of RAM, you can increase the amount of RAM assigned to the virtual machine. The ***509 SOF-ELK VM*** will perform better by giving it more RAM.
- You can also increase the number of processor cores available to the VM. You should assign no more than half the total number of CPU cores available on your host system.



One last thing to check before we start the VM. Make sure the USB settings are set for USB 3.0. Select `USB Controller` and make sure `USB compatibility` is set for `USB 3.0` (select this even if you don't have USB 3.0 on your system as VMWare will still attempt to copy files at a greater speed).

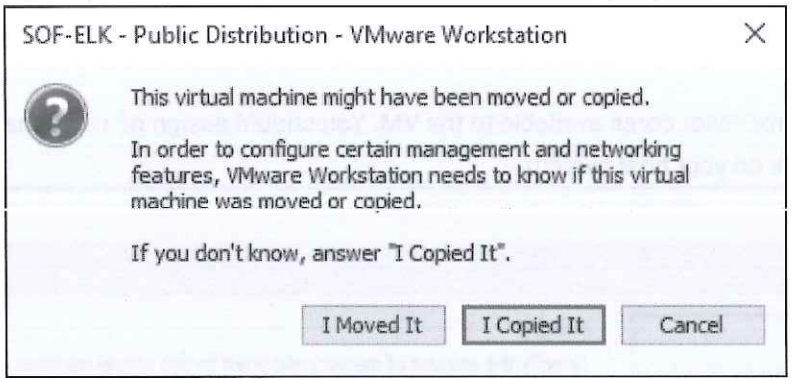


- Select `OK` at the bottom of the settings window. We are ready to start the VM by clicking the green arrow.



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

- If prompted whether this machine was moved or copied, choose `I Copied It`



- If you see any errors regarding `Device or Credential Guard`, you will need to disable Credential Guard or Device Guard. You cannot have two hypervisors running at the same time. See the document: ***Credential Guard / VMWare Workstation Incompatibility Fix***
- Another error you may encounter is `This host is VT-capable, but VT is disabled`. Most likely VT is disabled in your BIOS and will need to be enbabled.

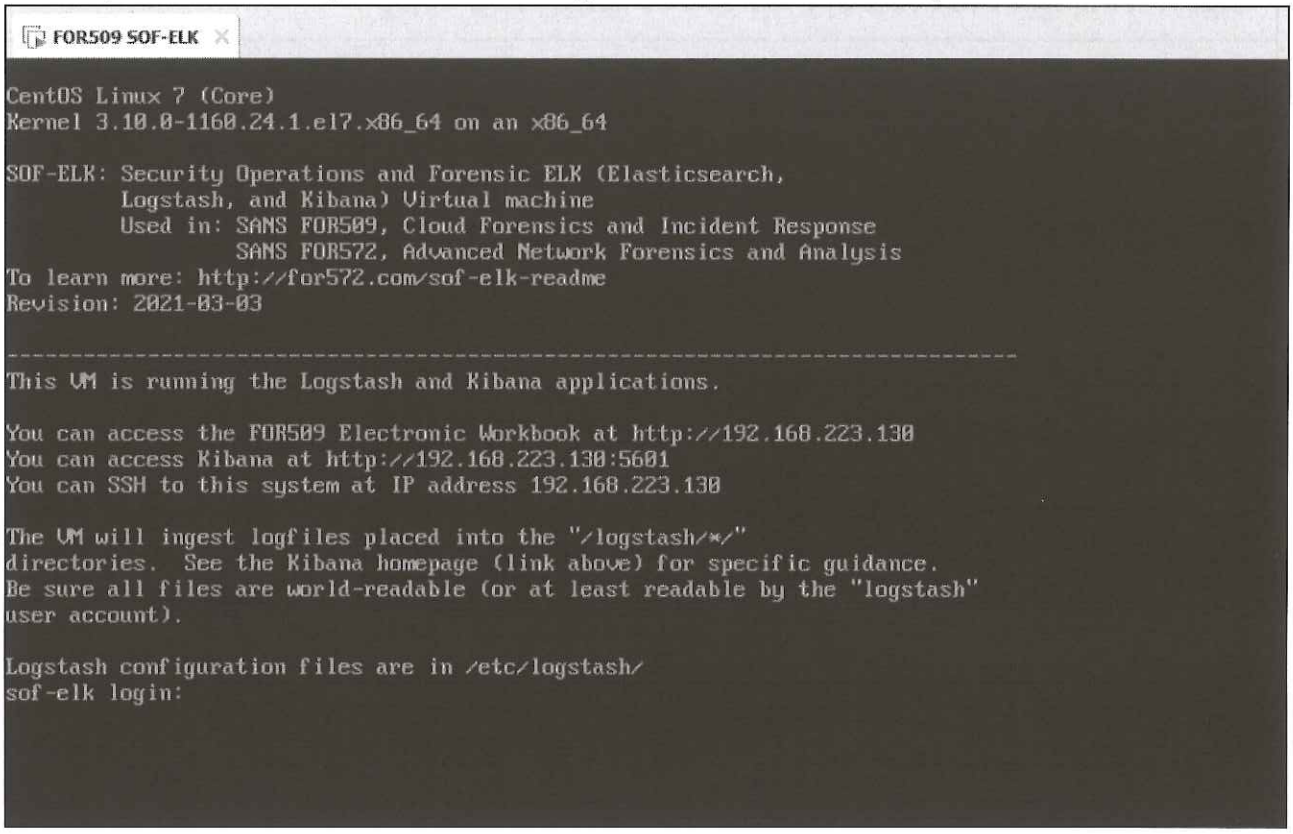
4. Running the 509 SOF-ELK VM

If you haven't already done so, start your VM by clicking the green icon



https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

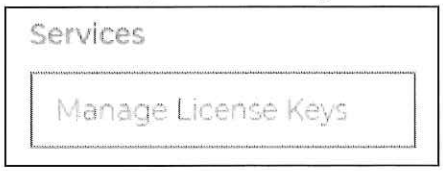
- Once started, you will see a message showing the IP address of your Kibana instance. While you can login to the machine, this is not necesary. *We will be accessing Kibana via a web browser on your host machine.*



Load MaxMind's GeoIP database

There is great value in being able to geolocate an IP address. Some key information that can be obtained include the country, city, ISP name, and ASN number. Due to licensing restriction we can't pre-load the GeoIP database for you and you will need to complete the following procedure.

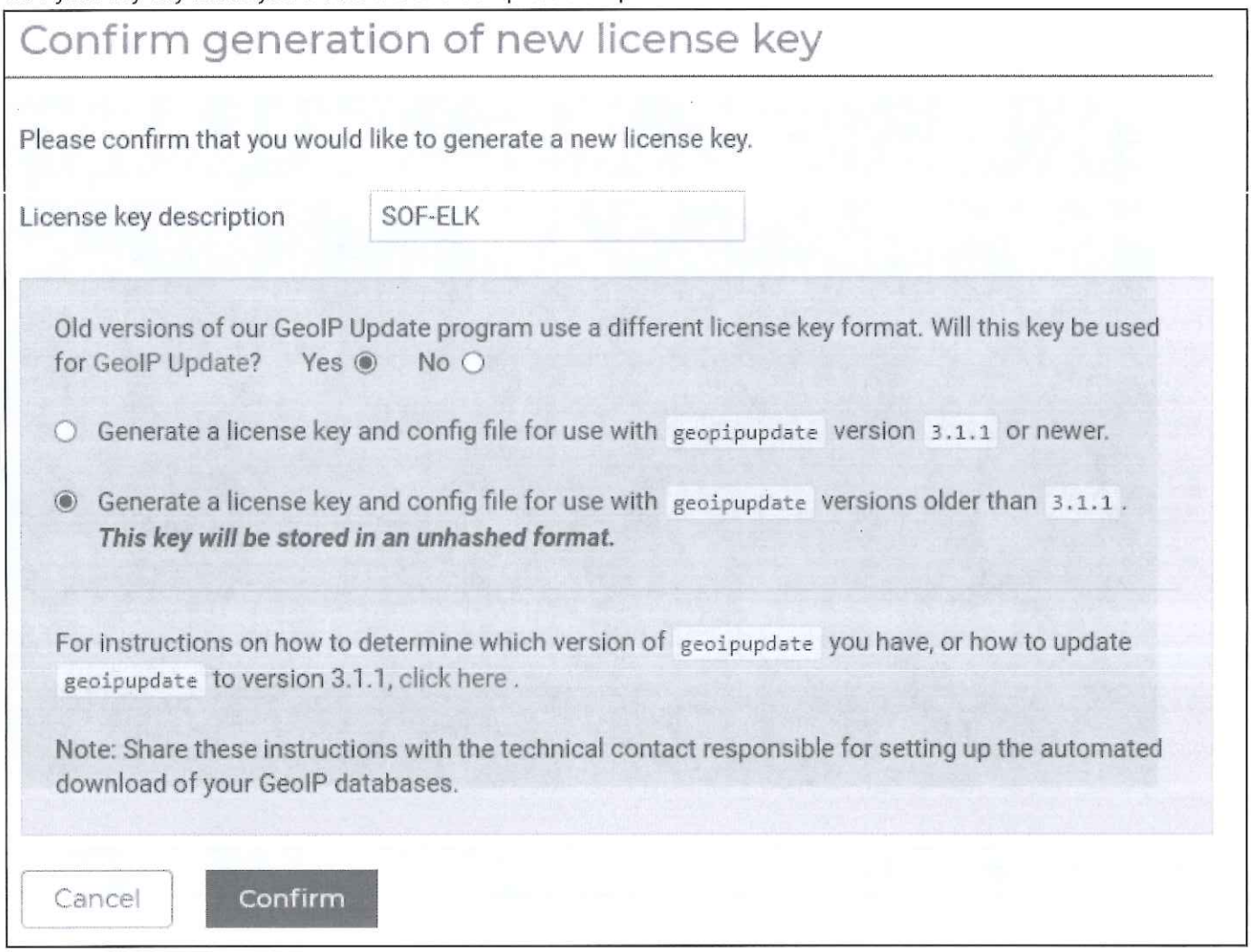
1. Create a free MaxMind account with this link
2. You will receive an email to activate your account and create a password
3. Login to the MaxMind website
4. Select **`Manage License Keys`**



5. Select **`Generate new license key`**

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

6. Give your key any name you would like and complete the options as shown below



7. Once you select `Confirm` you will get you account number and license key



Be sure to save this information

8. Log on to the SOF-ELK VM with the credentials

   - Username: ***elk_user***
   - Password: ***forensics***

You may log on to the console, however it's recommended to log in via SSH.

https://t.me/learningnets

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

9. Enter the command below and provide your account information

```
sudo /usr/local/sbin/geoip_bootstrap.sh
```

```
[elk_user@sof-elk ~]$ sudo /usr/local/sbin/geoip_bootstrap.sh
Do you want to download the MaxMind GeoIP databases?
(This requires free MaxMind account and internet access.)
This prompt will time out in 30 seconds.
Y/N: Y

If you do not already have a MaxMind account, sign up here:
  https://www.maxmind.com/en/geolite2/signup
Once signed in, generate a license key here:
  https://www.maxmind.com/en/accounts/155942/license-key
You have geoipupdate 2.5.0, so ensure you
  create a license key for this version.

Enter your MaxMind Account ID: 537
Enter your MaxMind License Key:
MaxMind GeoIP databases have been installed.
Restarting Logstash to pick up the new database files.

Do you want to set a weekly cron job that will update the MaxMind GeoIP databases automatically?
Y/N: Y
[elk_user@sof-elk ~]$
```

10. If you get an error, retry in a few minutes as it takes a little bit of time for the key to be active
11. You now have a GeoIP database loaded in your SOF-ELK VM which we will use in the next lab

Update SOF-ELK® VM

The SANS team is constantly making improvements to the SOF-ELK VM. To make sure you have the latest configuration and parsers, you will want to run the update script:

```
sudo sof-elk_update.sh
```

If there are no updates, you will get the following result:

```
[elk_user@sof-elk ~]$ sudo sof-elk_update.sh
Up-to-date
[elk_user@sof-elk ~]$
```

If anything has changed, you will see a list of the modified files:

```
[elk_user@sof-elk ~]$ sudo sof-elk_update.sh
[sudo] password for elk_user:
Updating 1990a3f..c197637
Fast-forward
 configfiles/6901-aws.conf         |  1 +
 configfiles/9801-output-aws.conf | 16 ----------------
 2 files changed, 1 insertion(+), 16 deletions(-)
 delete mode 100644 configfiles/9801-output-aws.conf
[elk_user@sof-elk ~]$
```

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Updating the E-Workbook

The electronic workbook site is stored locally in the VM so that it is always available. However, course authors may update the source content with minor fixes, such as correcting typos or clarifying explanations, or add new content such as updated bonus labs. You can pull down any available updates into the VM by running the following command:

```
workbook-update
```

If there are no updates, you will get the following result:

```
[elk_user@sof-elk ~]$ workbook-update
Beginning update process...
- No workbook updates available

Complete!
[elk_user@sof-elk ~]$
```

If anything has changed, you will get a messages that the workbook files have been updated:

```
[elk_user@sof-elk ~]$ workbook-update
Beginning update process...
- Updating workbook files

Complete!
```

Be sure to refresh any pages you are currently viewing (or restart the browser) to make sure you are seeing the latest content.

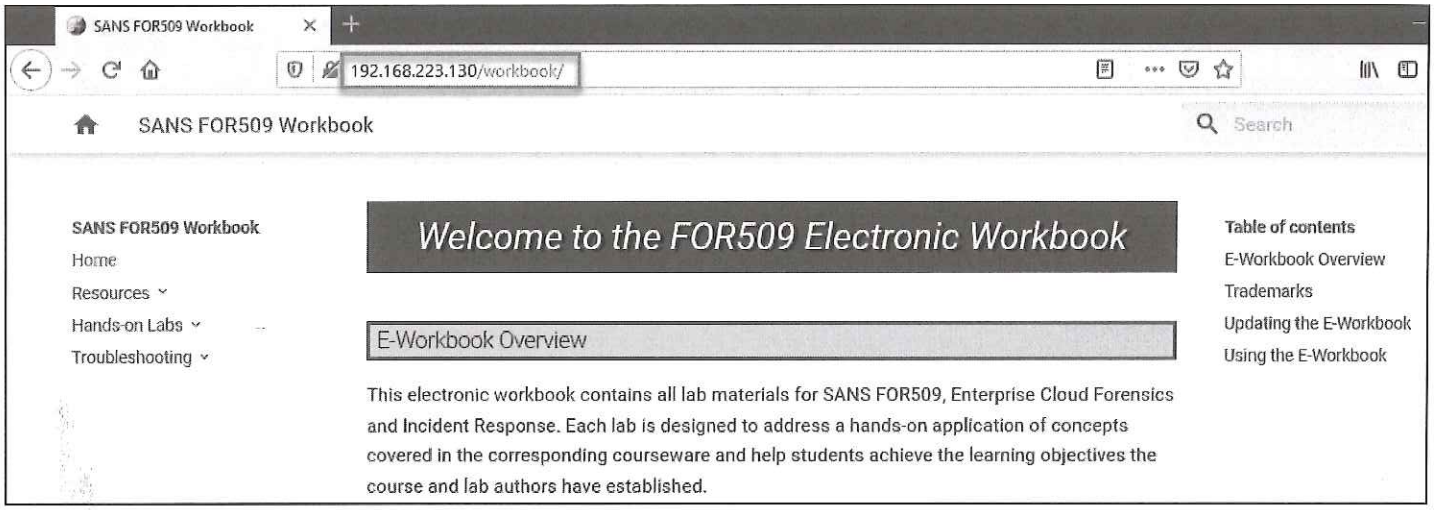
Access the E-Workbook and Kibana via your host's web browser

```
This VM is running the Logstash and Kibana applications.

You can access the FOR509 Electronic Workbook at http://192.168.223.130
You can access Kibana at http://192.168.223.130:5601
You can SSH to this system at IP address 192.168.223.130
```

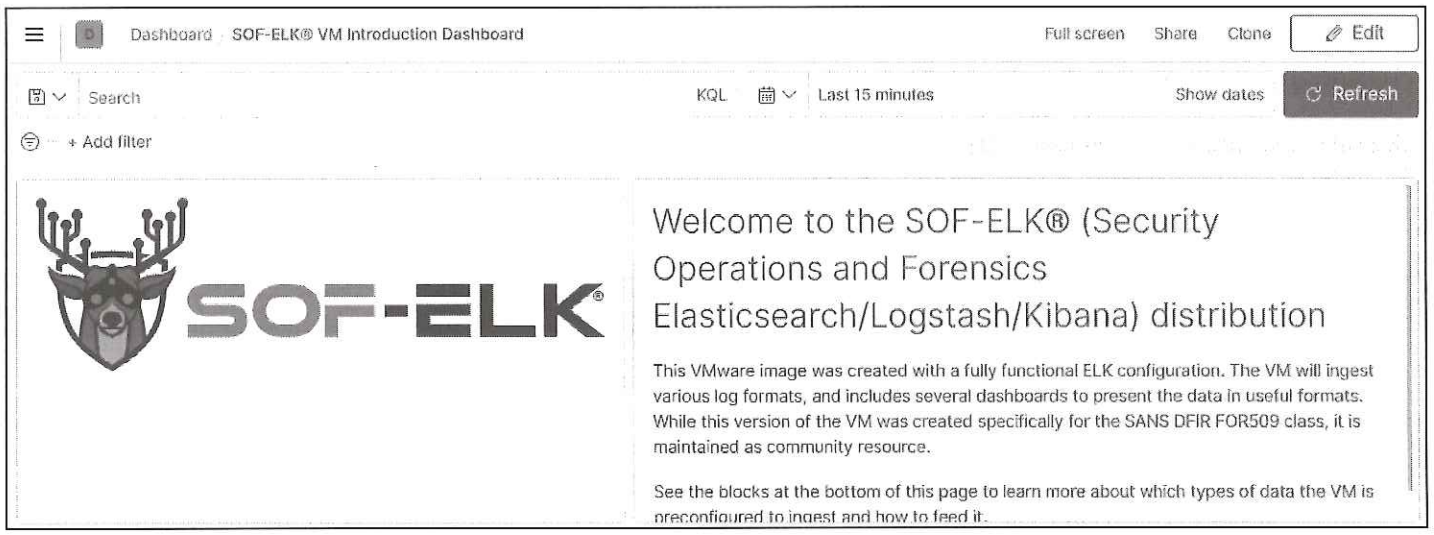
E-Workbook: Using a web browser on your host machine, open the following URL `http://<IP_ADDRESS>/workbook` where the IP is the one displayed in the VMWare console. In this case, it would be `http://192.168.223.130/workbook`

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon



Kibana: Using a web browser on your host machine, open the following URL `http://<IP_ADDRESS>:5601` where the IP is the one displayed in the VMWare console. In this case, it would be `http://192.168.223.130:5601`

You may have to wait a few minutes for Kibana to be ready. Once the page loads, you should see the Kibana default dashboard



Key Takeaways

- You are ready for an exciting week of learning!

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Lab 1.1: Visualize Data in SOF-ELK®

Objectives

- Learn about the Discover, Visualize and Dashboard analytics tab
- Create filters and searches
- Create a dashboard

Background

SOF-ELK is a powerful platform. In this tutorial, we will focus on the elements you will need to complete the FOR509 labs. We encourage you to experiment on your own and load your own data in the future.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Make sure you have completed lab 0
3. Access Kibana via the IP address shown on the SOF-ELK® VM

Load Data

The Microsoft 365 Unified Access Log has been exported from the portal and saved in `/home/elk_user/lab-1.1_source_evidence.zip`

1. Log on to the SOF-ELK VM with the credentials
   - Username: ***elk_user***
   - Password: ***forensics***

   You may log on to the console, however it's recommended to log in via SSH.
2. Extract `ual.csv` from the ZIP file above with the following commands:

```
cd ~
unzip -q lab-1.1_source_evidence.zip -d /logstash/office365
```

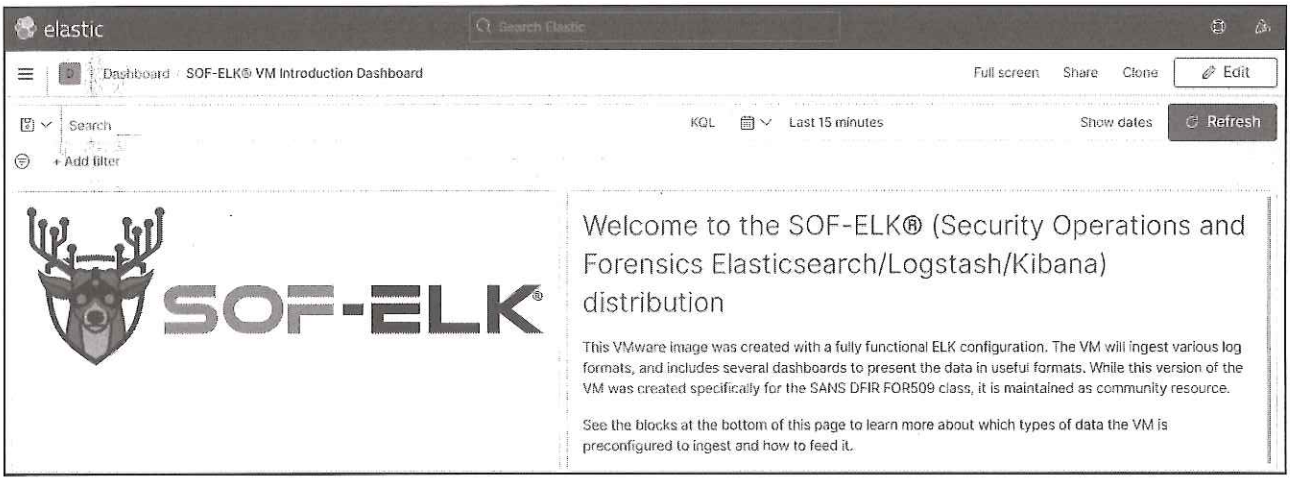

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

> ⚠ **Warning**
>
> Do not run this command more than once!

3. Wait 2 minutes for the data to be processed. The data is now available in the `office365-*` index.

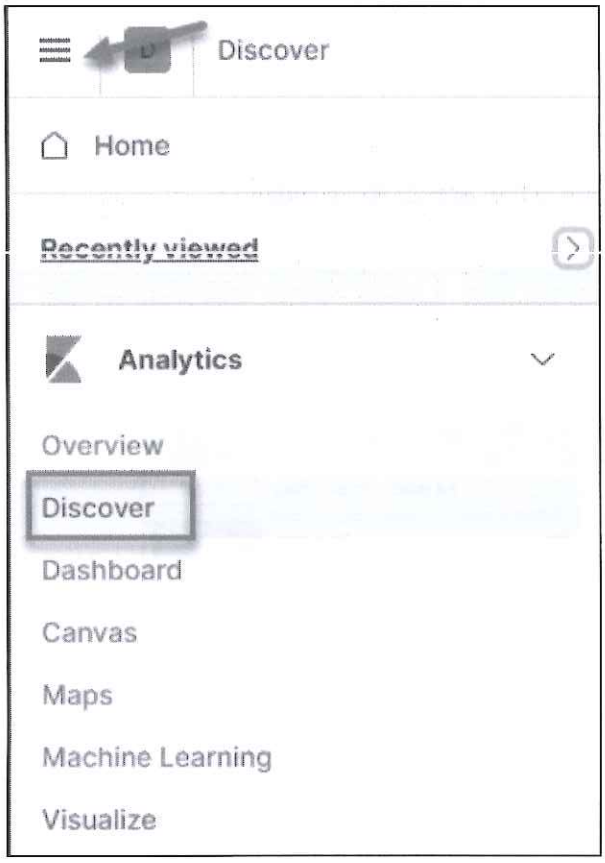
Lab Content

Kibana will initially show you the SOF-ELK VM Introduction Dashboard with a default timeframe of "Last 15 minutes".

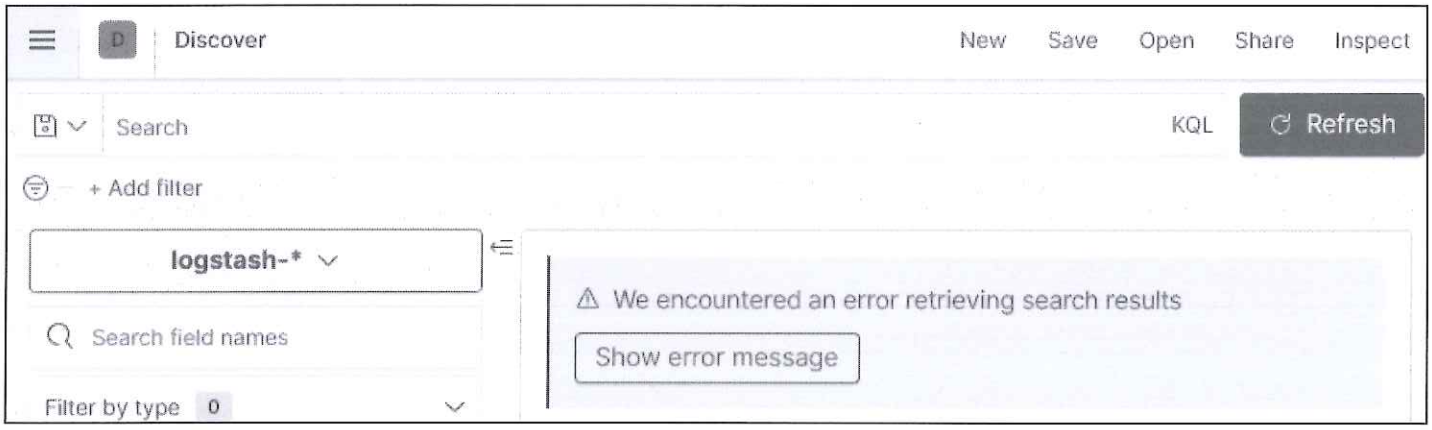


We will start with the `Discover` tab (top left).

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

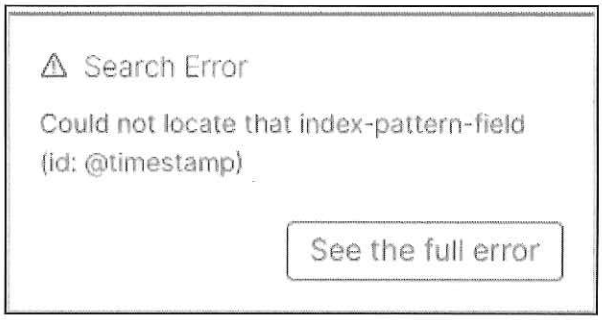


By default, Kibana starts with the `logstash-*` index but since we don't have any data loaded in that index for FOR509, you are going to get an error message.



You will also get a popup on the lower right of your screen which you can close.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

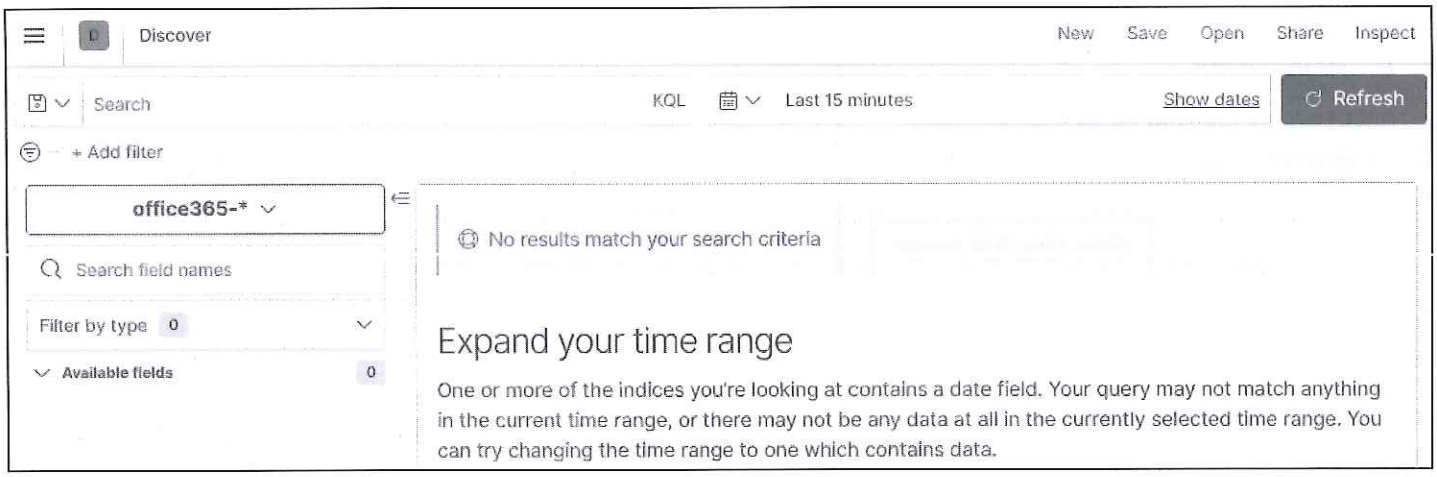


Our data is stored in different indices. Select the `office365-*` index:



You will get another error since you don't have any data from the "Last 15 minutes".

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

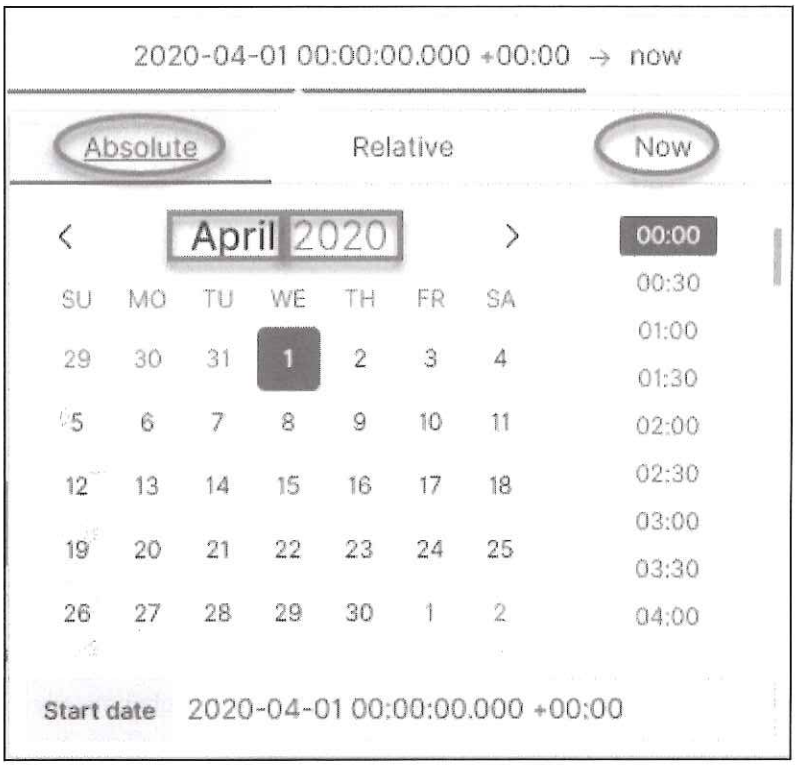


So, first thing is to set your timeframe. For the purposes of this tutorial, set your timeframe to `2020-04-01 00:00 to now`.

To set your timeframe, you will click on the date and select `Absolute`. This will bring up a calendar. You can navigate through the months by selecting `<` and `>`. However, a great shortcut is to click on the month or year. This will give you a menu where you can quickly select the appropriate month or year and is a lot faster.

https://t.me/learningnets

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



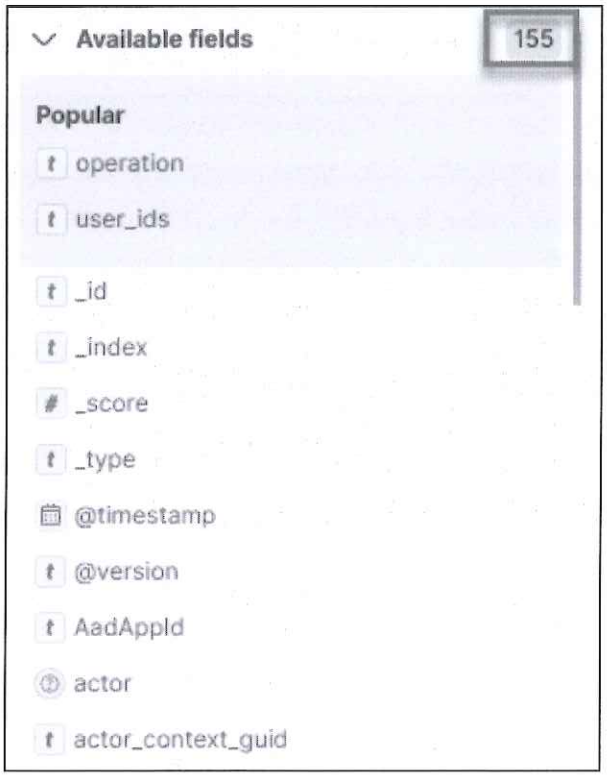


 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



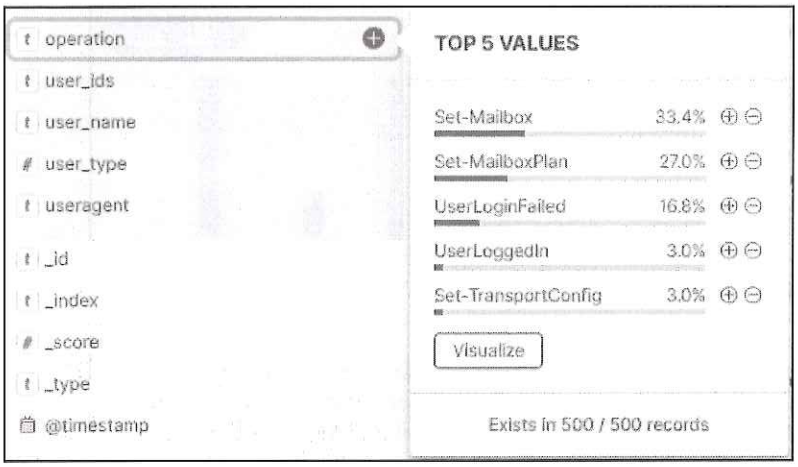
Don't forget to hit `Update`.

On the left, you will have a list of all the fields present in that index (155 in our example). Fields are sorted alphabetically with recently used fields at the top (highlihgted in light blue) under the heading "Popular". This is important to remember as you may be looking for a specific field down the list only for it to be at the top because you recently used it.



© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

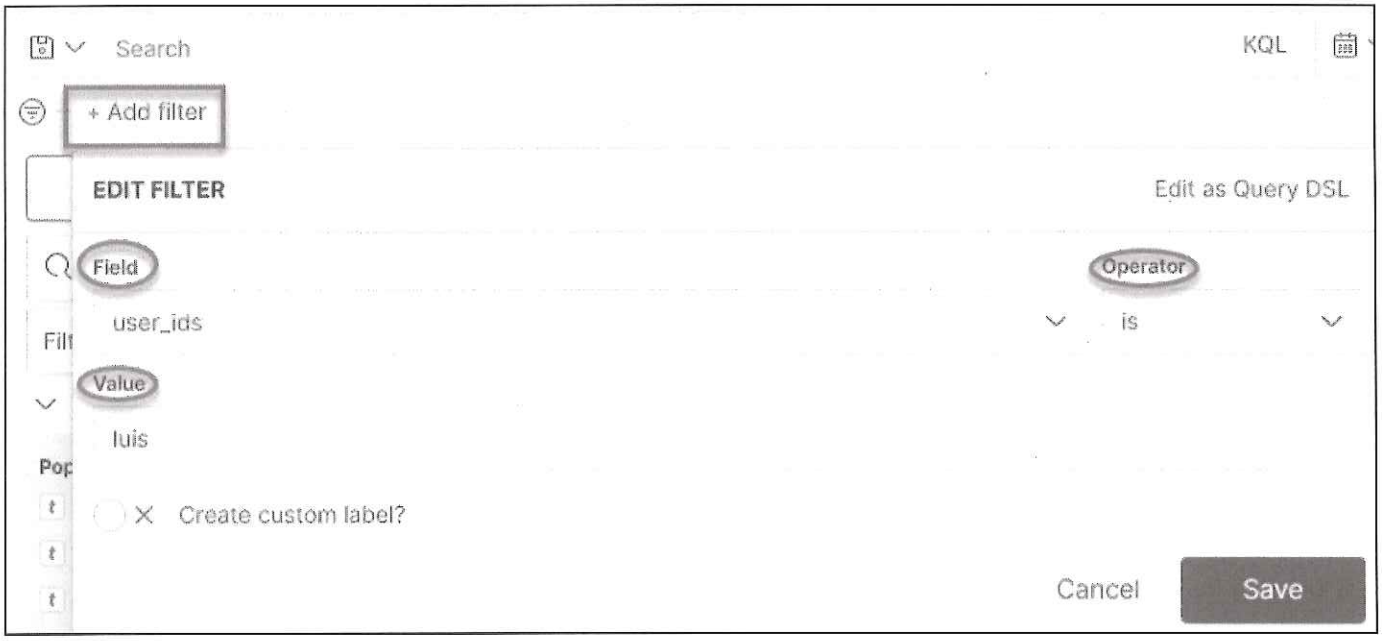
If you click on a field, it will give you the top 5 values. Note that this quick analysis is limited to 500 records even if you have thousands in your index. Also, the results will be different based on the timeframe you have selected as well as any filters or searches that are currently active.



1. Filters and searches in the Discover analytics tab

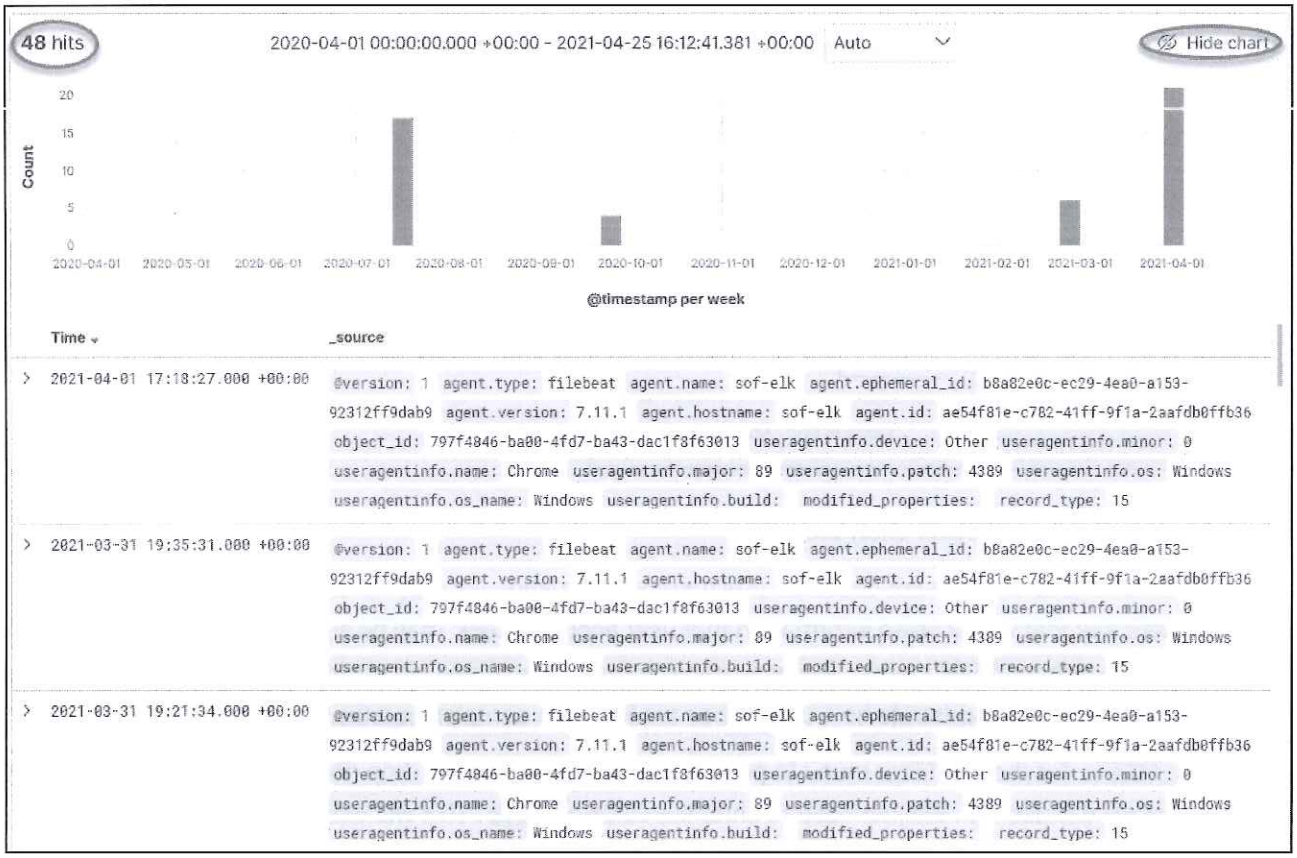
   The first step is to reduce our data set based on preliminary information we may have received. For the purposes of this example, let's say that we received information that user account `Luis` may be subject to a brute force attack. We will therefore search for failed logins. This is a simple enough search and we could do everything on the search bar, but let's use a filter to demonstrate how useful they are for more complex queries.

   Select `+ Add filter` for the Edit Filter menu to pop-up. Under "Field", use the drop down menu to select `user_ids`. For the operator we will use `is`. We just need to enter the value of `luis`. This will work because `user_ids` is an analyzed field. If you accidentially select `user_ids.keyword`, the value would need to be `Luis@pymtechlabs.com`. Kibana will try to help you by showing you that choice as you type.



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

The main screen now shows us a graph as well as the list of raw records. On the top left, we see the number of records that remain after our filter is applied. On the top right, you can hide the graph if you want to save some real estate on your screen.



You can expand any of the records by selecting the > next to that record.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



This long list of records isn't the ideal way to view the data. Instead, we can select a few fields and create a table. Select `user_ids`, `operation` and `workload` by selecting the + next to them.



You now have a much simpler view of the records and can still select > if you want to view the details of any record.

48 hits

Time	user_ids	operation	workload
2021-04-01 17:18:27.000 +00:00	Luis@pymtechlabs.com	UserLoggedIn	AzureActiveDirectory
2021-03-31 19:35:31.000 +00:00	Luis@pymtechlabs.com	UserLoggedIn	AzureActiveDirectory
2021-03-31 19:21:34.000 +00:00	Luis@pymtechlabs.com	UserLoggedIn	AzureActiveDirectory
2021-03-31 19:13:36.000 +00:00	Luis@pymtechlabs.com	UserLoggedIn	AzureActiveDirectory
2021-03-31 19:12:49.000 +00:00	Luis@pymtechlabs.com	UserLoggedIn	AzureActiveDirectory
2021-03-31 19:12:44.000 +00:00	Luis@pymtechlabs.com	UserLoggedIn	AzureActiveDirectory
2021-03-31 19:11:08.000 +00:00	Luis@pymtechlabs.com	UserLoggedIn	AzureActiveDirectory

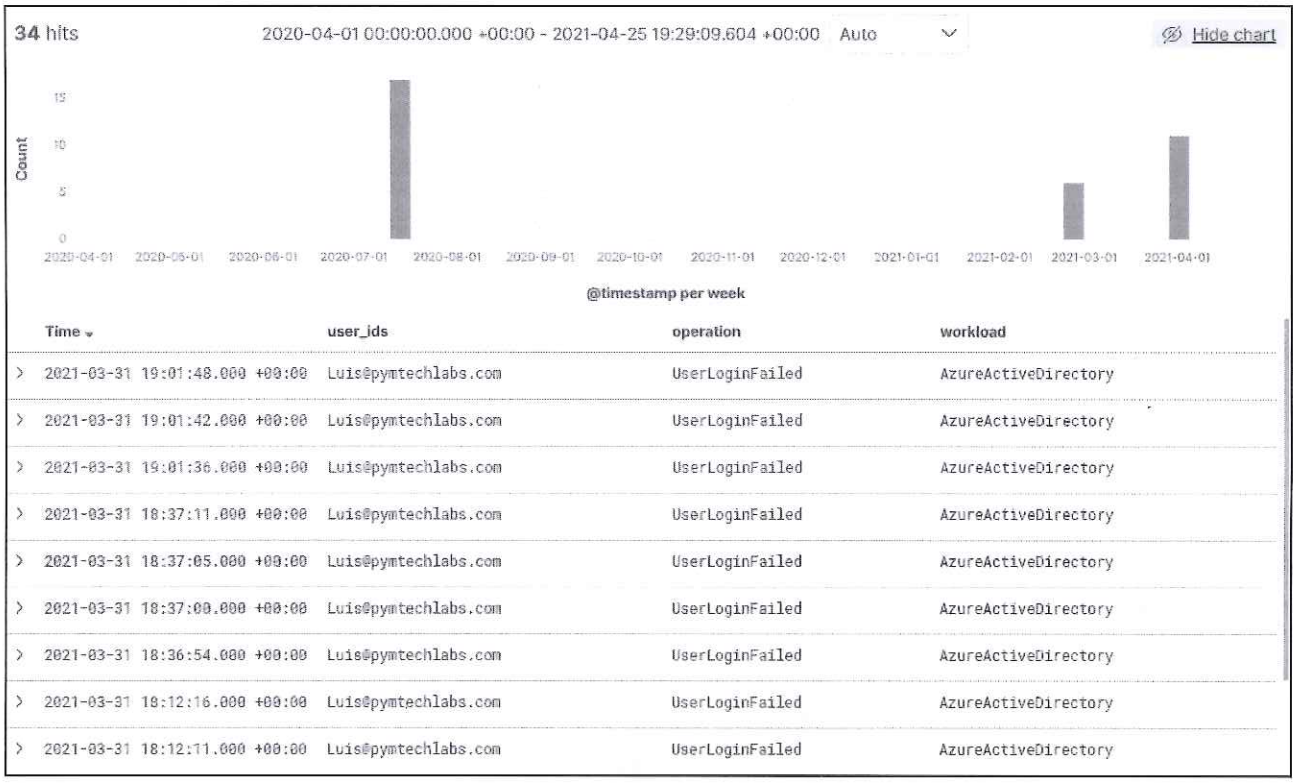
We now want to limit our search to failed logins. In the search bar enter:

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

```
operation : UserLoginFailed
```



and don't forget to click `Update`.



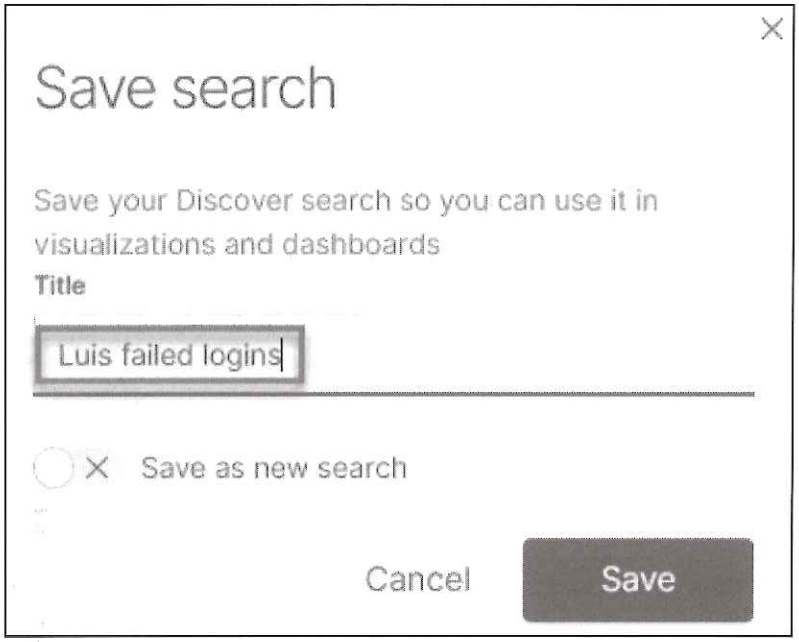
Time	user_ids	operation	workload
2021-03-31 19:01:48.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 19:01:42.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 19:01:36.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 18:37:11.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 18:37:05.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 18:37:00.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 18:36:54.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 18:12:16.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory
2021-03-31 18:12:11.000 +00:00	Luis@pymtechlabs.com	UserLoginFailed	AzureActiveDirectory

We now see that Luis had 34 failed logins over the timeframe and that these failed logins are distributed over 3 separate days. An interesting data point but before we draw any conclusions, let's use the visualization feature and compare successful versus failed logins for all our users.

Before we move on, let's save this filter and search. Call it `Luis failed logins`.



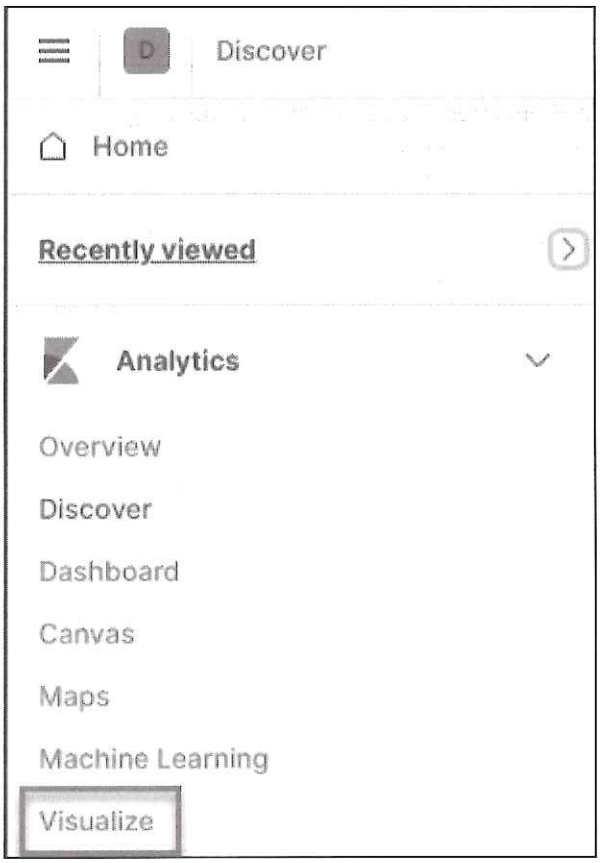
© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Before you move to the next section, clear your filters and don't forget to hit `Update`.

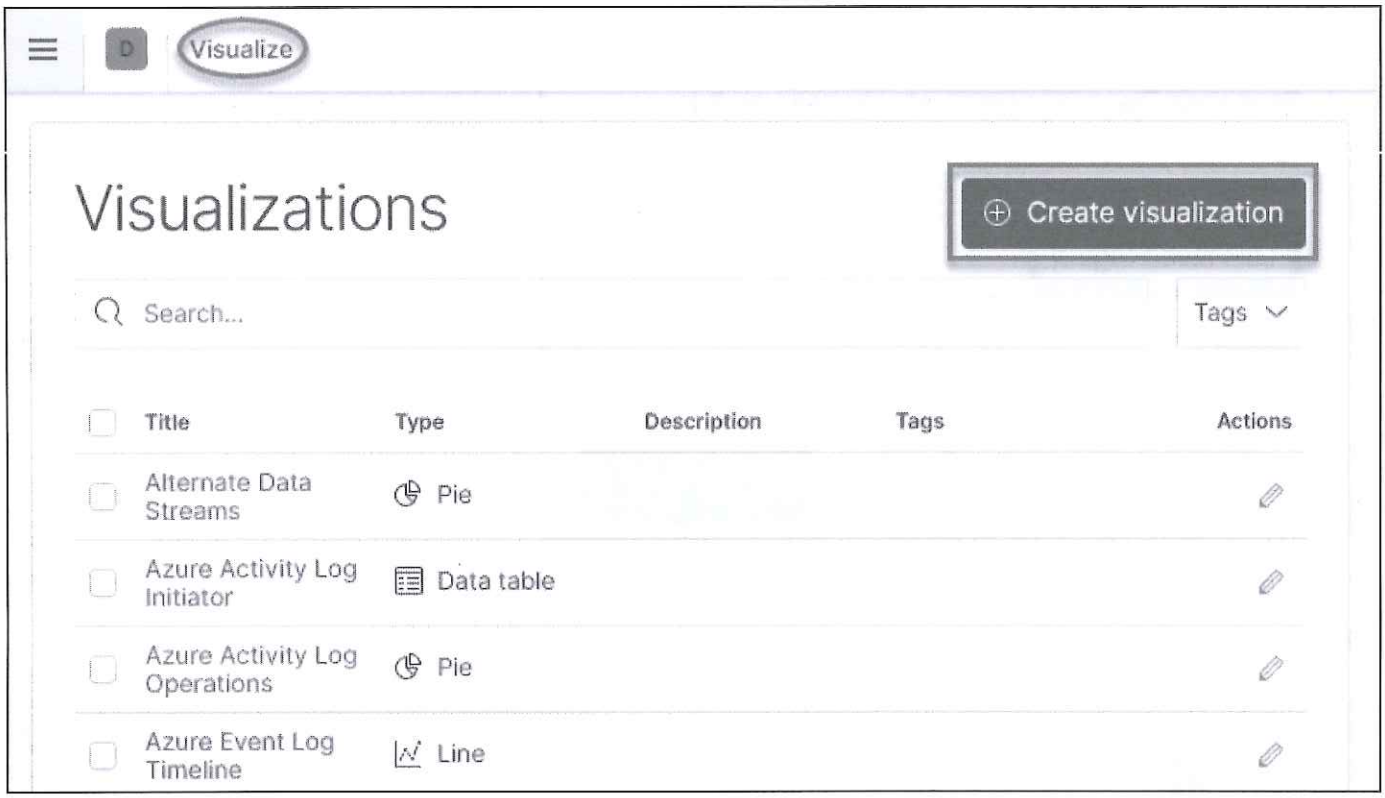
2. Creating graphs with the Visualization tools

Switch to the Visualize tab.

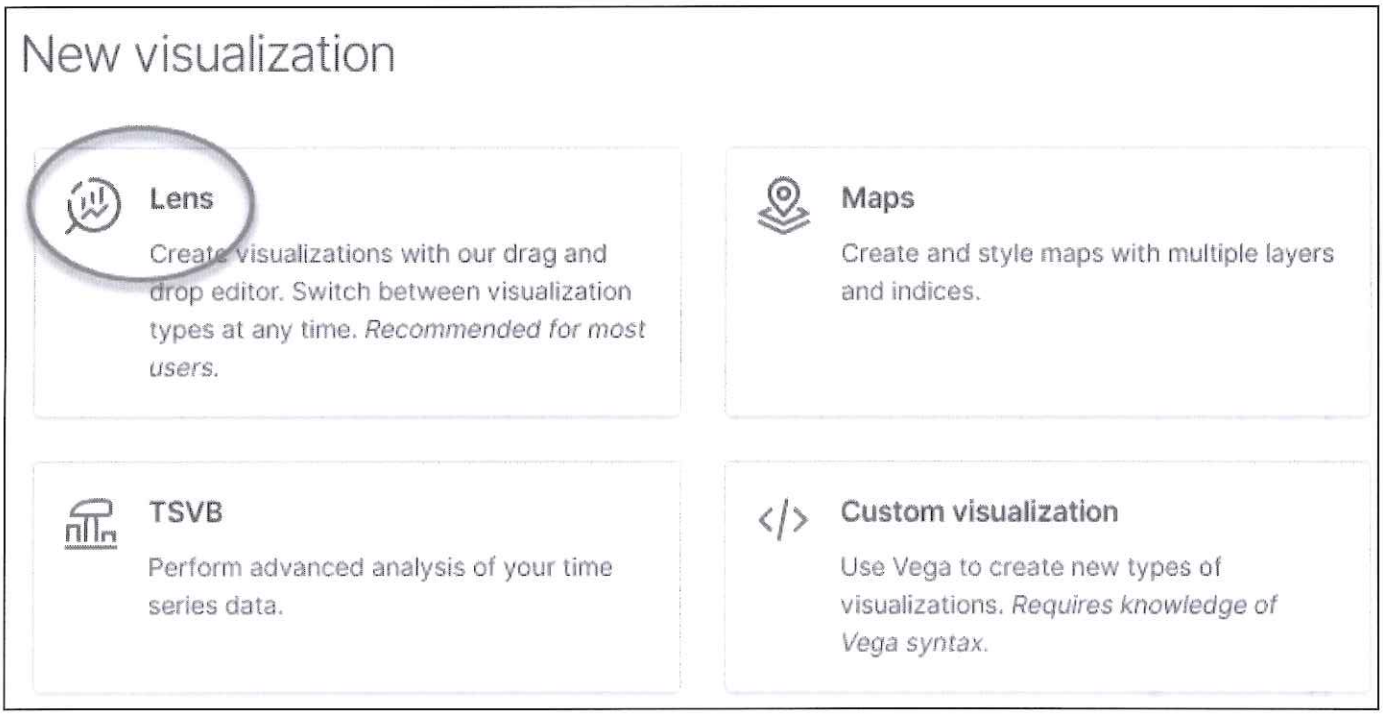


 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

You may get a list of previously saved visualizations or a prior graph. If you get an existing graph, simply select `Visualize` and you will get the list. Select `Create visualization`.



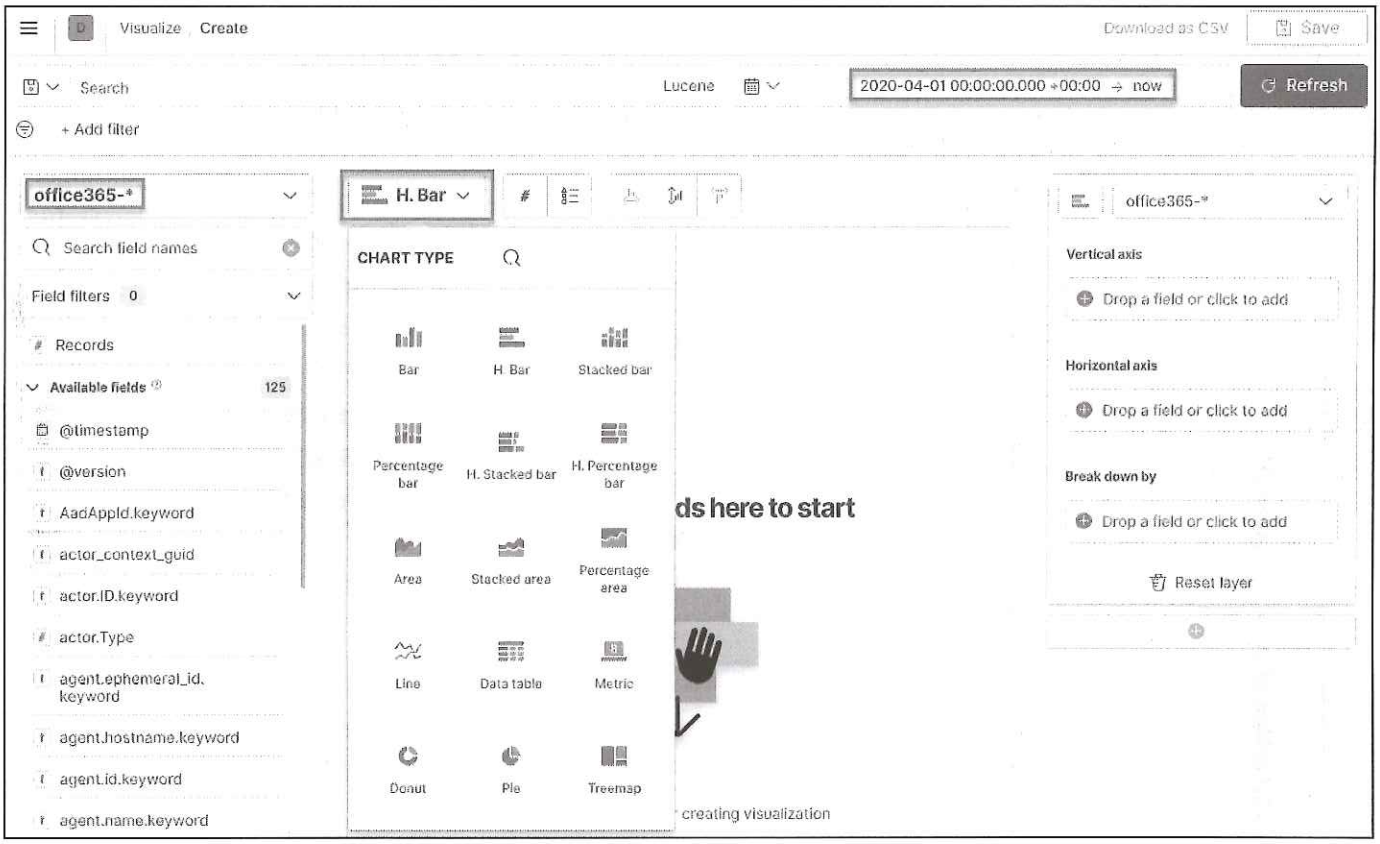
Select `Lens` which is the easiest way to create a visualization as it provides drag and drop functionality.



https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

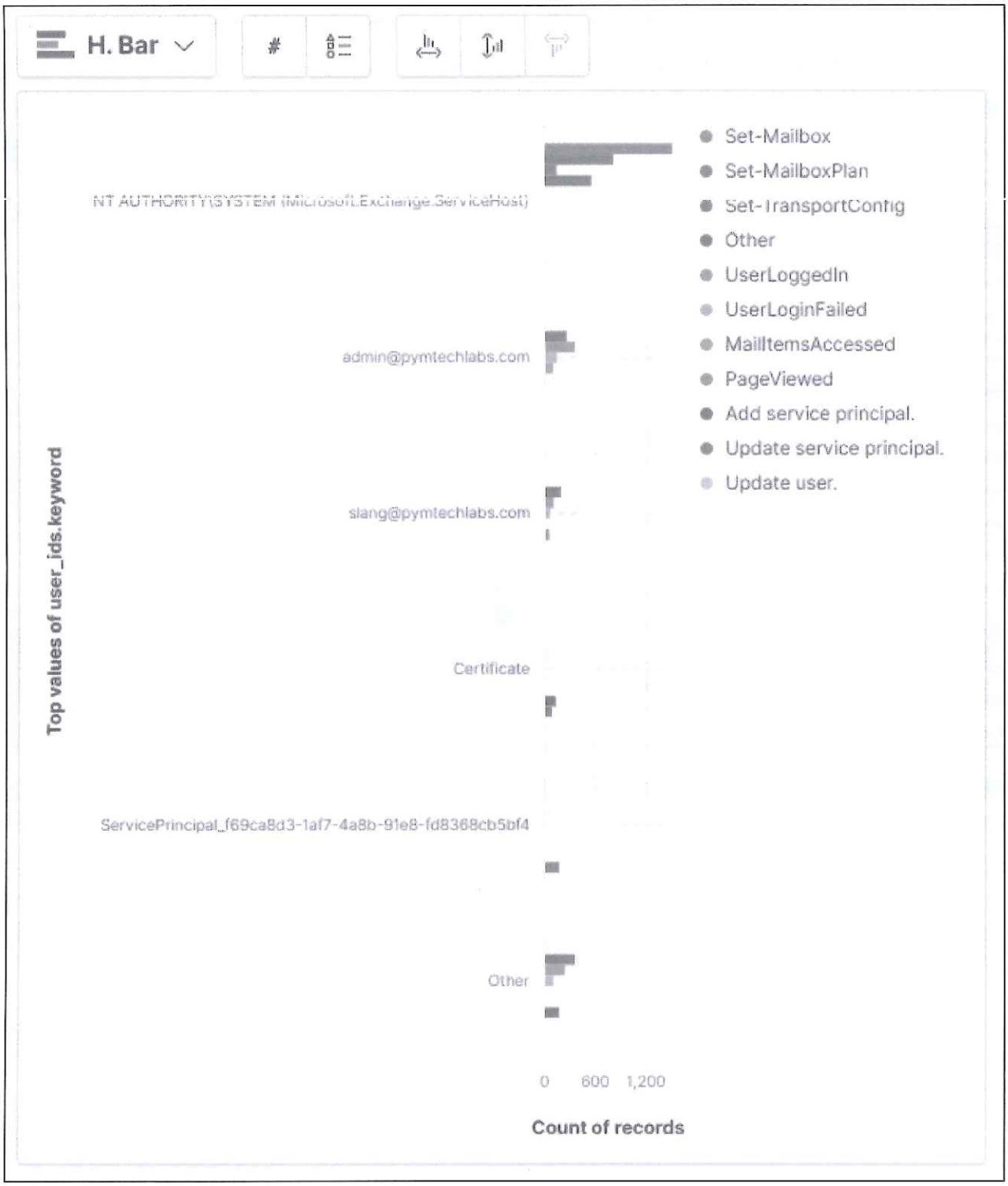
Make sure your index is still set to `office365-*` and the timeframe `2020-04-01 00:00 to now`.

You can select any chart type you would like. In this case, we will select `H. Bar`.



First drag and drop the field `user_ids.keyword`. **Second** drag and drop the field `operation`.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



We now have two issues to deal with:

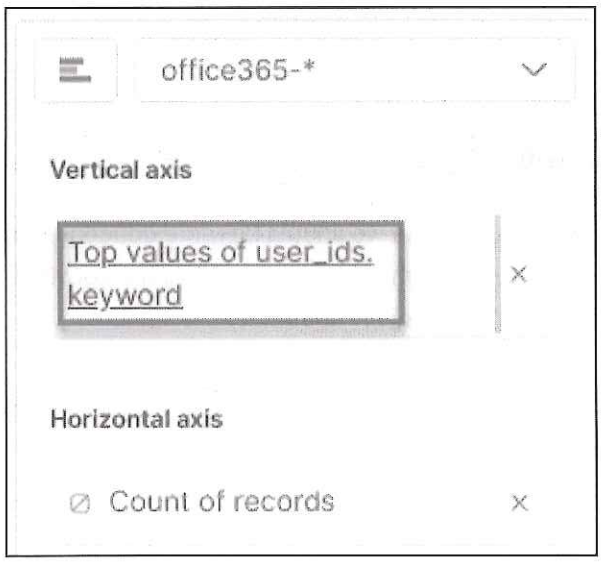
- we have too many `operation` that have nothing to do with logins
- we have system type ids

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Create a filter to limit `operation` to `UserLoggedIn` and `UserLoginFailed`. The operator `is one of` allows you to create a list of items which is very useful in this situation.

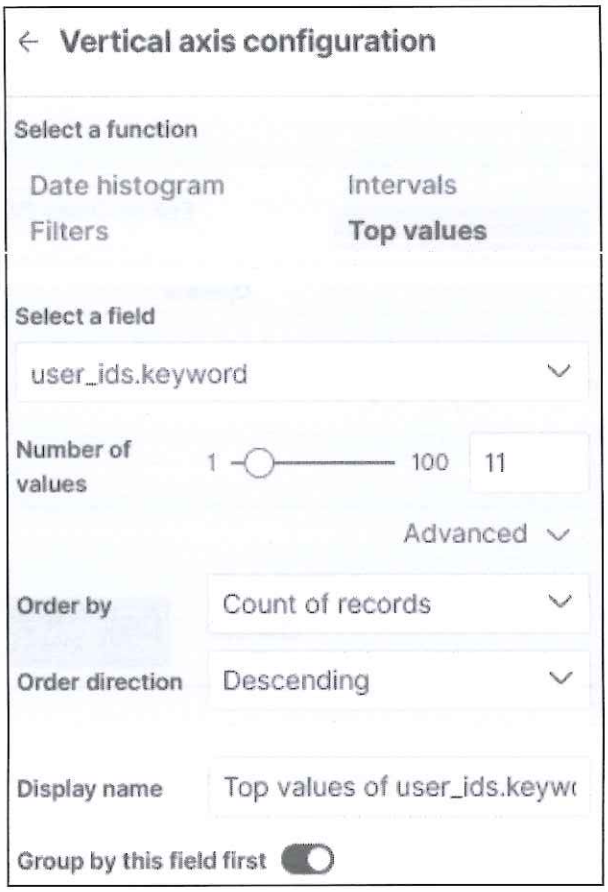


We now have a chart that only shows us successfull and failed logins. Before we write a search to remove the system-type user ids, we need to expand the `Other` category to make sure we see all records. On the top right, select `Top values of user_ids.keyword`.



Increase the `Number of values` until the `Other` category disapears. In this case 11 will do it.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

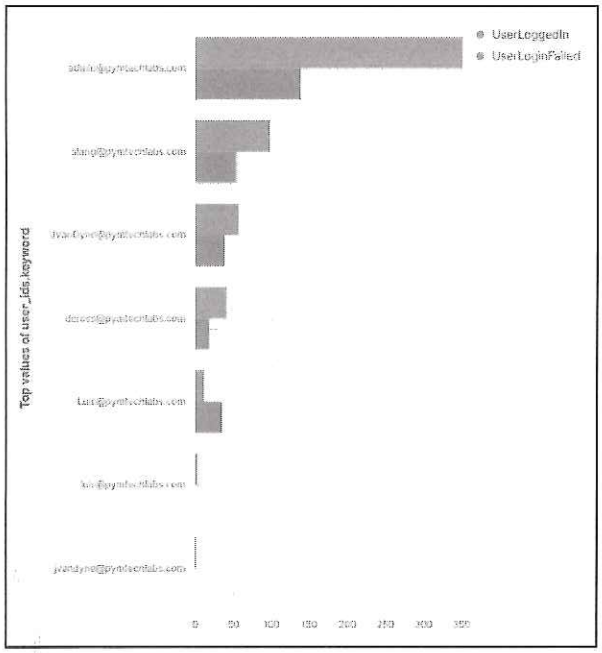


Use the search:

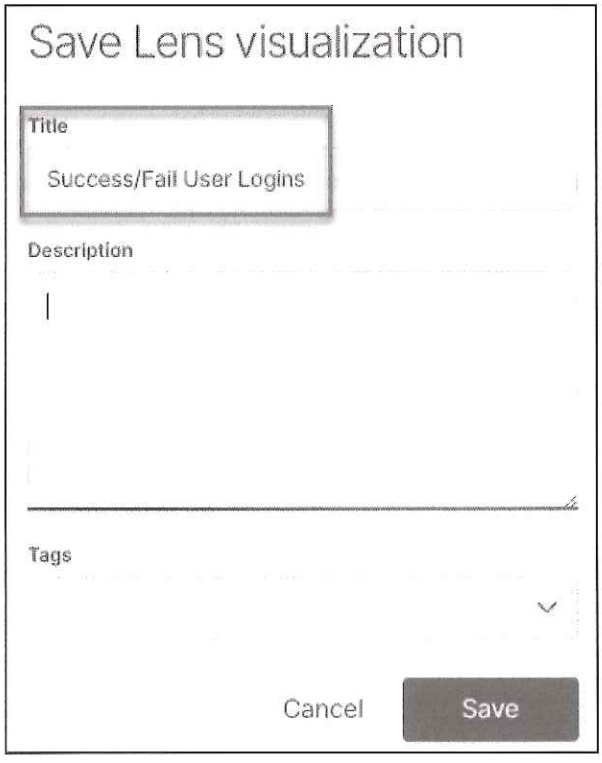
```
not user_ids : (675* OR 1fb* OR Unknown OR "Not Available")
```

We now have a nice chart of every user's successful and failed logins. Looks like we should be more concerned about all the failed logins against `admin@pymtechlabs.com`. Some of you may think why would you use such an obvious username. The answer is simple: free data generation! Yes, the account has 2 factor authentication enabled.

Technet24



Last step is to save our chart. On the top right, select `Save` and call it `Success/Fail User Logins`.

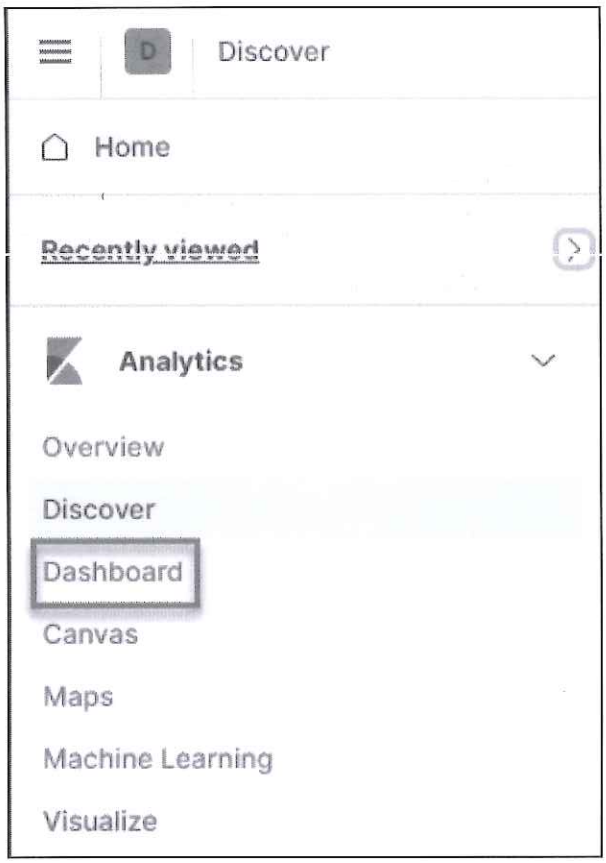


We are now ready to create a dashboard.

3. Create a dashboard

There's nothing like a nice dashboard to impress management. So let's create a dashboard.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



This will take you back to the introduction dashboard. Click on the word `Dashboard` to open the dashboard menu.

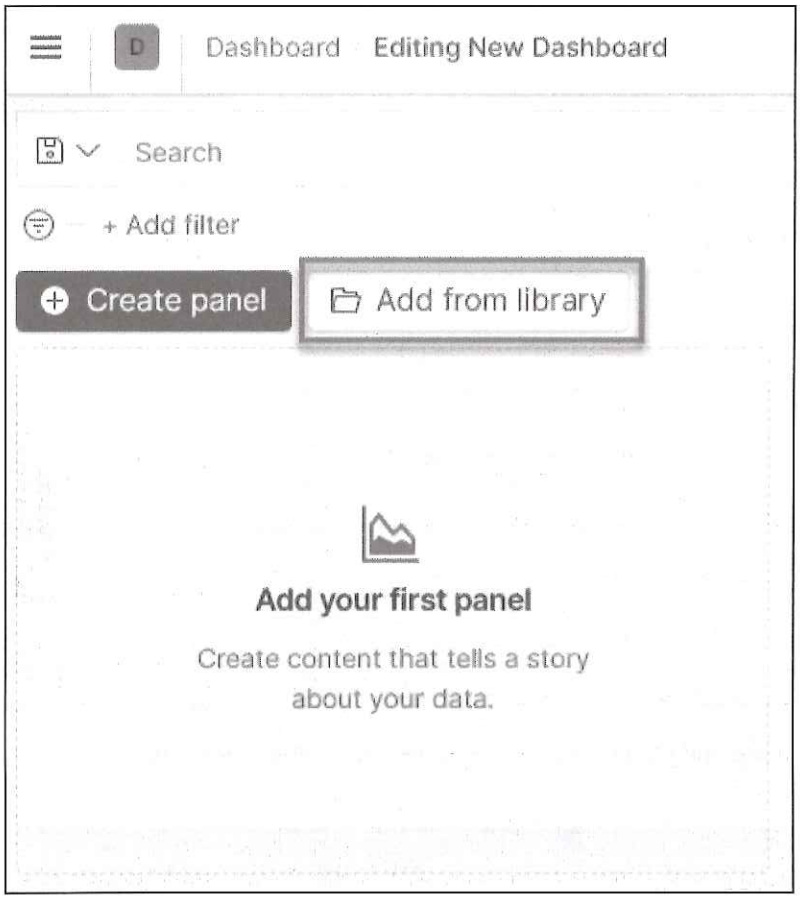


Select `Create dashboard`.



Since we previously saved our search and our chart, we just need to add them from library.

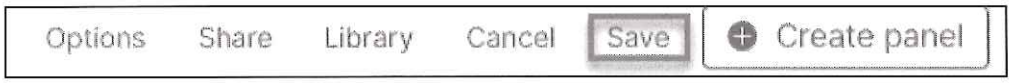
© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Repeat the procedure twice to add:

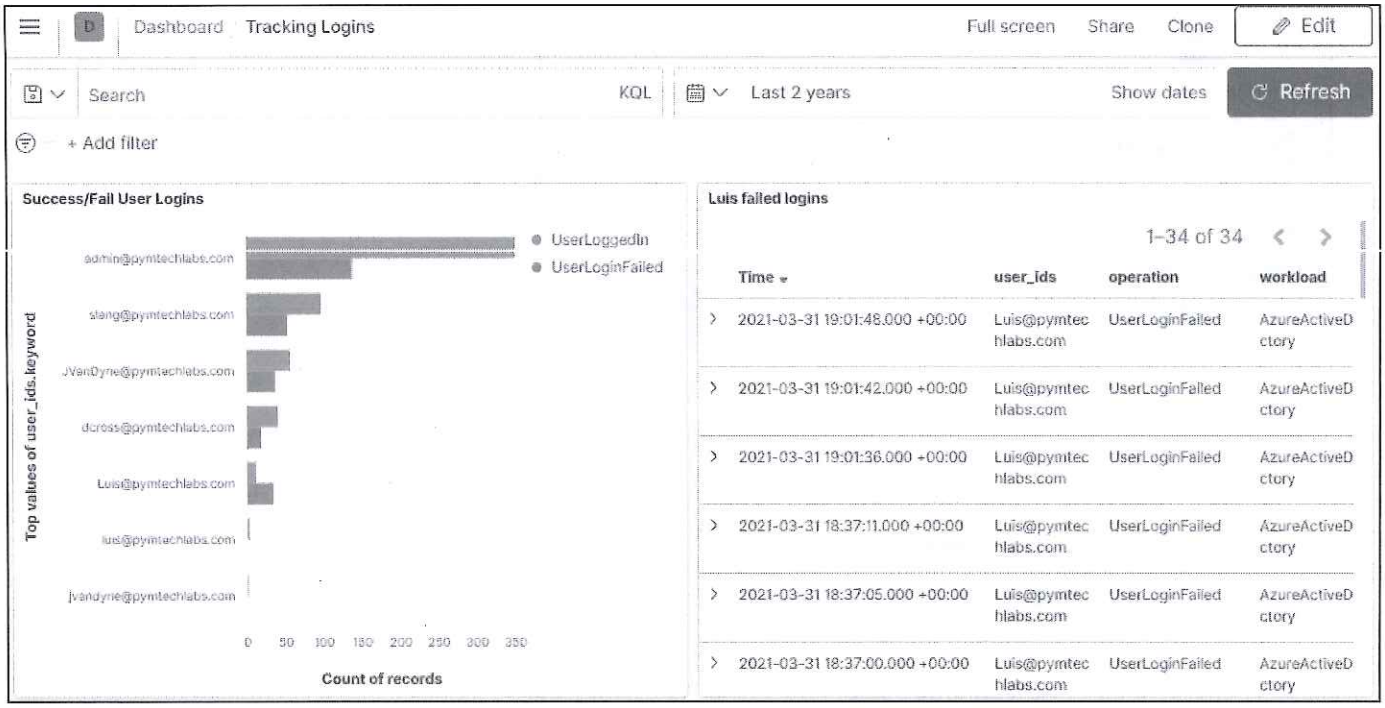
- `Success/Fail User Logins` chart
- `Luis failed logins` search

You can now save your dashboard.



You now have a complete dashboard.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



As you can see, dashboards are very easy to create and possibilities are only limited by your creativity.

Key Takeaways

- Kibana is a powerful platform, yet easy to use
- Now that you have a basic understanding of SOF-ELK, you are ready to explore the FOR509 labs!

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Lab 1.2: Find the Source of a BEC

Objectives

- Review logs from Microsoft 365 to understand user activity
- Search for possible unauthorized access

Background

At the end of June 2020, Janet Van Dyne was attending the International Biochemical Engineering conference in Amsterdam. While there she finally heard back from the payroll department regarding the problems she has been having with her paycheck. However, something tingled her bio-synthetic wings regarding the email. She sent Darren Cross an email asking for his advice but with the time difference, it was going to be a while before she received an answer. Wanting the issue resolved as soon as possible, she clicked on the link in the email.

The link took her to the usual Microsoft 365 login page where she entered her credentials, but not to the payroll site as she expected. She informed Frank Pym of the suspicious email and it's now your task to figure out what happened.

Preparation

To prepare:

1. Make sure your SOF-ELK VM is running
2. Make sure you have completed lab 0 and lab 1.1
3. Access Kibana via the IP address shown on the SOF-ELK VM

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful.

In lab 1.1 you loaded the Microsoft 365 Unified Access Log into SOF-ELK.

If you haven't completed either of these steps, please go back and do so now.

Lab Content

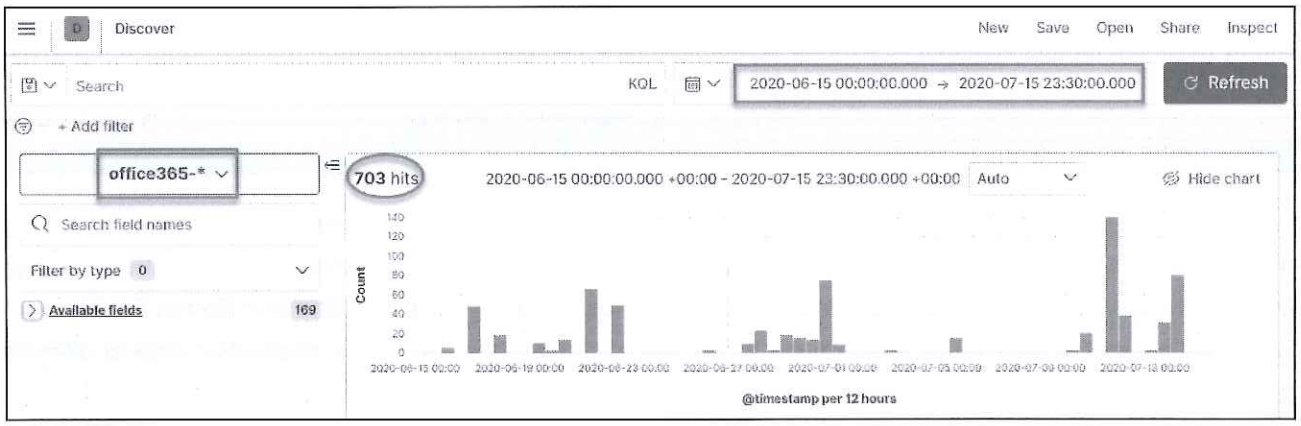
Start in the Discover tab

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Be sure to clear any prior filters.

We weren't given the exact time frame for the conference, only told "at the end of June 2020". Let's set our timeframe to `2020-06-15 00:00 to 2020-07-15 23:30 UTC`

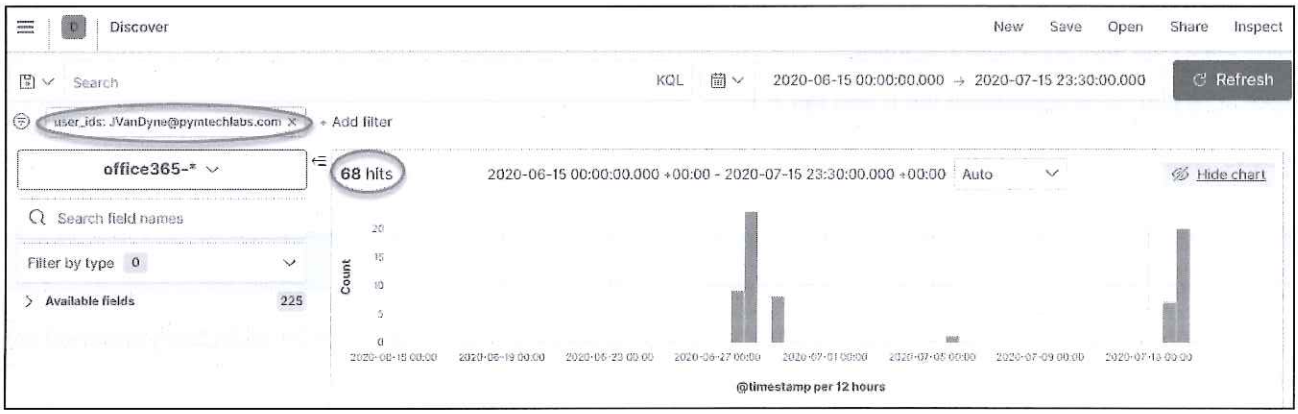
You should see `703 hits`. If you don't make sure you have selected the correct index. Click to see picture.



1. Filter for Janet Van Dyne

Create a filter to only show events related to Janet Van Dyne. How many records remain?

68



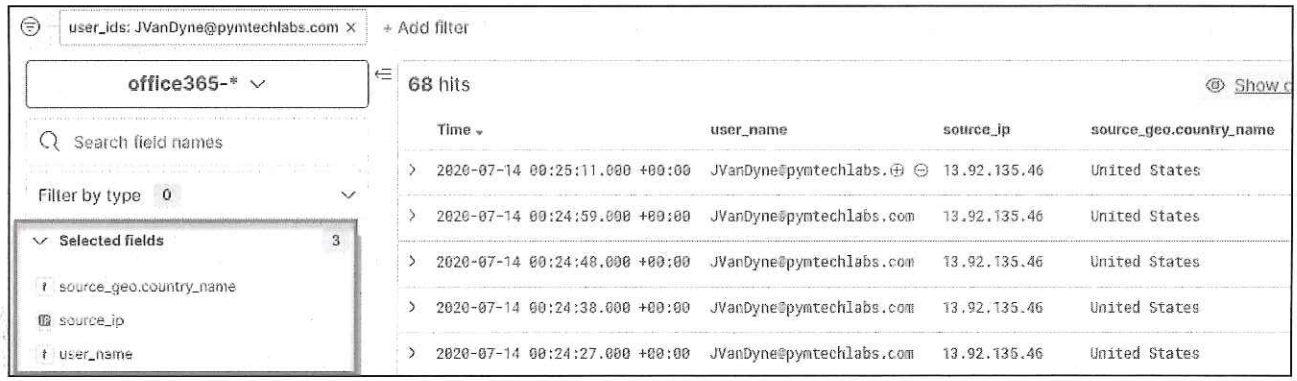
You could write the filter on the search bar, but using the "Add filter" option keeps your working area cleaner. Either way works just fine.

Which fields would you select to analyze the data?

- user_name
- source_ip

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Thanks to the geoip data, we can find out where these IPs are from. Add the field `source_geo.country_name` to your selected fields.



2. Look for suspicious locations

When was Janet attending the conference?

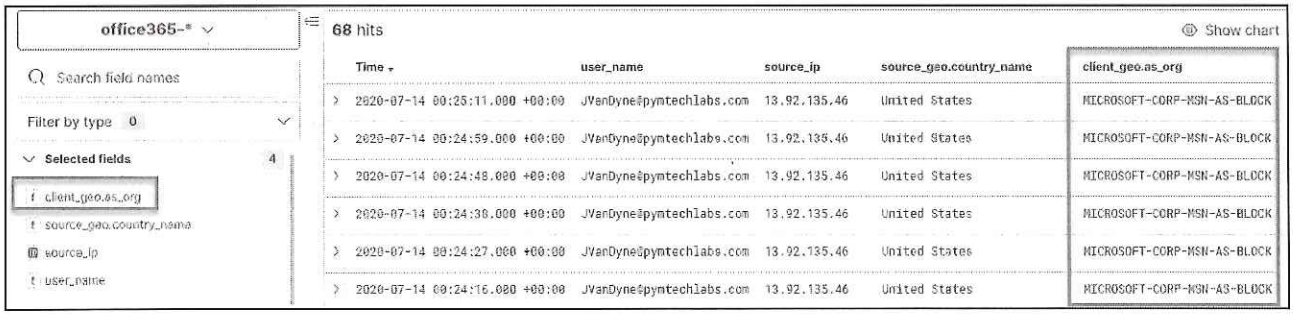
Hint: look for IPs from the Netherlands
2020-06-27 to 2020-06-29

Are there entries that look suspicious?



Note

It can be difficult to identify the origin of an IP address. The geoip data also includes the name of the ISP. Add the field `client_geo.as_org` to your selected fields. You will notice many entries from Microsoft.

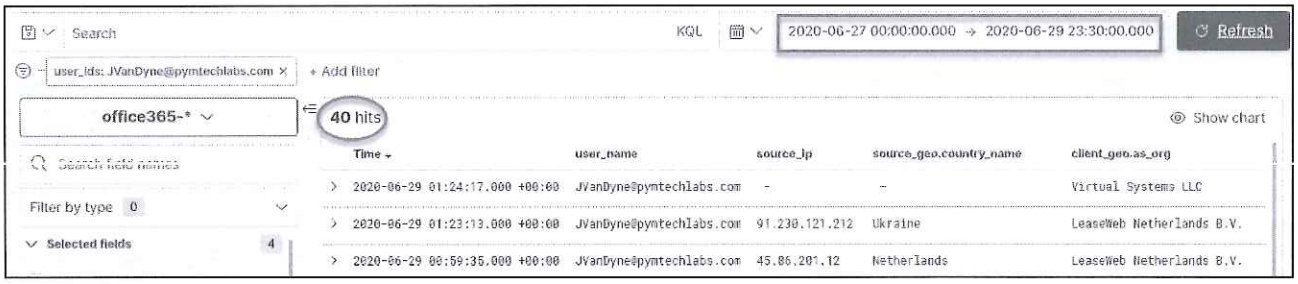


3. Analyze the logs

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

At this point it would be a good idea to narrow down the timeframe further to

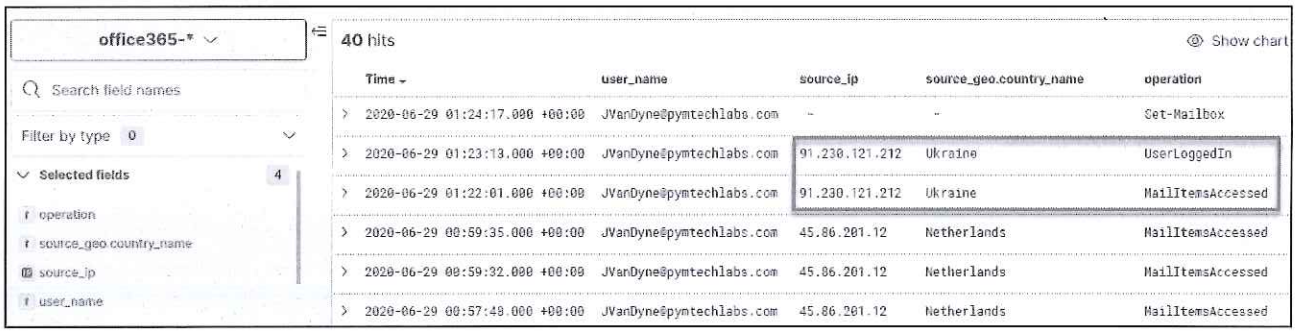
`2020-06-27 00:00 to 2020-06-29 23:30`



What activities did the suspicious log entries perform?

MailItemsAccessed and UserLoggedIn

You can either open each record and look through the various fields or add the `operation` field to your selected fields



Given that Janet Van Dyne is in Amsterdam (confirmed by numerous log entries from the Netherlands) she is most likely not the one who logged in from the Ukraine.

Our logs have a limited number of events so the next step is pretty obvious. However, in your enterprise, you are likely to have a much larger number of events. To figure out what actions the attacker may have taken, we need to widen our timeframe and search for their IP address.

Don't forget to remove any active filter and selected fields.

What fields contain IP addresses?

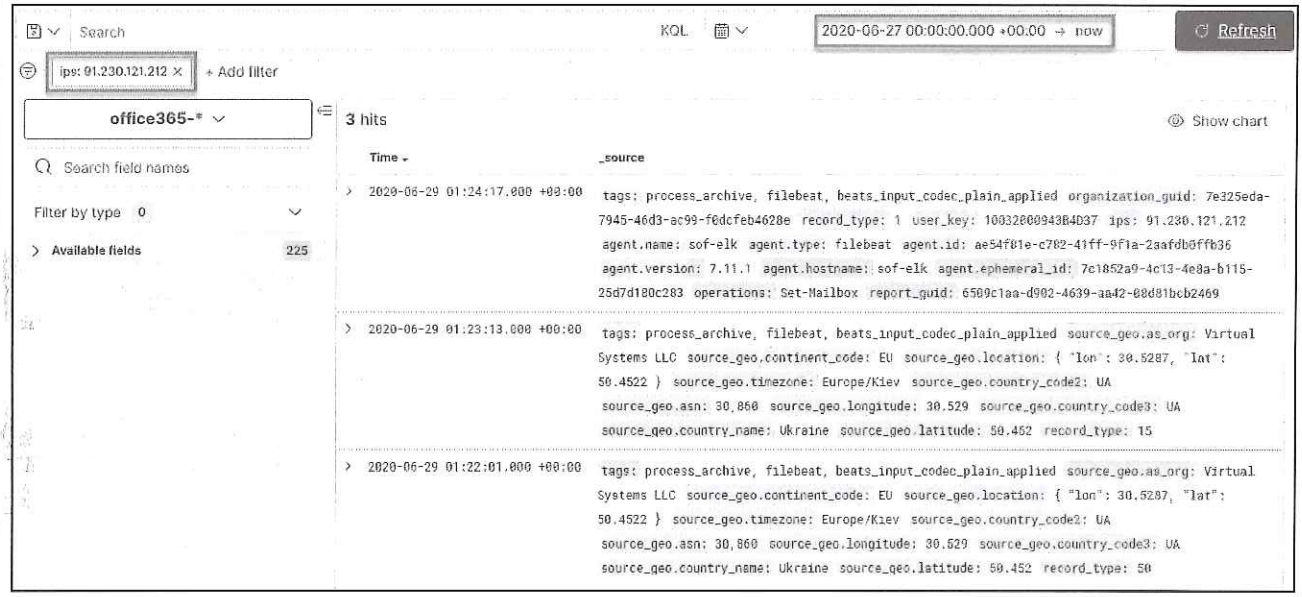
- source_ip
- client_ip
- ips

The field `ips` is simply a list of all IPs found in the record. This is very useful since we don't always know which IP field a log will choose. Also, remember that the authors had to make some mapping choices in the logstash script. In reality, the UAL fields are called `ClientIp` and `ActorIPAddress`. This mapping is necessary due to the inconsistent naming across different logs.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

How many events have the bad IP address?

3



Note

We extended the time from the known date of the bad activity until `now`. This provides the widest possible view in case the attacker performed multiple actions over multiple days. Remember that our current view is limited to the `office365-*` index. In a real situation, you would want to check this IP address against all your indices.

What action did the attacker perform?

First the attacker accessed Janet's mailbox

t	mailbox_owner_upn	JVanDyne@pymtechlabs.com
t	operation	MailItemsAccessed

Second, the attacker made a change to Janet's mailbox, specifically they set a forwarding address

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

t	operations	Set-Mailbox
t	organization_guid	7e325eda-7945-46d3-ac99-f0dcfeb4628e
t	organization_name	pymtechlabs.onmicrosoft.com
t	originating_server	DM6PR06MB6364 (15.20.3131.026)
◕	parameters.DeliverToMailboxAndForward	true
t	parameters.ForwardingSmtpAddress	smtp:JVanDyne@pyntechlabs.com

What method did the attacker used to access Janet's mailbox?

IMAP

t	client_info_string	Client=POP3/IMAP4;Protocol=IMAP4

IMAP is a favorite method for bad actors to test if they have captured valid credentials.
`client_info_string` is a good field to monitor for potential problems.

Is there something unusual about that email address?

The attacker registered a domain that has one letter misspelled compared to the real domain: pyntechlabs instead of pymtechlabs

Key Takeaways

- Make sure to audit all Set-Mailbox actions and look for the parameter `DeliverToMailboxAndForward` and `ForwardingSmtpAddress`.
- There is a similar parameter called `ForwardingAddress` which has the same effect; however, it requires administrative privileges to set.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Lab 2.1: Reviewing CloudTrail Logs

Objectives

- Learn how to analyze IAM logs in CloudTrail
- Learn how to determine where an access originated from
- Learn how to determine how the access occured

Background

Welcome to Pymtech's AWS Group! We need you to take a look at our CloudTrail IAM logs to figure out what's been going on. We've noticed some strange activity in our AWS tenant and we are hoping you can figure it out. We've exported the logs out CloudTrail into SOF-ELK® under the AWS index.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the AWS parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

The AWS Cloudtrail logs for this lab have already been exported from our S3 Bucket. We've tried to make the loading process as close to what you will do in the real world. As such with how AWS stores data there is a two step loab process.

The CloudTrail Logs for lab-2.1 have been saved into `/home/elk_user/lab-2.1_source_evidence.zip` .

1. Log on to the SOF-ELK VM with the credentials
    - Username: ***elk_user***
    - Password: ***forensics***

    You may log on to the console, however it's recommended to log in via SSH.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

2. Extract the all the files from the ZIP file above with the following commands:

```
cd ~
unzip -q lab-2.1_source_evidence.zip
```

3. Run the AWS Cloudtrail ingestion script

```
cd ~
aws-cloudtrail2sof-elk.py -r ./lab-2.1_source_evidence -w /logstash/aws/lab1.json
```

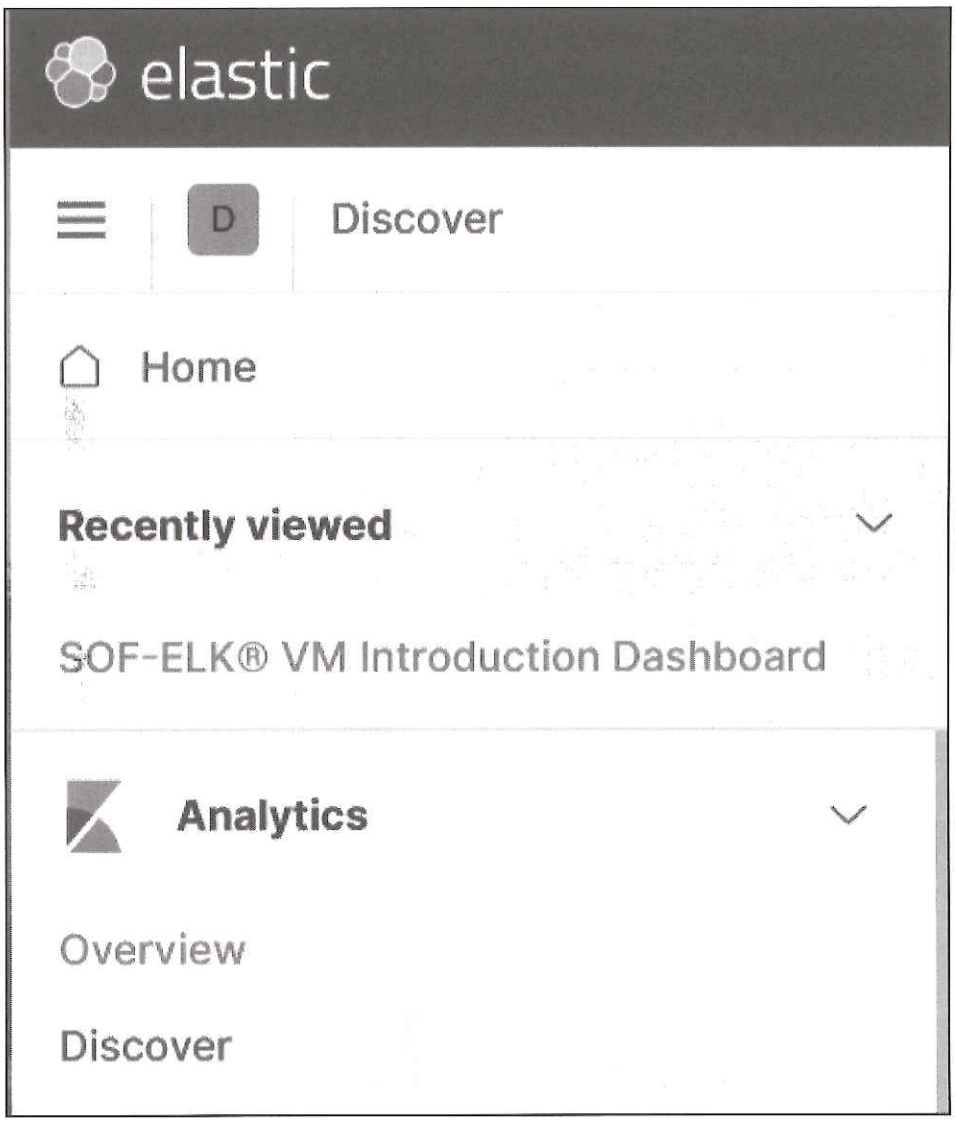
> ⚠ **Warning**
>
> Do not run this command more than once!

4. Wait 2 minutes for the data to be processed. Once it is complete the data will be available in the `aws-*` index.

Lab Content

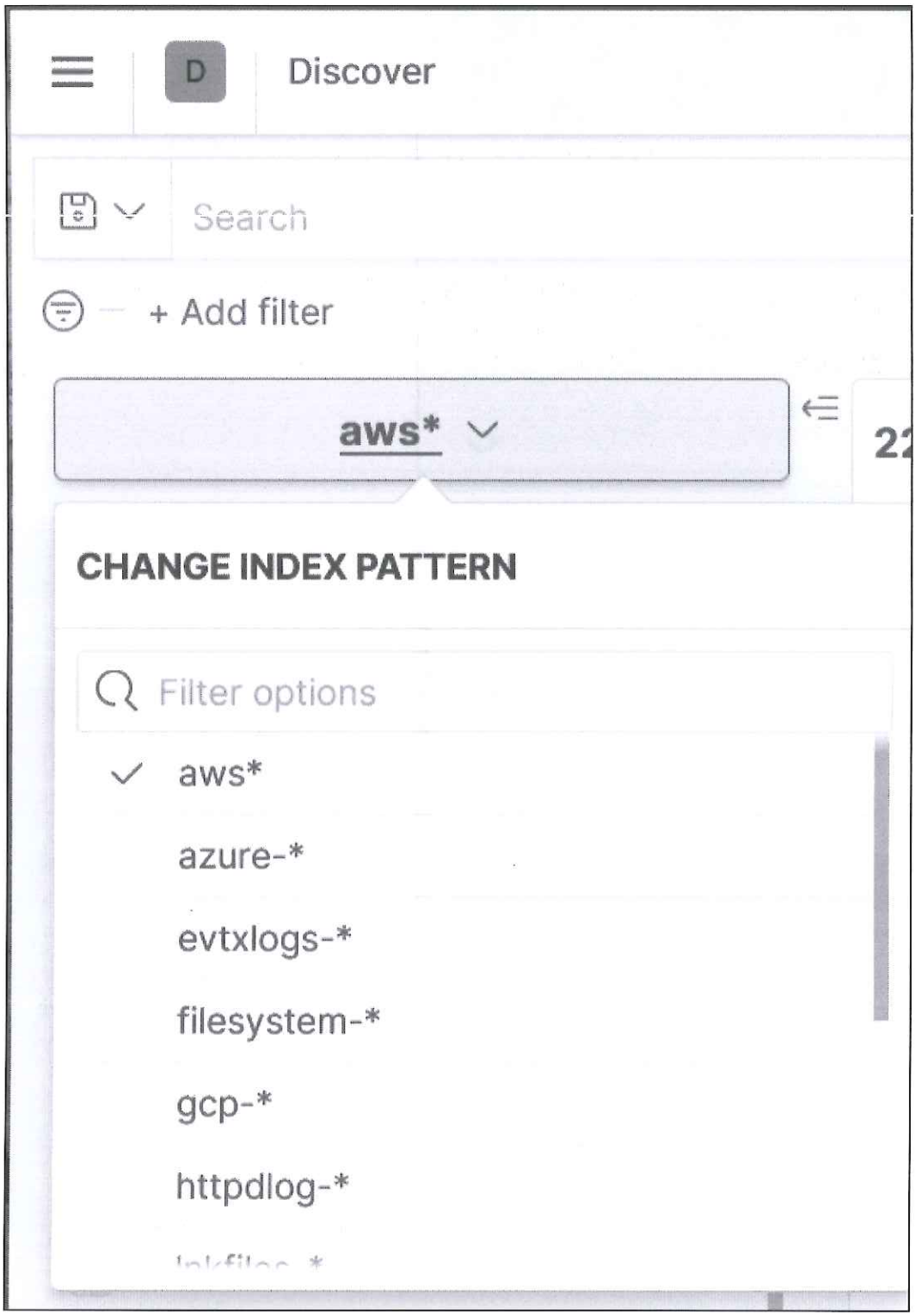
Once you've connected to Kibana your going to want to click on the menu on the upper left and select 'Discover'

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Now that you are in the Discover screen you will want to choose the AWS index, click on the down arrow and select aws as shown in the picture below.

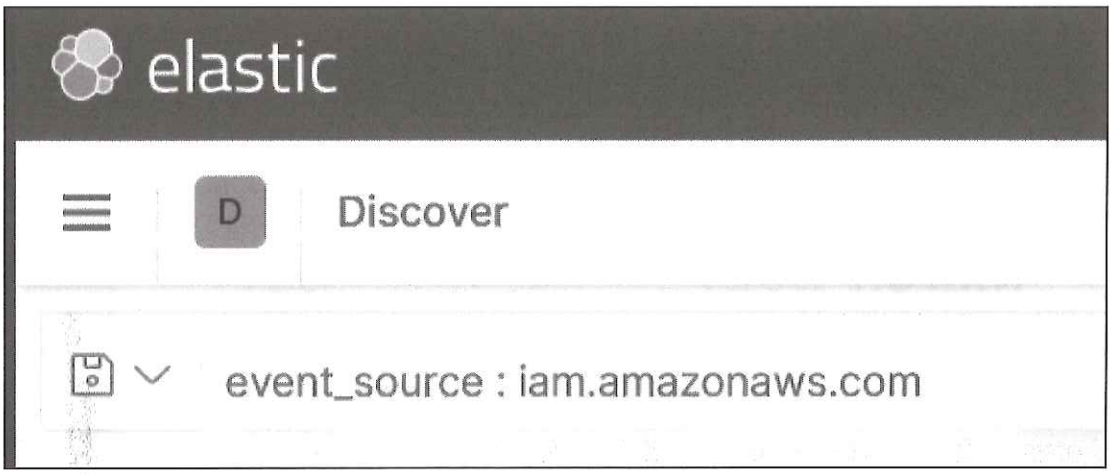
 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



In the filter bar on the top you will want to filter down our CloudTrail logs to just those that were generated by the IAM service. This service tracks the authentications to the AWS tenant, whether through the console, api or from assumed roles.

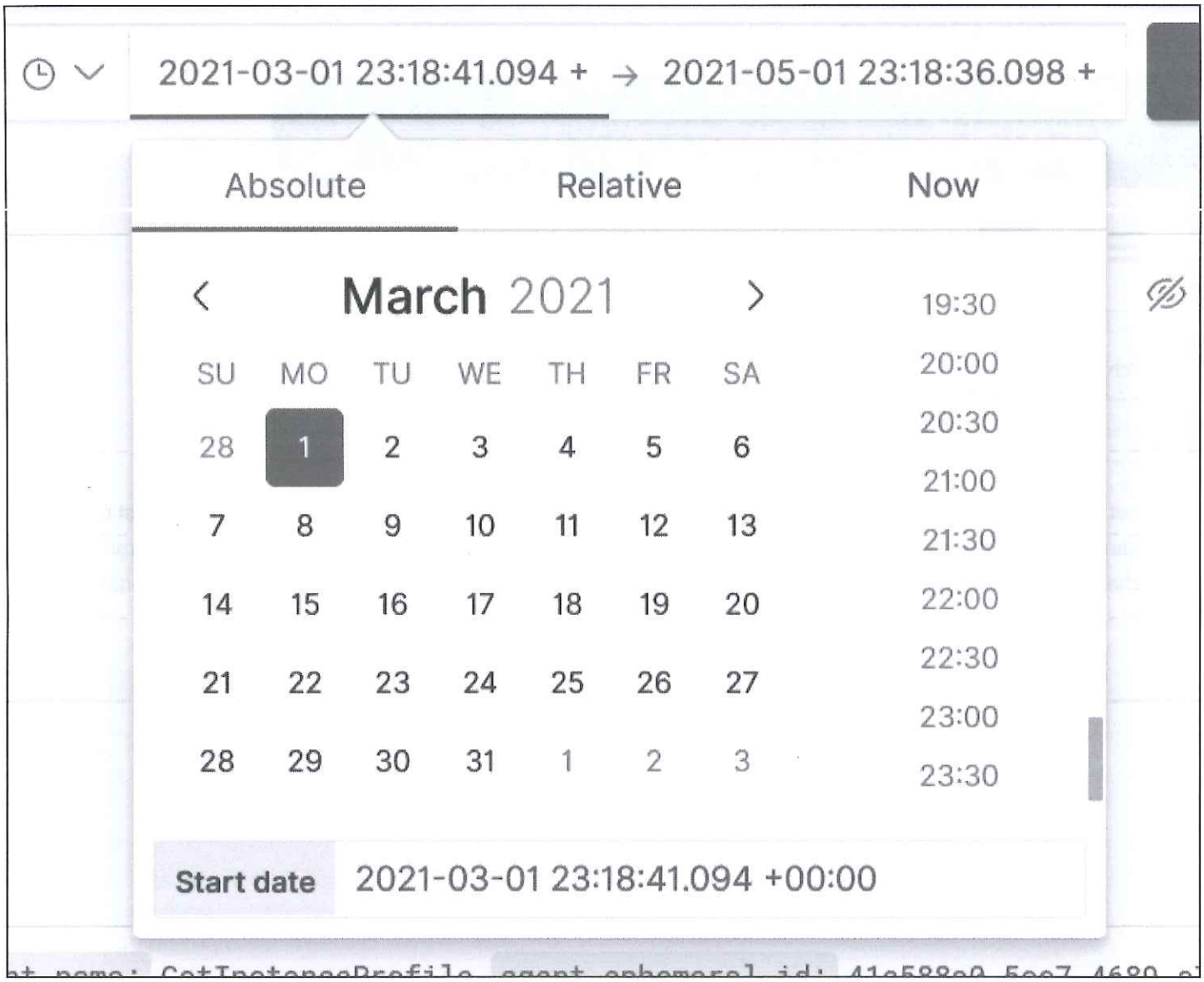
© 2021 Pierre Lidome, David Cowen, and Josh Lemon
https://t.me/learningnets
Technet24

```
event_source: iam.amazonaws.com
```

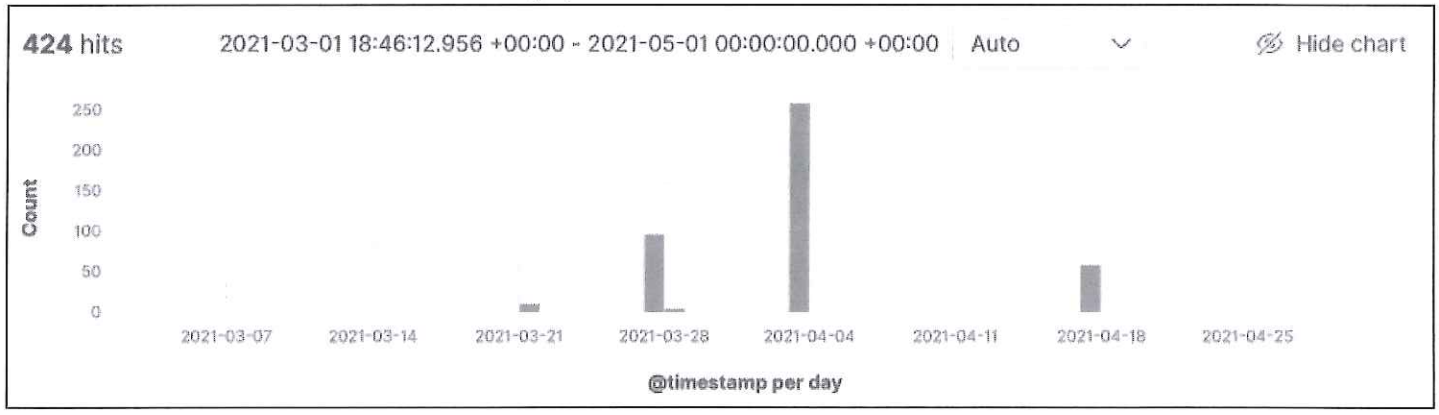


Now that we've selected the right index we need to set the time frame we want to examine. Pymtech IT staff let us know that strange things started happening after March 1, 2021 and before May 1, 2021. Let's set that as our time frame by using the date filter box on the upper right just like you did in the lab 1.2. It should look like the following screenshot:

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

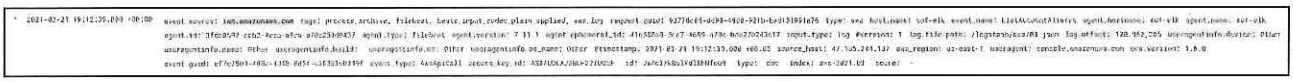


You should now have 424 events and a time graph that looks like the one below.



Let's start be focusing on the events on 3/21/21 which seems to the beginning. Let's take a look at the first record.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



What is the Source IP of this entry?

Look for field named source_host

47.185.244.137

How did the access occur?

Look for field named useragent

The AWS Console

What type of event was this?

Look for field named event_type

An API Call

Whose API key was used?

Look for the ARN field

arn:aws:iam::305681518678:root

When you click on items within the web console they are recorded as API calls because the website is making API calls on your behalf.

Look through the records, do you see any sign of how the session was authenticated?

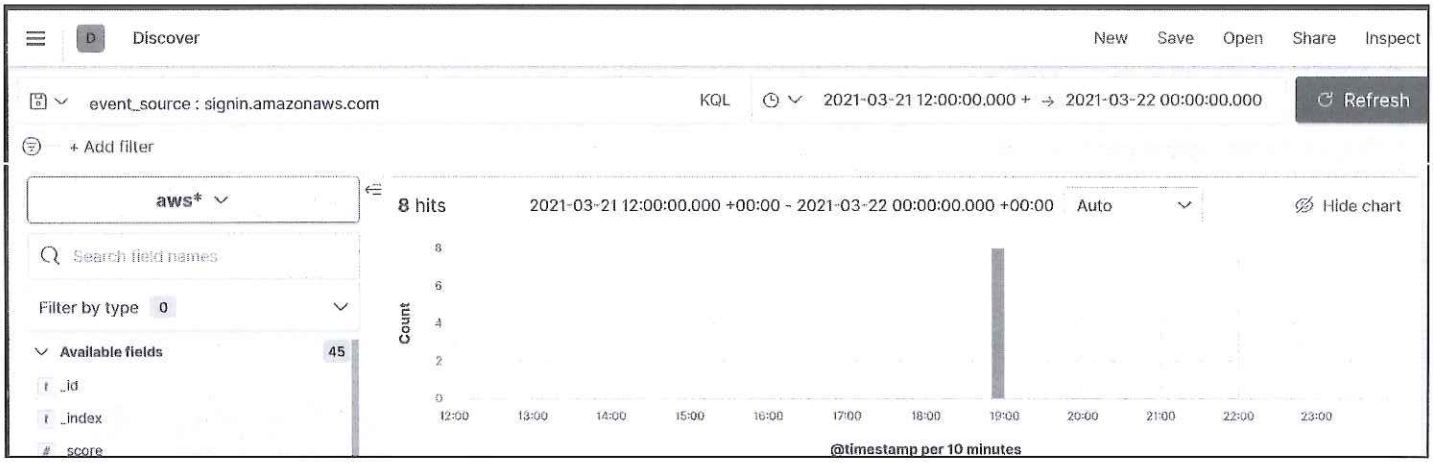
Change the event_source filter to signin.amazonaws.com

- *IAM records record IAM related API calls*
- *The Signin event source records logins*

After you change your event_source filter but leave the time filter in place your view should look like this:

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

```
event_source: signin.amazonaws.com
```



Take a look at the 8 events generated that day and answer the following questions:

How did the user authenticate to AWS (Console, API or IAM user)

Look at the field event_name

ConsoleLogin means logged in at the web console

What operating system was the user using?

Look at the field useragentinfo.os

Windows

What version of the operating system was the user using?

Look at the field useragent

Windows 10

What browser was the user using?

Look at the field useragentinfo.name

Firefox

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

What version of the browser was the user using?

Look at the field useragent

Firefox 86

How else could you tell that this was a Console Login?

Look at the field event_Type

AWSConsoleSignin

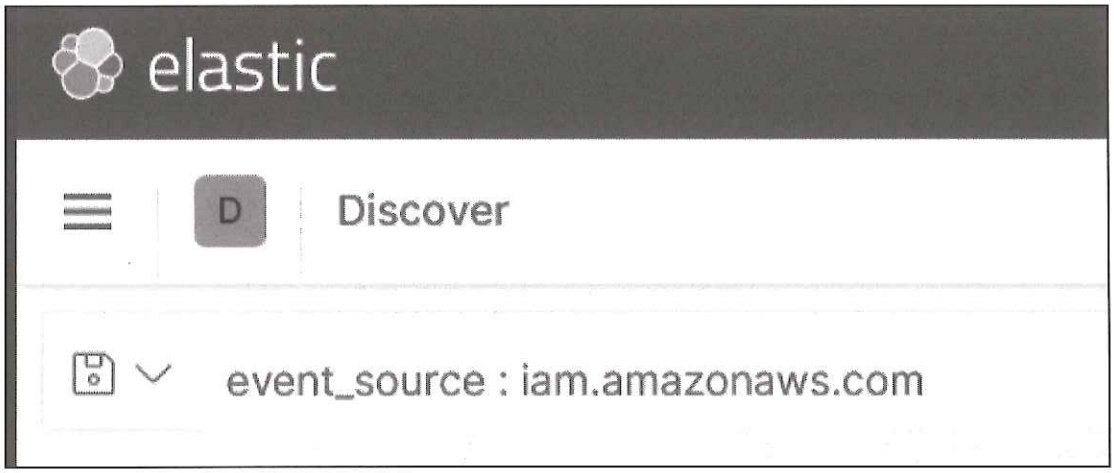
On what other days did logins occur?

Change your time filter to 3/1/21-5/1/21

3/27/21, 4/3/21, 4/17/21

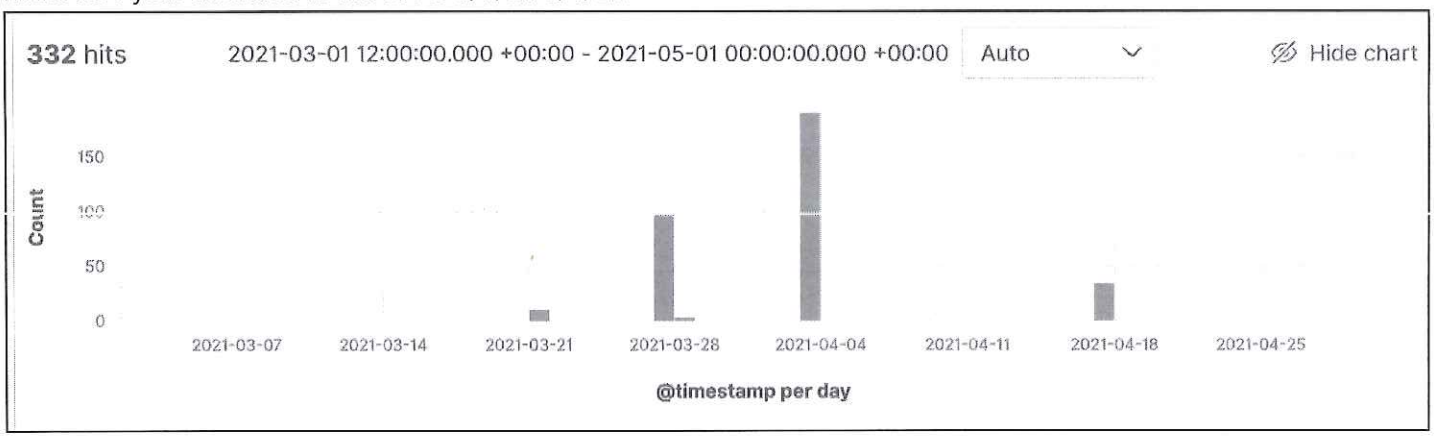
Change your filter back to iam.amazonaws.com

```
event_source : iam.amazonaws.com
```



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Make sure your date filter is still set to 3/1/21-5/1/21.



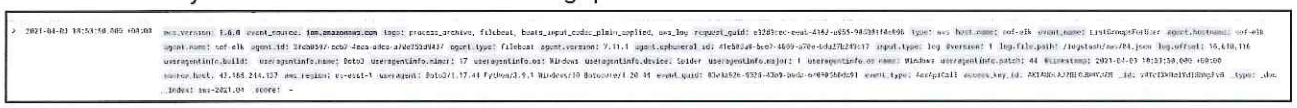
Is there any day that looks more interesting than another?

Look at the counts per day

4/3/21 has a large spike of event

Click on the day with the large amount of activity by clicking on it's green histogram bar.

Look at the entry below and answer the following questions.



What kind of access was this (Console/API/Assumed Role)?

Look at the field event_type

AwsApiCall

Did this access originate from the console?

Look at the field useragent

No it was the AWS Boto3 API library for windows

What API Key was used to make this access?

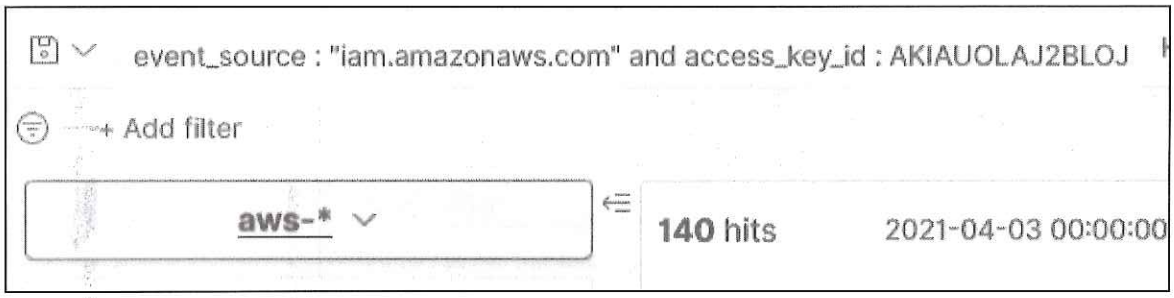
https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Look at the field access_key_id

AKIAUOLAJ2BLOJUMYJZM

Add a filter to your view to focus just on the API key you found in the last quesiton and you should get 140 hits on 4/3/21.

```
event_source : "iam.amazonaws.com" and access_key_id: AKIAUOLAJ2BLOJUMYJZM
```



Read through the event_name on 4/3/21 and answer the following questions:

What was the first operation taken with the API?

Look at the field event_name

ListRoles

How long did the access key run commands against the API on this day?

Look at first and last timestamp

18:36 - 18:53 17 Minutes

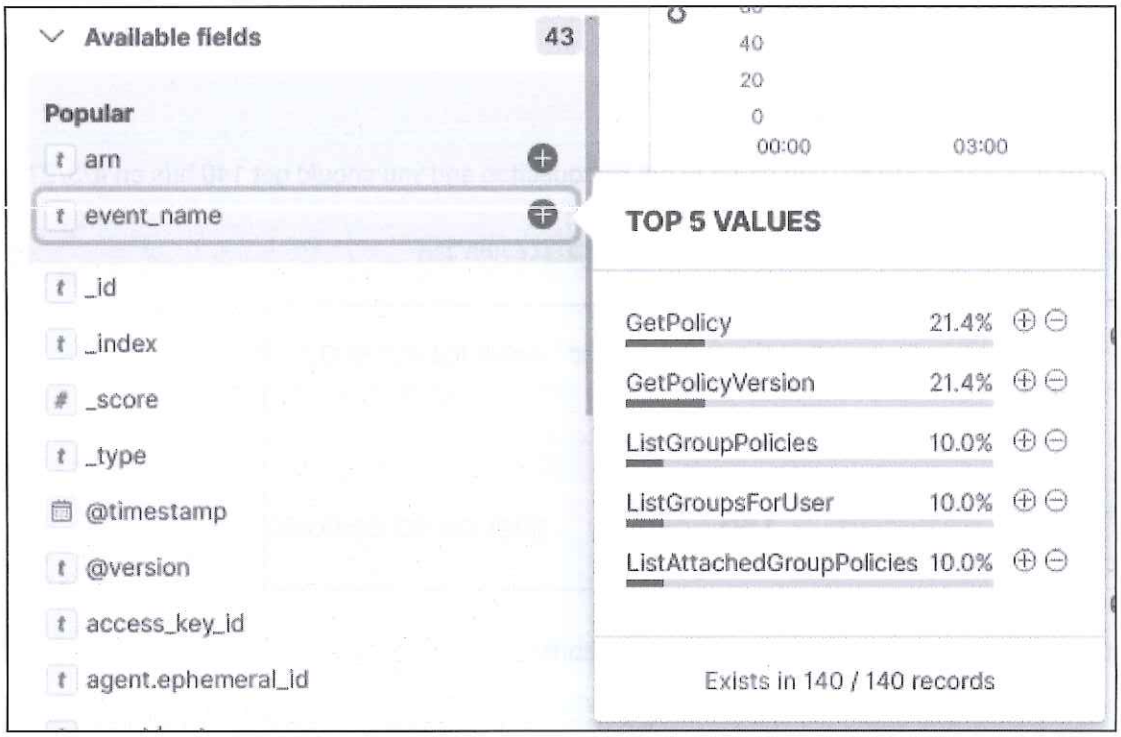
Whose API key was used to do this?

Look at the ARN field

arn:aws:iam::305681518678:user/hpym

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Click on the field event_name on the left hand side of the window, it will show you the top 5 requested events.



With the facts on hand what appears to happening here?

The API key was used to probe users group memberships and policies

If an attacker were to get ahold of an API key for your organization this would be activity could expect to see. We've talked to Hank and from what he remembers he was doing some security testing, we may be ok for now.

```
!!! warning
    Make sure to clear your filters before moving on to the next lab
```

Key Takeaways

- You can now determine the differnce between a Console login and an API authentication
- Profiling account accesses and their origin is important when determining if credentials have been compromised
- Always look for new keys being created or accounts/API Keys logging in from new IPs

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Lab 2.2: Finding Rogue VMs

Objectives

- Learn how to analyze ec2 CloudTrail logs
- Learn how to find evidence of new Virtual Machines being created
- Learn how to analyze the configuration of the system created

Background

In the prior lab we noted that an API key appears to have been probing for roles within our tenant. The IAM and Signin event sources had a small number of log entries. Switching to the EC2 log we find a larger set to analyze.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM

Load Data

The data for Lab 2.1 has the logs you need for this lab.

Lab Content

1. Make sure you date filter is set to 3/1/21 - 5/1/21
2. Change your filter to focus on ec2 events by filtering your event_source for ec2.amazonaws.com as show below:

```
event_source:"ec2.amazonaws.com"
```

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon



3. You now have 74,916 log entries to look at. That is likely to much for an analyst to start with, so let's focus on the facts we know. The API activity occurred don 4/3/21 what ec2 events happened on that day. Change your date filter to 4/2/21-4/4/21.

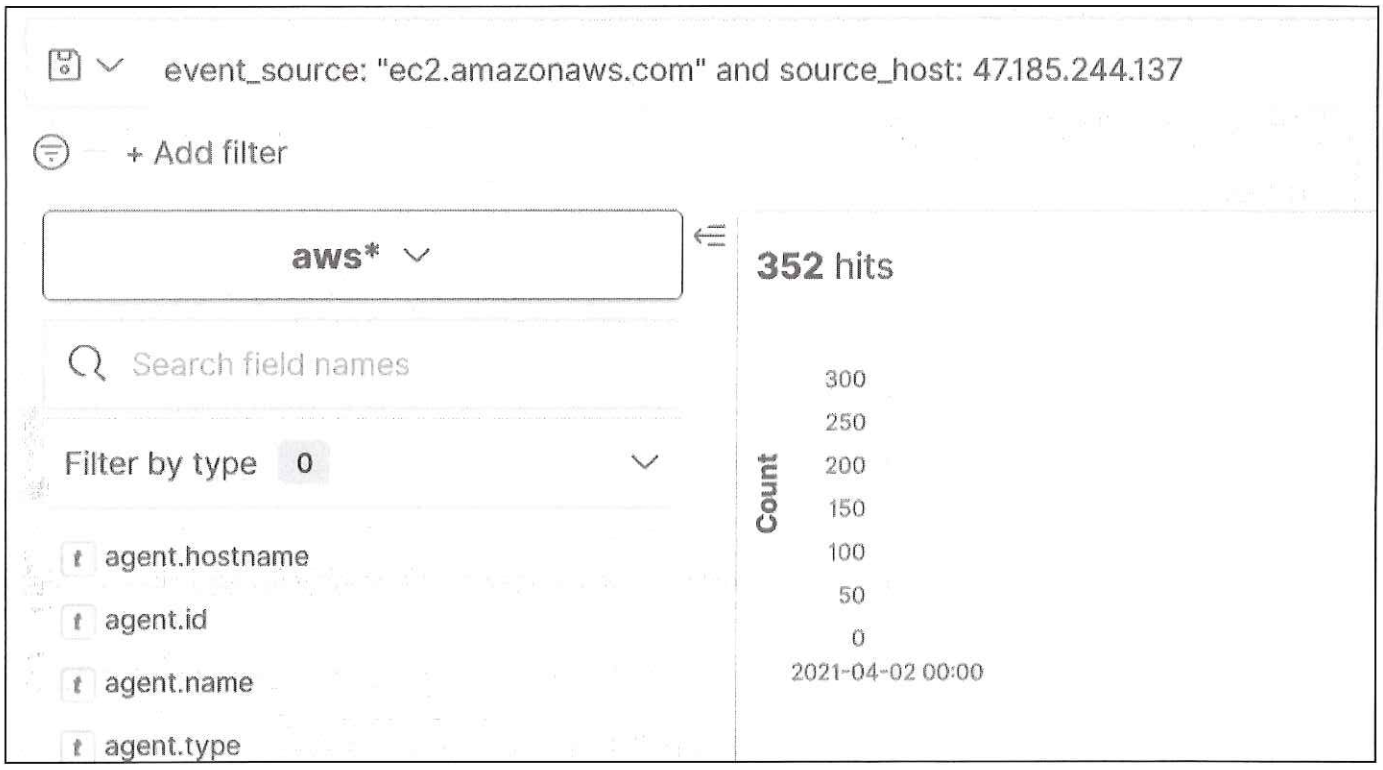
4. It looks like our company is using an auto scaling solution called AWS Elastic Bean Stalk.

Time ^	_source
2021-03-01 00:00:17.000 +00:00	event_source: ec2.amazonaws.com host.name: sof-elk event_name: DescribeInstanceStatus request_guid: a4b3f1e0-f43c-4449-b84a-ec8986b2ea2d @version: 1 useragentinfo.os_name: Other useragentinfo.build: useragentinfo.os: Other useragentinfo.name: Other useragentinfo.device: Other source_host: autoscaling.amazonaws.com @timestamp: 2021-03-01 00:00:17.000 +00:00 tags: process_archive, filebeat, beats_input_codec_plain_applied, aws_log

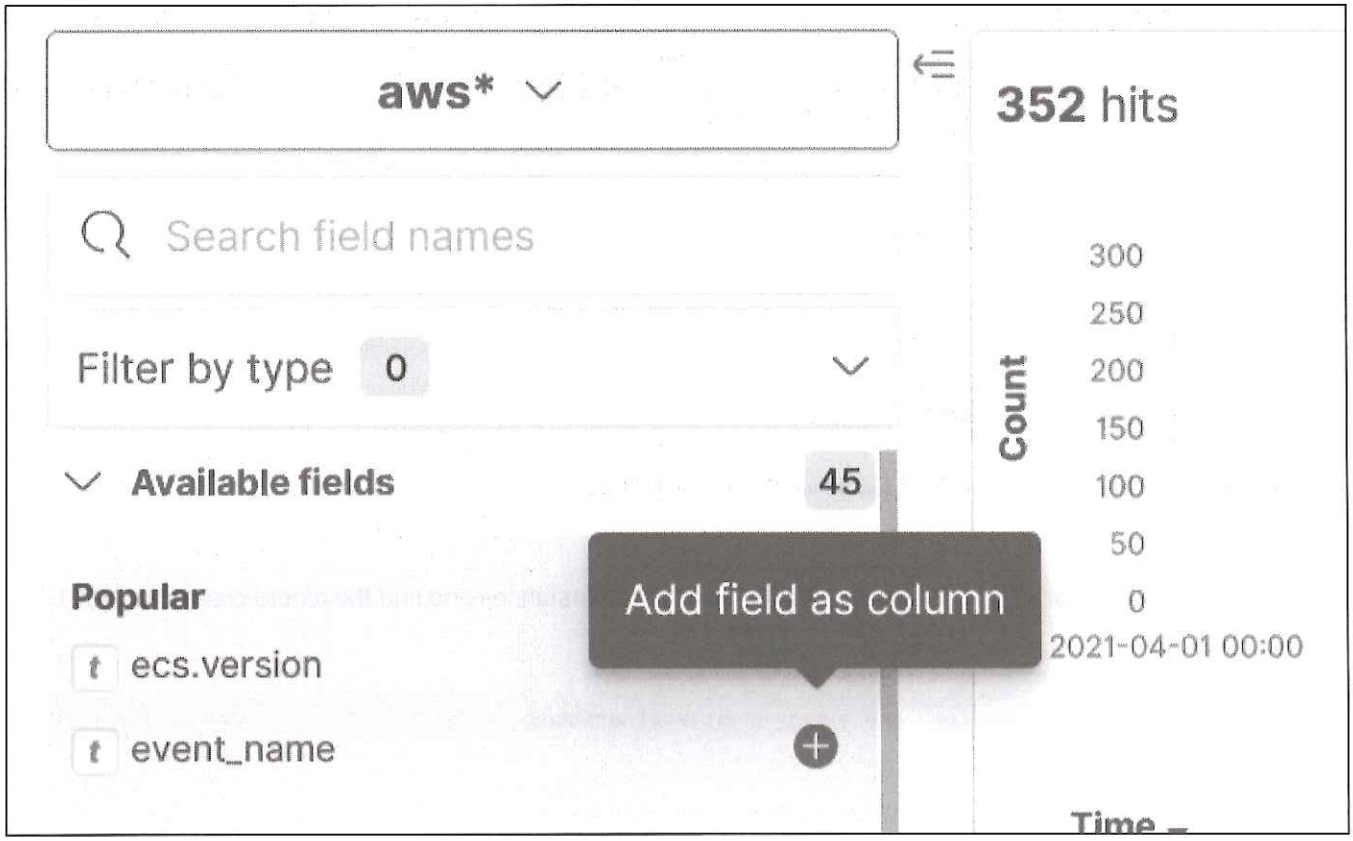
5. Let's filter out the Elastic Beanstalk entries to see if any new virtual machines were created on our day of interest. We will do this by filtering down the source of the request to the IP address we noted in the prior lab, 47.185.244.137.

```
event_source: "ec2.amazonaws.com" and source_host: 47.185.244.137
```


https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



We now have 352 events, a much more managable number. Let's now look for what events occured. Click on event_name on the left hand side and click the plus sign.



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

What was the last event to be executed?

Look at the event_name

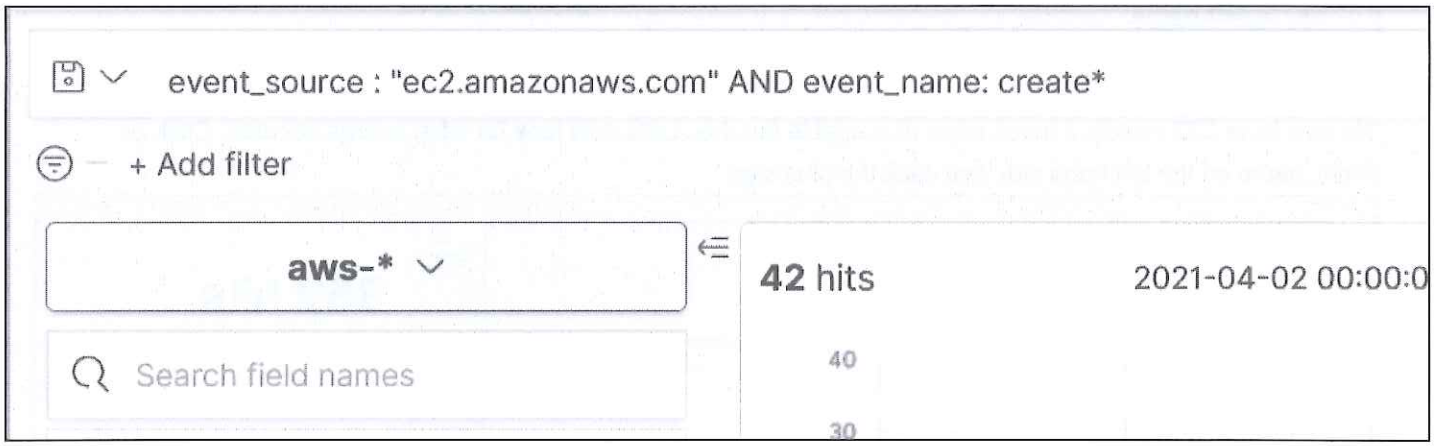
RunInstances

What does RunInstances mean?

Look at your slides

RunInstances is what is logged when an EC2 VM is started

Looks like someone started a new EC2 instance, let's determine what was created. Change your filter to look for all event_name entries that start with create.



What was created?

Look for the unique event names

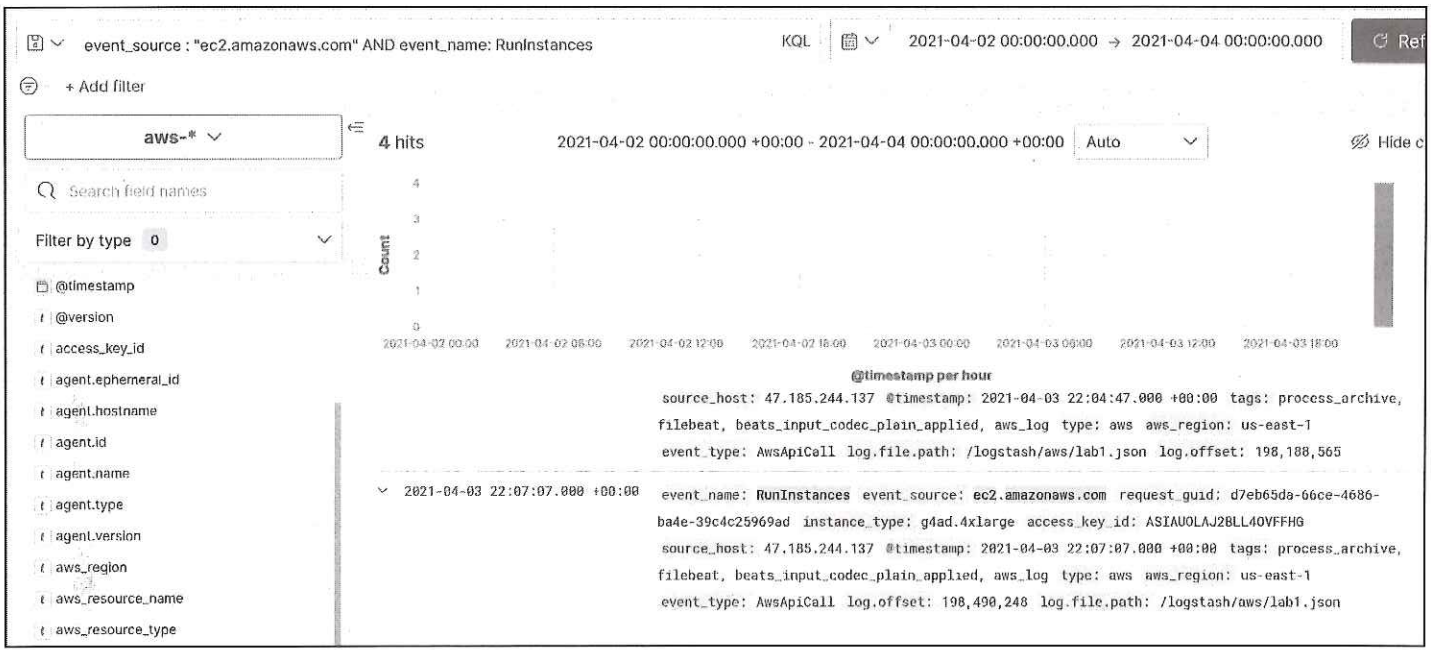
CreateTags, CreateNetworkInterface, CreateKeyPair, Create SecurityGroup

Change your filter to look for all event_name entries that match RunInstances and find the record created on 2021-04-03 22:07:07.000

```
event_source: "ec2.amazonaws.com" AND event_name: RunInstances
```


https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24



What is the imageID of the EC2 VM?

Look at the field image_id

ami-037ce2fddcbfdbf52

What kind of VM was it?

??? tip "Look at the instance_type field" ***g4ad.4xlarge***

What was the name of the ssh key pair generated?

Look at the field key_name

NewEC2

What account was used to create the EC2 VM?

Look at the field arn

root

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

In talking to the admins this was a false positive. Our root account is not compromised, yet!

```
!!! warning
    Make sure to clear your filters before moving on to the next lab
```

Key Takeaways

- You can now filter down to EC2 logs in Cloudtrail
- You now know how to find and interpret actions being taken against EC2 hosts

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Lab 2.3: VPC Flow Logs

Objectives

- Understand how to read AWS Flow Logs
- Learn how to profile network traffic
- Find possible exfiltration of data

Background

Pymtech Labs got an alert from the SOC, it looks like between 5/2/21 - 5/3/21 a large data transfer was spotted going out of our new AWS network. We need you to look at the netflow from our AWS environment to see if you can find out what happened.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the AWS parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

The AWS Cloudtrail logs for this lab have already been exported from our S3 Bucket. We've tried to make the loading process as close to what you will do in the real world. As such with how AWS stores data there is a two step loab poccess.

The CloudTrail Logs for lab-2.3 have been saved into `/home/elk_user/lab-2.3_source_evidence.zip` .

1. Log on to the SOF-ELK VM with the credentials
    - Username: ***elk_user***
    - Password: ***forensics***

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

You may log on to the console, however it's recommended to log in via SSH.

2. Extract the all the files from the ZIP file for ingestion into Kibana above with the following commands:

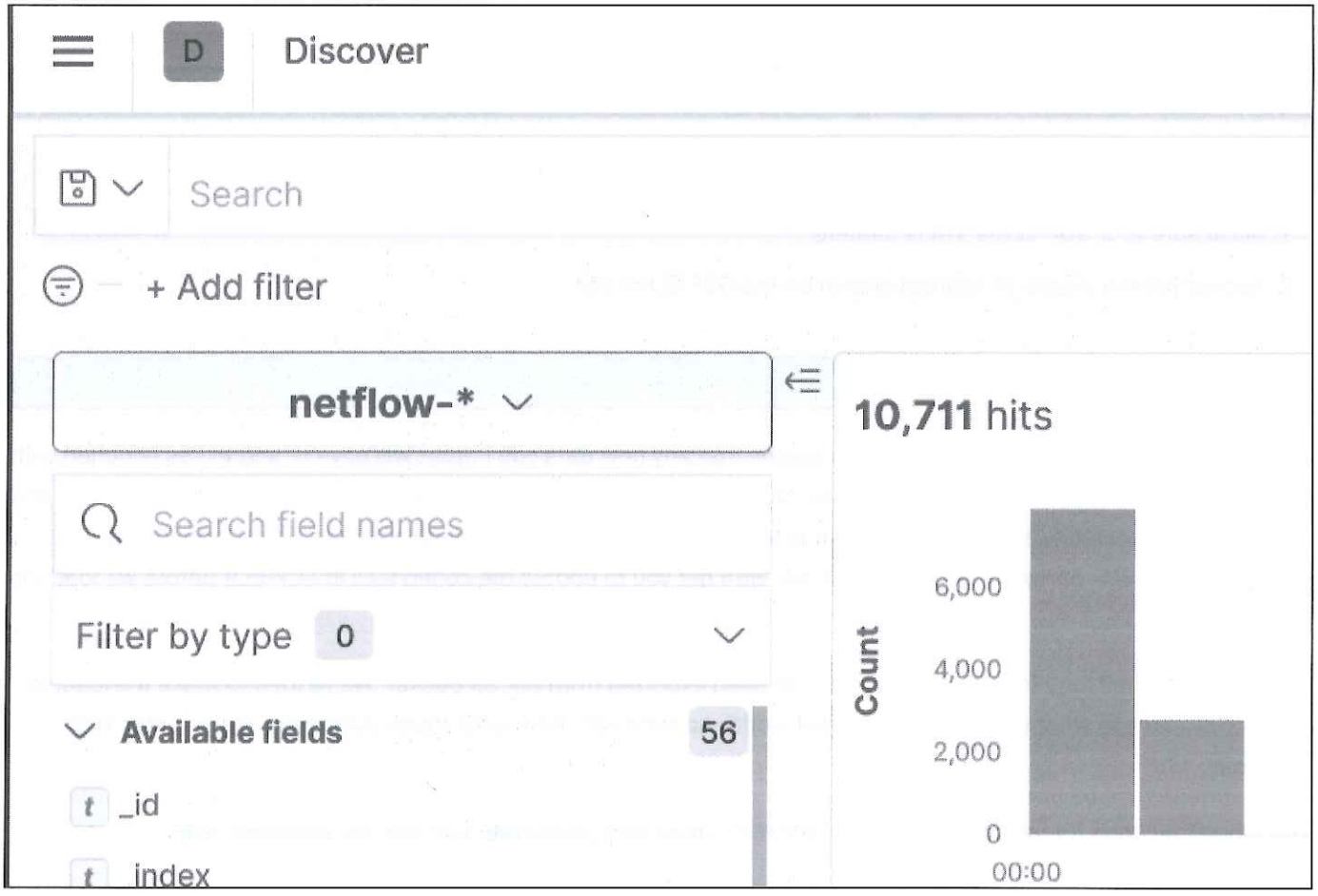
```
cd ~
unzip -q lab-2.3_source_evidence.zip  -d /logstash/nfarch
```

> **Warning**
>
> Do not run this command more than once!

3. Wait 2 minutes for the data to be processed. Once it is complete the data will be available in the `netflow-*` index.

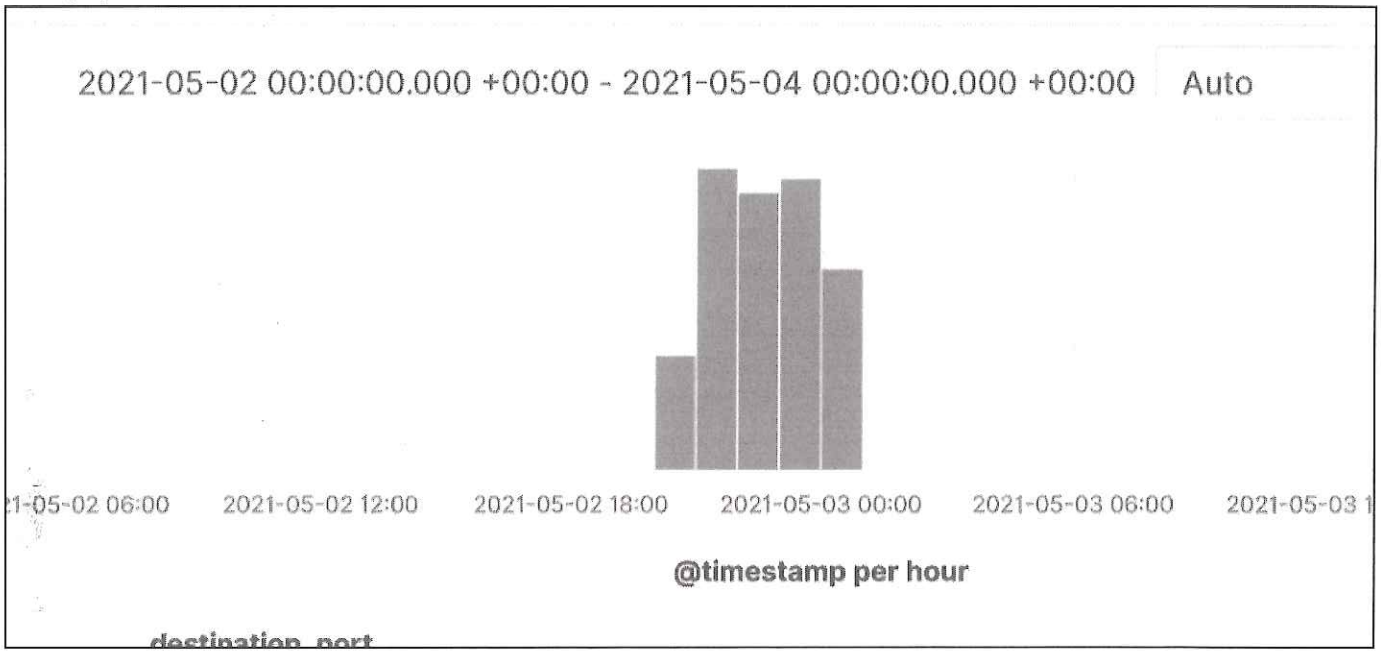
Lab Content

1. On the discover tab select the Netflow index



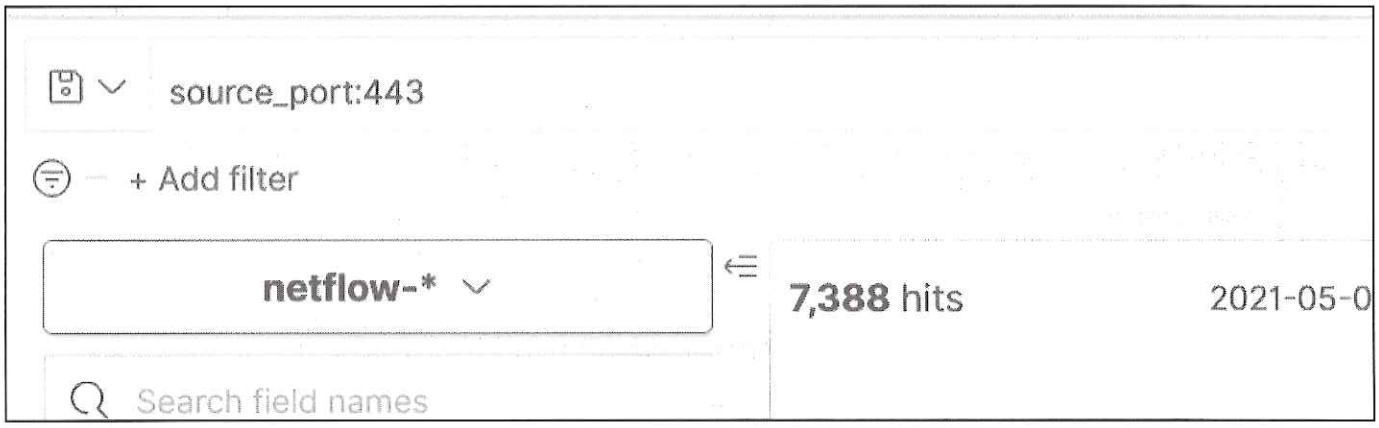
© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

2. Change your time frame to 5/2/21 to 5/4/21



3. Add a filter for source_port:443

```
source_port:443
```



4. Look for the record that occured on "2021-05-03 00:40:57.000Z' and answer the following questions:

What the source of the traffic?

Look at the source_ip field

54.224.26.45

What was the destination of the traffic?

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Look at the destination_ip field

***192.168.52.168 ***

How long did the session last?

Subtract flow_end from flow_start

Look at flow_duration

6 seconds

How much data was transmitted and received?

Look at total_bytes

34,999

Was there is a download or an upload?

Look at in_bytes vs out_bytes

out_bytes is 0, in bytes is 34,999

It is a download

What organization owns the ip that hosted the data downloaded?

Make sure you've done lab 0 and imported the MaxMind database

Look at the source_geo.as_org

Amazon

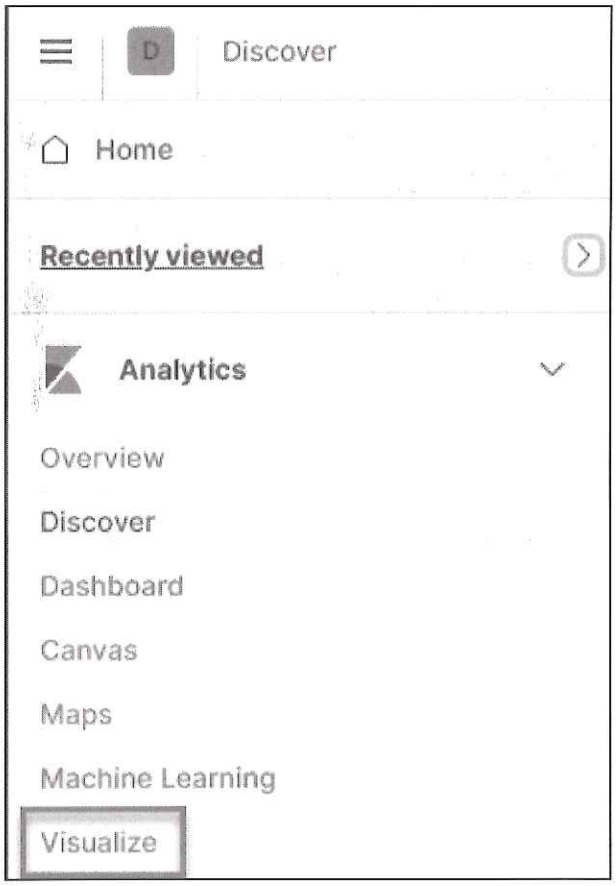
What country is the ip hosted in?

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

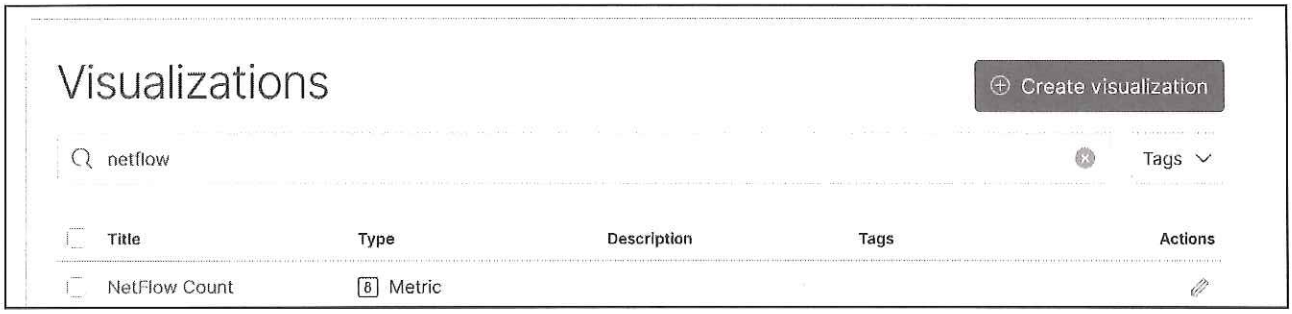
Technet24

> **Look at source_geo.country_name**
>
> ***United States***

4. Now that you know how to read a log, let's change our view to look for the alleged data theft. Click on the menu button and then Visualize.



5. Filter for netflow visualizations



6. Click on 'Netflow Statistics by Destination AS'



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

7. You should now see a view similar to what is below:

Export

Exporter	Volume	Packets	Flows
ASN24940: Hetzner Online GmbH	17.4GB	12,480,734	20
ASN: Not Available	850MB	2,534,154	48,218
ASN16509: AMAZON-02	13.4MB	84,740	2,840
ASN14618: AMAZON-AES	13MB	100,598	1,909
ASN199790: IP Telecom Bulgaria	2MB	48,261	11,044
ASN18403: The Corporation for Financing & Promoting Techno...	341KB	1,507	168
ASN14061: DIGITALOCEAN-ASN	169.5KB	935	229

Which Organization has the largest amount of data transfer?

The top row has the name

Hetzner Online GmbH with 17.4GB

8. Go back to the visualize page and filter for netflow again. This time choose "Netflow Statistics by Destinaion IP" you should see something similar to the below:

Export

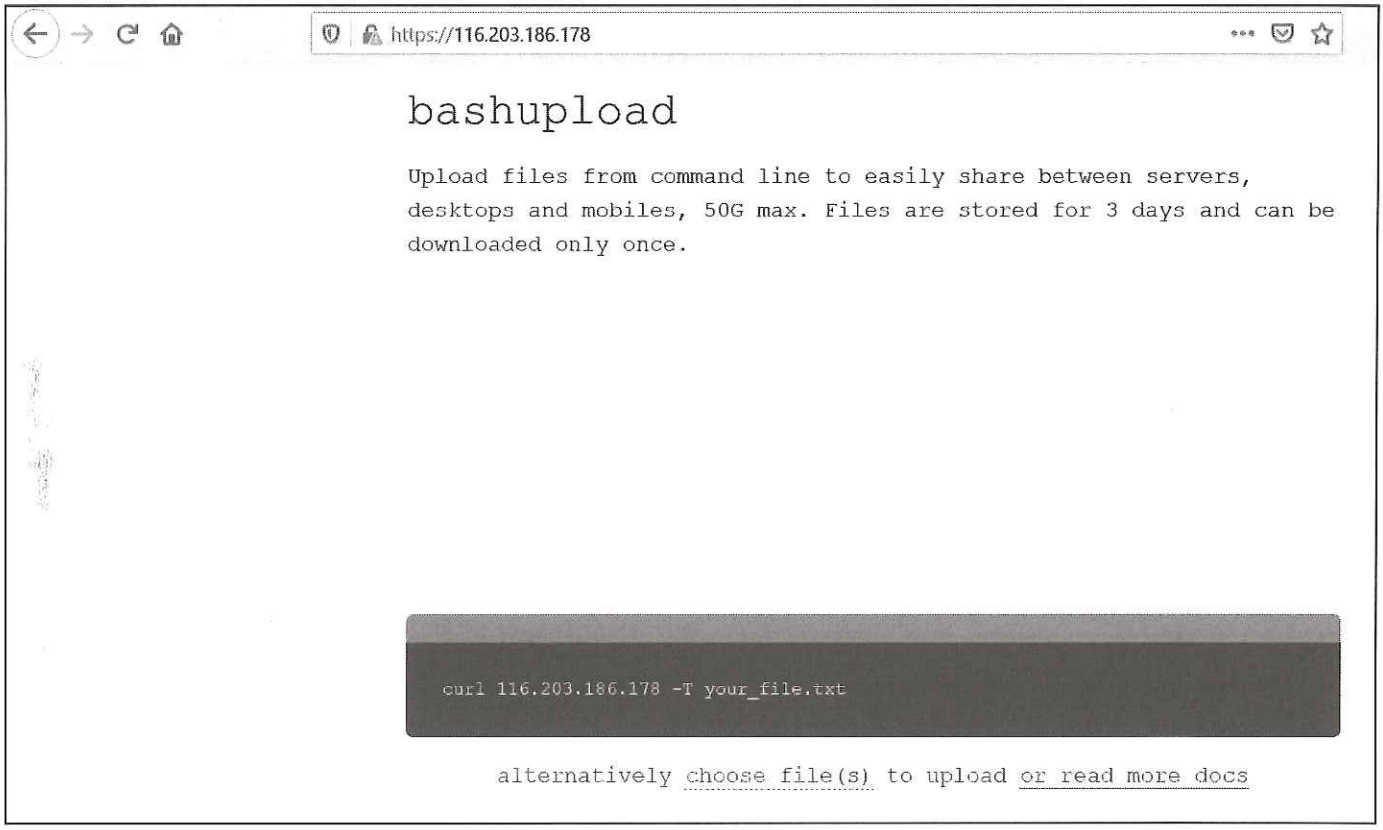
Destination IP	Volume	Packets	Flows
116.203.186.178	17.4GB	12,480,684	12
192.168.52.168	276.6MB	271,089	5,893
192.168.29.80	238.4MB	241,463	5,936
192.168.25.115	204.9MB	209,469	6,181

Which ip corresponded to the traffic we saw ranked by org in the previous step?

116.203.186.178

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

9. Going to that IP shows a service called bashupload.com



What does bashupload allow for?

Uploading files from the command line

Warning

Make sure to clear your filters before moving on to the next lab

Key Takeaways

- You've learned how to read an AWS VPC Flow log
- You've learned to determine the difference between an upload and a download
- We've discovered a large amount of data exfiltrated, we should look into this and find out how this happened.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Lab 2.4: S3 Analysis

Objectives

- Learn how to read S3 server access logs
- Determine how a s3 bucket acl gets changed
- Determine who accessed the s3 bucket

Background

Scott had a long frustrating day and set a s3 public to public access to get a data transfer going to an agency. He forgot to make the bucket private after and wants to know if you can determine if anyone downloaded the data from the bucket.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the AWS parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

The AWS Cloudtrail logs for this lab have already been exported from our S3 Bucket. We've tried to make the loading process as close to what you will do in the real world. As such with how AWS stores data there is a two step loab poccess.

The CloudTrail Logs for lab-2.4 have been saved into `/home/elk_user/lab-2.4_source_evidence.zip` .

1. Log on to the SOF-ELK VM with the credentials
    - Username: ***elk_user***
    - Password: ***forensics***

   You may log on to the console, however it's recommended to log in via SSH.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

2. Extract the all the files from the ZIP file above with the following commands:

```
cd ~
unzip -q lab-2.4_source_evidence.zip
```

3. Run the AWS Cloudtrail ingestion script

```
cd ~
aws-awss32sof-elk.py -r ./lab2.4_source_evidence -w /logstash/awss3/lab4.csv
```

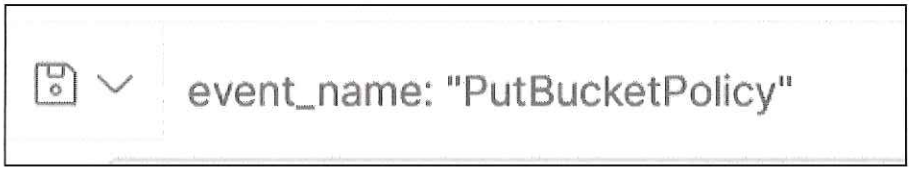
> ⚠ **Warning**
>
> Do not run this command more than once!

4. Wait 2 minutes for the data to be processed. Once it is complete the data will be available in the `awss3-*` index.

Lab Content

1. Go to the Discover screen
2. Select the AWS Index
3. Set your date filter to 4/30/21 - 5/2/21 Scott thinks he made the changes then.
4. Set a filter for the event_name PutBucketPolicy

```
event_name: "PutBucketPolicy"
```



What day did scott change the permissions on the bucket?

2021-05-01

What bucket was affected?

> **Look at the aws_resource_name field**

arn:aws:s3:::pymresearch

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

> ⚠ **Warning**
>
> Make sure to clear your filters before moving on to the next lab

Key Takeaways

- You now can determine when a bucket policy was modified

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Lab 2.5: Tracking Lateral Movement

Objectives

- Learn what AWS services attackers focus on to expand their access
- Learn what AWS services can be leveraged for latermal movement
- Determine the impact of a single compromised account

Background

From the AWS VPC Flow logs lab we know that a host was compromised and data was exfiltrated out. In many instances this is accomplished when API keys are stolen and an attacker looks to move laterally within the cloud tenant. We need you to determine where this attack came from and what was accessed.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the AWS parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

The AWS Cloudtrail logs for this lab have already been exported from our S3 Bucket. We've tried to make the loading process as close to what you will do in the real world. As such with how AWS stores data there is a two step loab poccess.

The CloudTrail Logs for lab-2.5 have been saved into `/home/elk_user/lab-2.5_source_evidence.zip` .

1. Log on to the SOF-ELK VM with the credentials
    - Username: ***elk_user***
    - Password: ***forensics***

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

You may log on to the console, however it's recommended to log in via SSH.

2. Extract the all the files from the ZIP file above with the following commands:

```
cd ~
unzip -q lab-2.5_source_evidence.zip
```

3. Run the AWS Cloudtrail ingestion script

```
cd ~
aws-cloudtrail2sof-elk.py -r ./lab-2.5_source_evidence -w /logstash/aws/lab5.json
```

> ⚠ **Warning**
>
> Do not run this command more than once!

4. Wait 2 minutes for the data to be processed. Once it is complete the data will be available in the `aws-*` index.

Lab Content

1. On the discover screen select the AWS Index
2. Make sure your date range is set to 4/30/2021 - 5/3/2021

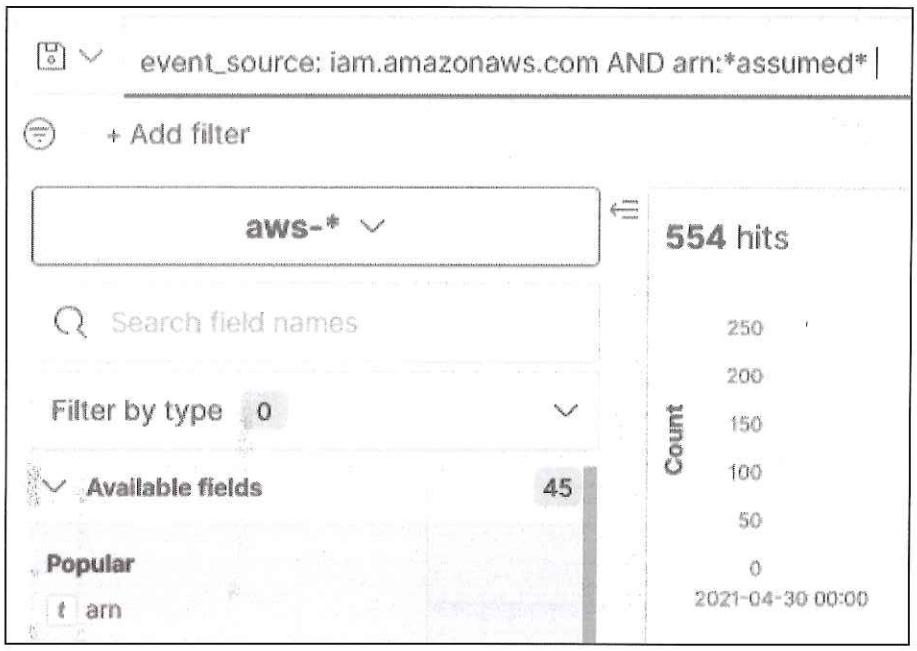
   One of the most common ways that attackers get ahold of keys it to compromise a host and steal it's IAM role. To find out if this happened here let's check our IAM logs for accesses from assumed-roles.

3. Filter for the event_source of iam.amazonaws.com and an assumed role in the ARN

```
event_source: iam.amazonaws.com AND arn:*assumed*
```


https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

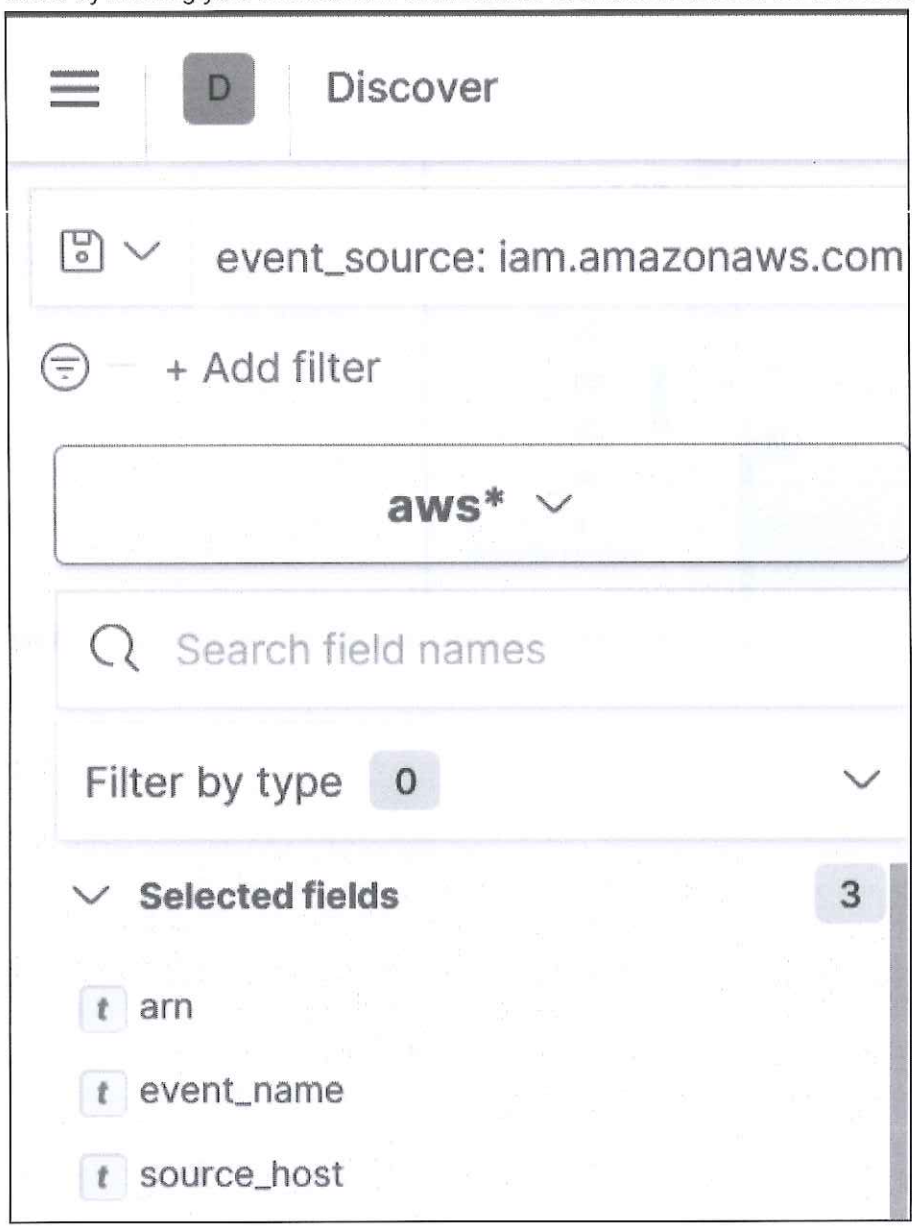
Technet24



Select three fields to focus on what was happening here 'arn, event_name and source_host'. Reminder you can select

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

fields by moving your mouse over them on the available fields list on the left and clicking the plus sign.



4. Scroll down and look for a source_host that isn't from amazon

What host did you find other than Amazon?

Try a filter like "event_source: iam.amazonaws.com AND arn: *assumed* AND NOT source_host: *amazon*

5.62.19.62

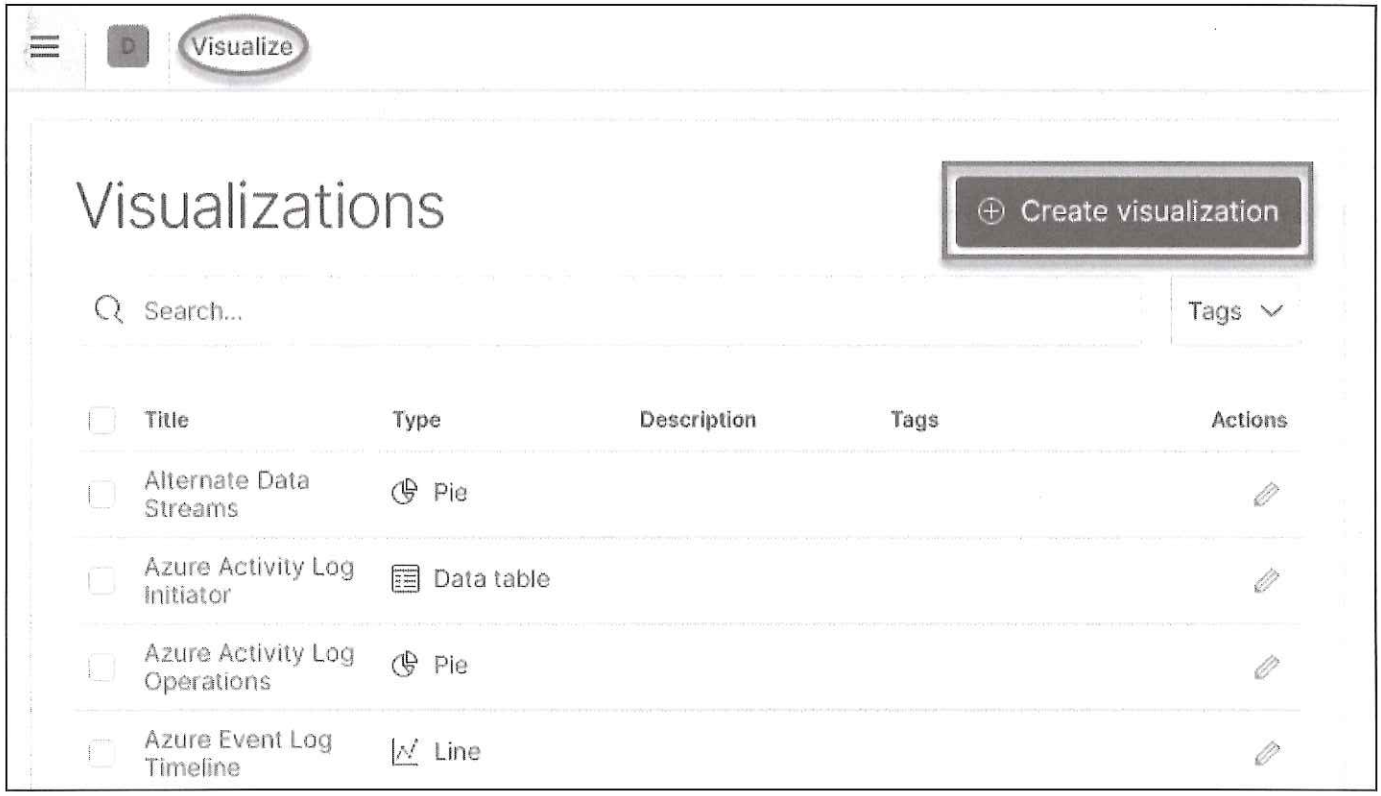
What country does that ip belong to?

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

> **Try a website like https://www.ip2location.com/demo**
>
> *** Russia ***

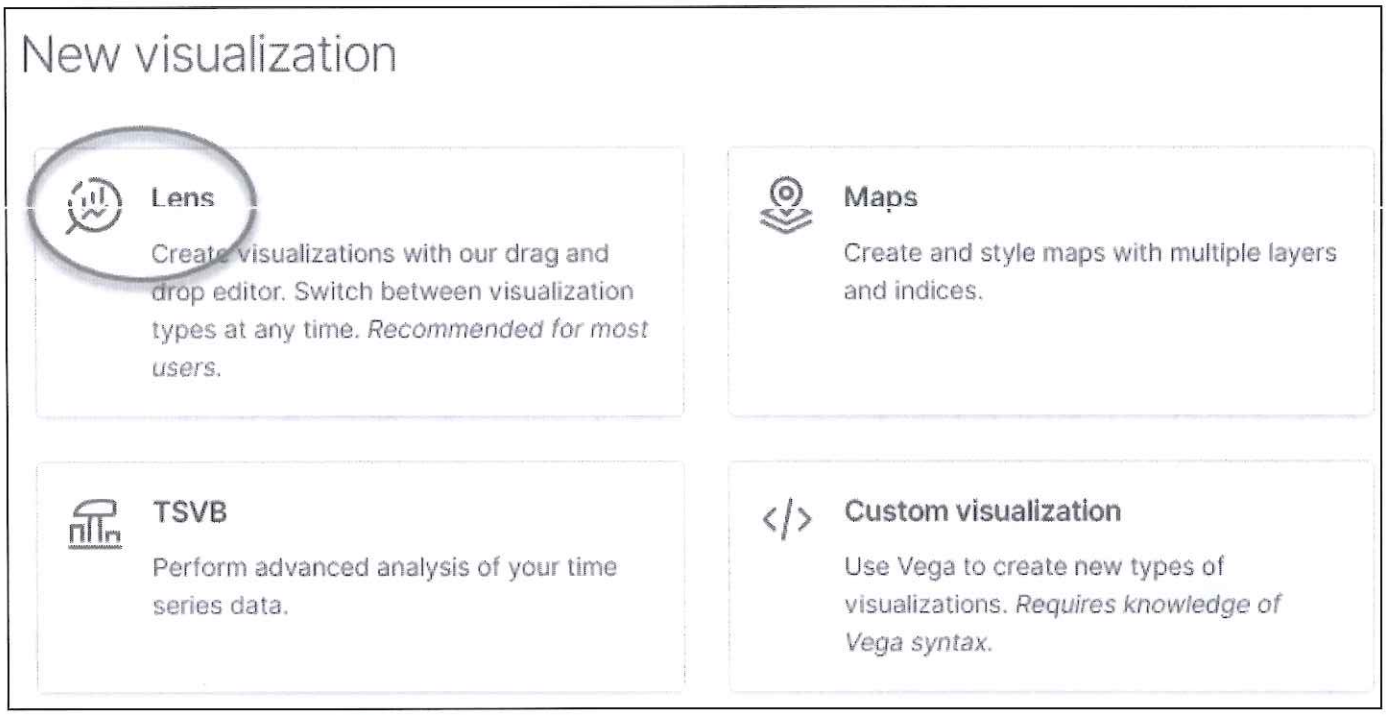
> **What role did the attacker compromise?**
>
> > **Look at the ARN field**
> >
> > ***eks-ctl-dev-cluster***

5. Now that we have an IP let's find out what other Amazon APIs it was accessing. Click on the Visualize screen again, but this time we are going to create a visualization.
6. Click on Create Visualizaton



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

7. Choose the Lens visualization



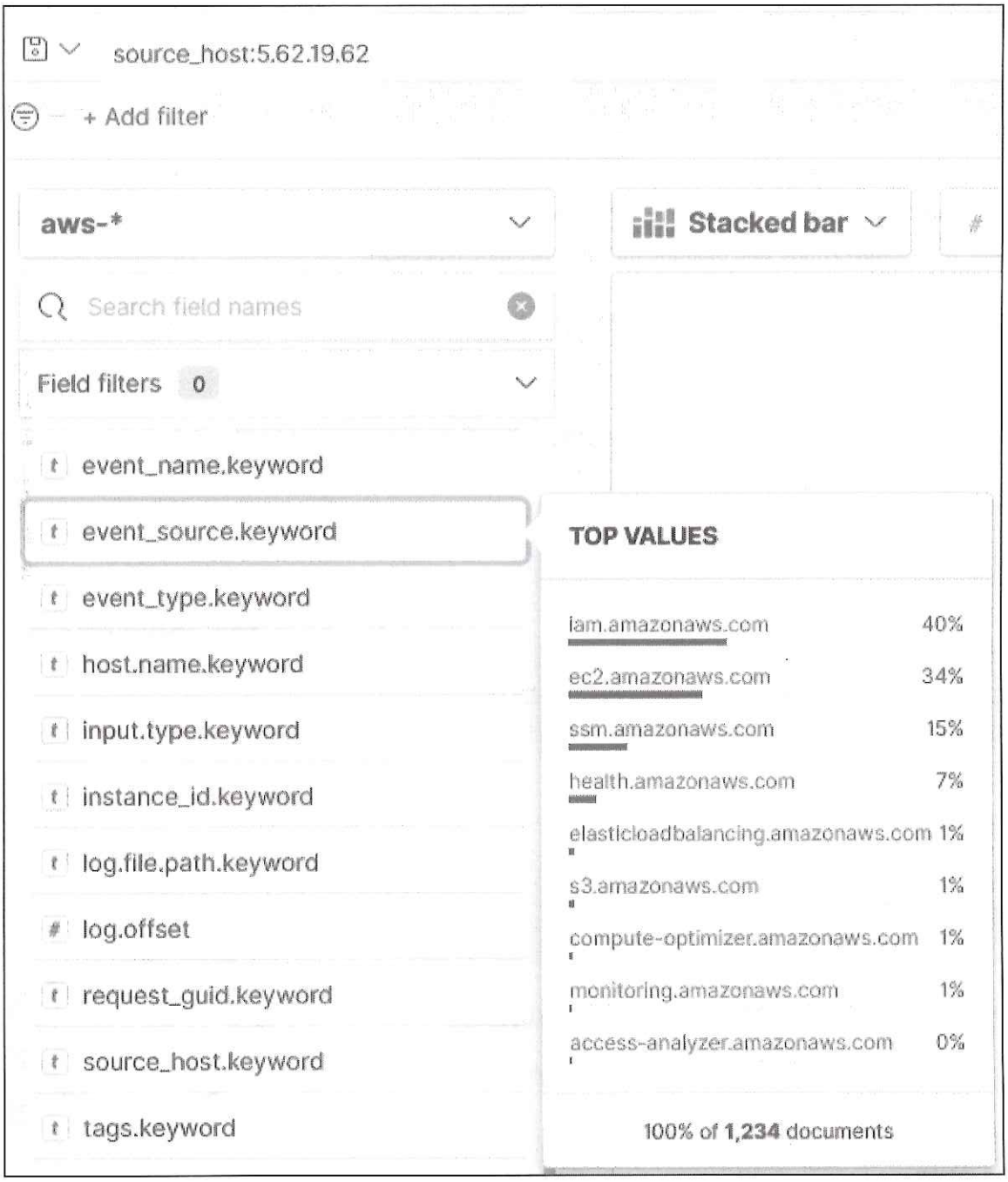
8. Add a filter for our IP to the top and make sure the AWS index is selected

```
source_host:5.62.19.62
```



9. Select the event_source.keyword from the available fields and drag and drop it into the middle frame

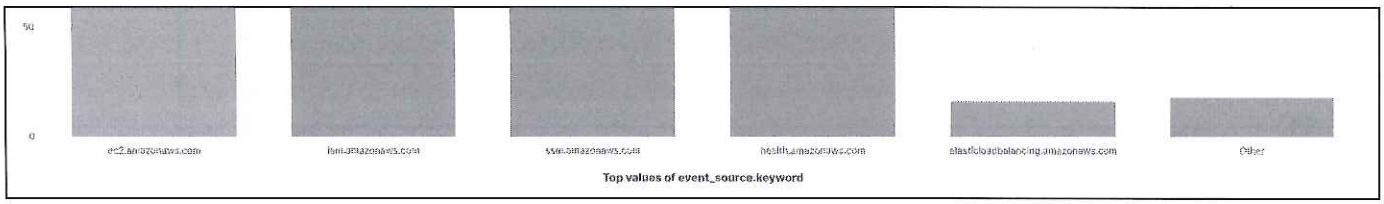
© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



10. You should now see the top event sources (API calls) that our attackers IP is associated with.

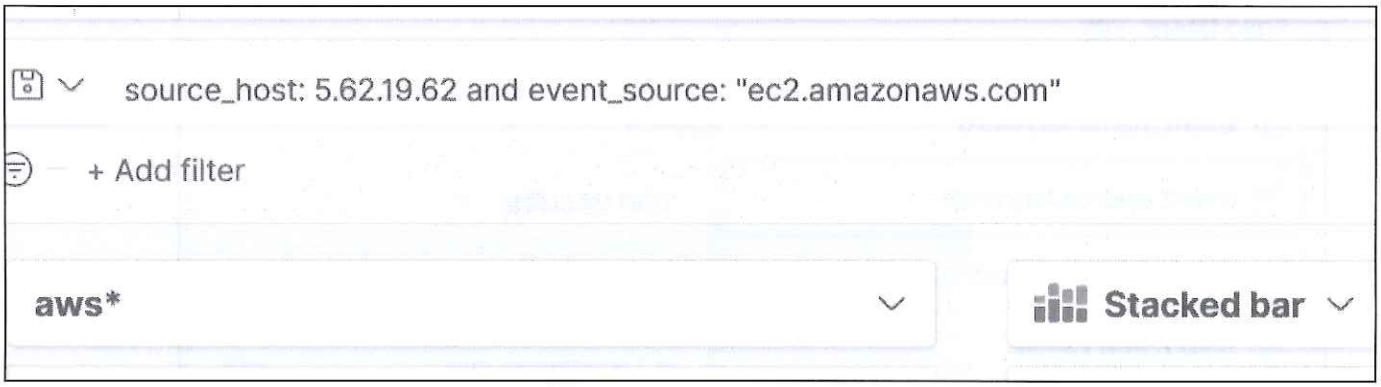
> **What are the top 3 services?**
>
> ***EC2, IAM, SSM***

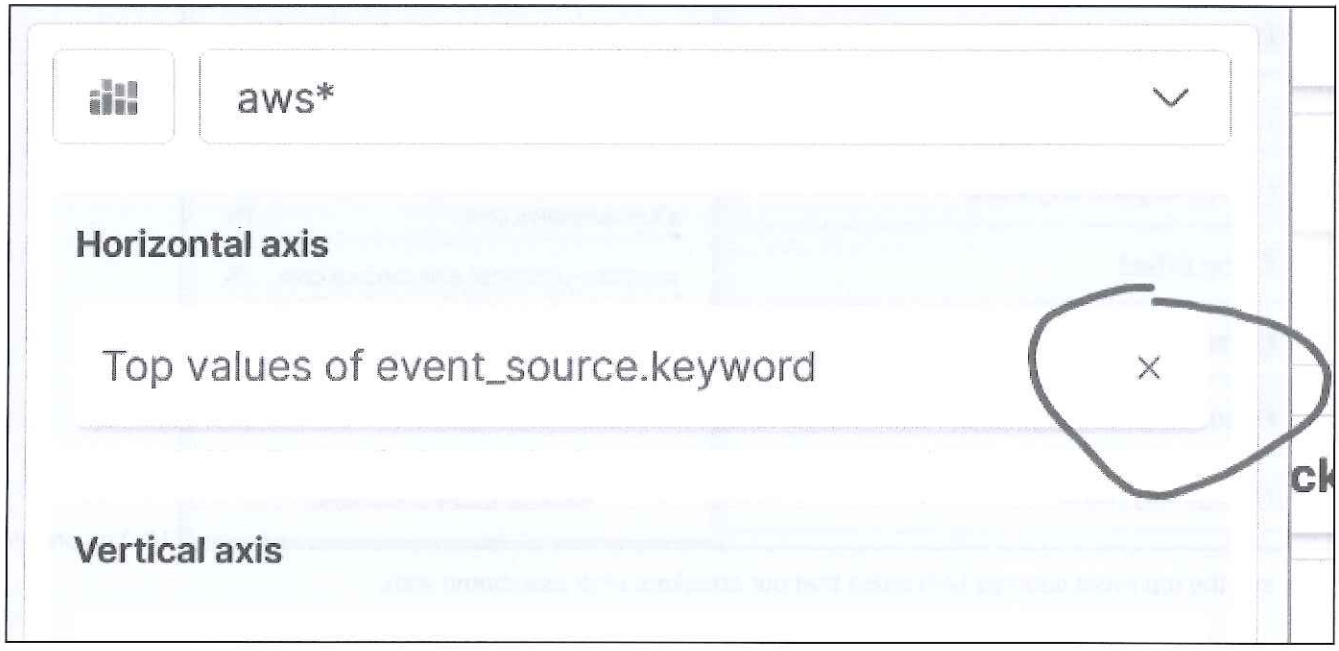
 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



9. Let's check to see what the most called ec2 commands are by changing our filter to source_host: 5.62.19.62 and event_source: "ec2.amazonaws.com" and clearing out the prior field selection.

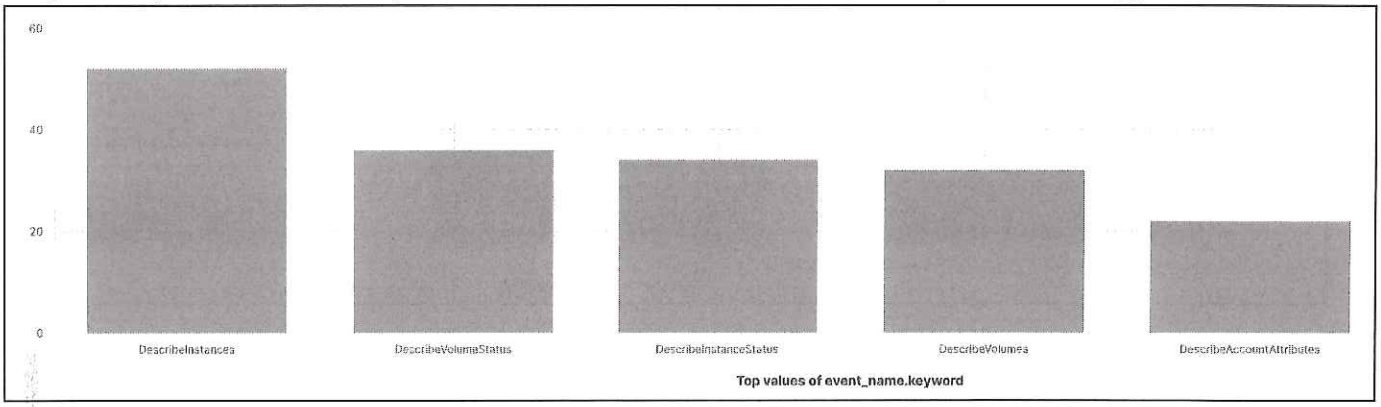
```
source_host:5.62.19.62 and event_source:"ec2.amazonaws.com"
```





© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

10. Drag and drop the event_name.keyword field into the middle screen to find the top API events logged for EC2.



What are the top 3 event names (Not Including Other)?

DescribeInstances, DescribeVolumeStatus, DescribeVolumes

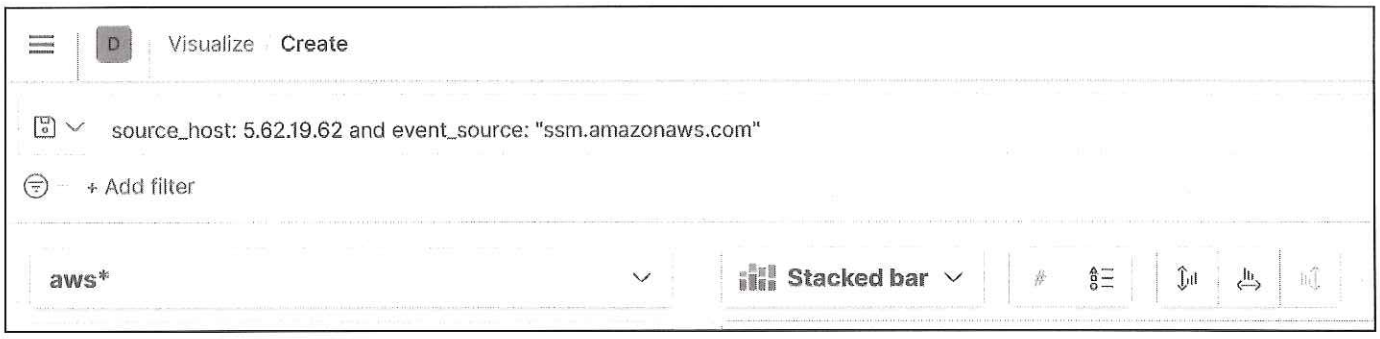
What is the attacker doing?

Describe events will list out resources by type

The attacker is listing out all the EC2 VMs we have in our tenant

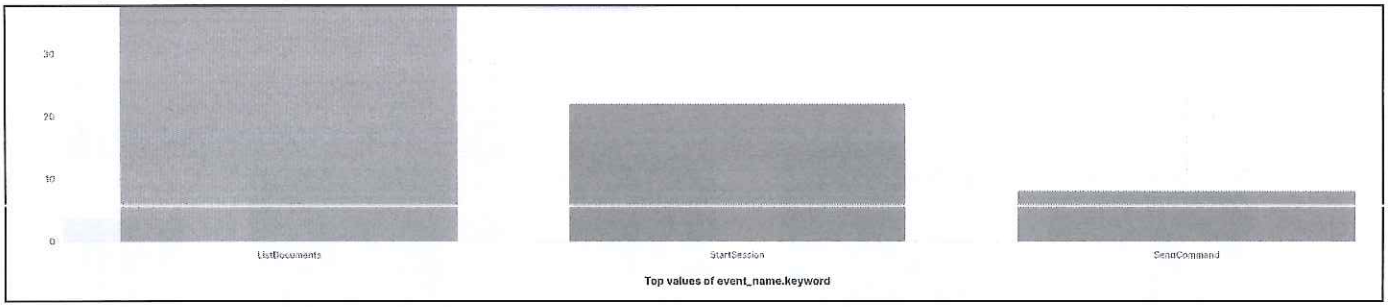
11. Now we need to see what the attacker was doing with SSM. SSM allows administrators to perform actions across their VM fleet, change the event_source filter to ssm.amazonaws.com.

```
source_host:5.62.19.62 and event_source:"ssm.amazonaws.com"
```



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

12. Your graph should change to list three SSM commands executed.



What were the three commands sent via SSM?

ListDocuments, StartSession, SendCommand

- ListDocuments is part of SendCommand, it allows an authorized user (or attacker) to send commands to EC2 VMs and have them executed as root.
- StartSession will open a command shell on the remote EC2 vm, without the need for a password or ssh key. Looks like our attacker got access to an IAM role and then moved over to executing commands on our EC2 system!

Warning

Make sure to clear your filters before moving on to the next lab

Key Takeaways

- When credentials are exposed proper role based access controls are essential
- Once an attacker has credentials they can scan access and move between resources quickly
- SSM will allow an attacker with the proper level of account access to execute commands across your fleet of EC2 VMs

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Lab 2.6: Container Investigations

Objectives

- Learn about the metadata service

Background

We've tracked the attack back to a EKS IAM role. EKS stands for Elastic Kubernetes Service and while this service which manages containers does not usually directly get exploited, many of the premade templated containers are out of date and are exploited regularly.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM

Lab Content

1. To be completed

> ⚠ **Warning**
>
> Make sure to clear your filters before moving on to the next lab

Key Takeaways

-

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Lab 3.1: Using SOF-ELK® with Azure Logs

Objectives

- Become familiar with the Pymtechlabs environment
- Discover users in Pymtechlabs
- Discover the machines in Pymtechlabs
- Discover the "normal" IPs Pymtechlabs employees may be using to access cloud resources

Background

Pymtechlabs has received intelligence that some of their cloud systems have been compromised. The regular IT team had an emergency and is unavailable. Before they left, they downloaded the logs from Azure and imported them to the SIEM (SOF-ELK). You will need to figure out which system(s) and account(s) have been compromised.

Since we haven't talked about the different log sources yet, this lab will guide you through the various steps to familiarize you with SOF-ELK and the Pymtechlabs environment.

Preparation

To prepare:

1. Make sure your SOF-ELK VM is running
2. Access Kibana via the IP address shown on the SOF-ELK VM
3. Relevant timeframe: `2021-03-12 00:00 to 2021-04-02 00:00 UTC`

Load Data

Except for the bonus section at the end, the data for this lab has been pre-loaded in the VM for your convenience.

If for some reason you need to re-load the data, it's located in `/home/elk_user/lab-3.1_backup_evidence.zip`

Lab Content

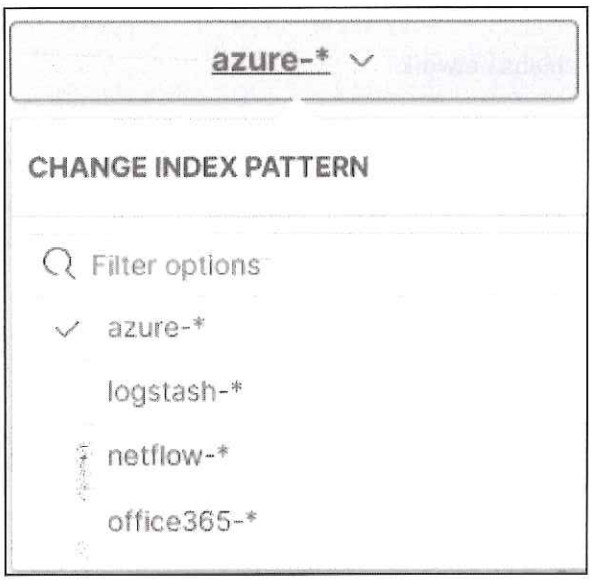
Review the indices in SOF-ELK

Start in the Discover tab

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

When data is imported in SOF-ELK, it's assigned to a specific index. In this lab we will be using the `azure-*` index.



This index contains any one of the following logs:

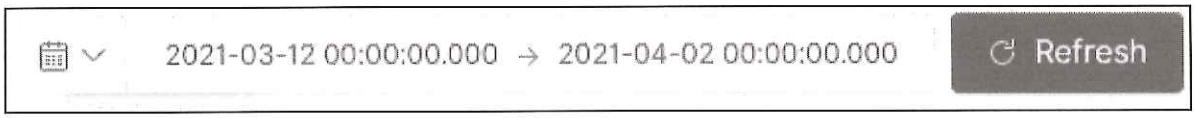
- insights-activity-logs
- insights-logs-auditlogs
- insights-managedidentitysigninlogs
- insights-noninteractiveusersigninlogs
- insights-serviceprincipalsigninlogs
- insights-logs-signinlogs

The activity, audit and signin logs have different schema, so as you look at various events you will notice:

- not all fields contain data
- some data is repeated in different fields
- data in a field may be formated one way in one record and a different way in another

It's important to be aware of these issues and not let them impede your investigation.

As mentioned in the preparation step, be sure to sure to set your search timeframe to `2021-03-12 00:00 to 2021-04-02 00:00 UTC` hit `Update`.



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Discover users in Pymtechlabs

Our investigation will be easier if we know the various users in the Pymtechlabs network.

1. Fields with user name information

Looking at the field names on the left, what are some fields that may contain username information?

a. user_id

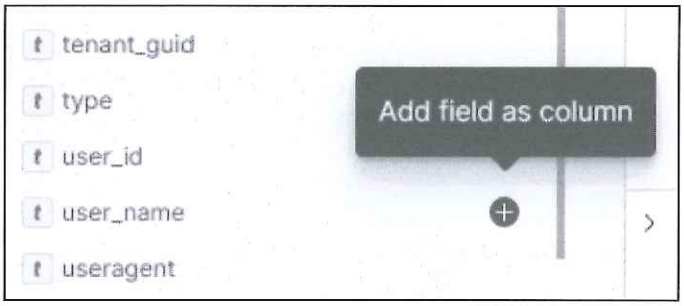
b. user_name

c. user_principal_name

What information do these fields contain?

- user_id: the GUID of the user
- user_name: the name of the user
- user_principal_name = UPN - the email & login ID

For each field above, select the + sign next to it to add it as a column



Your screen will change from a list with all the raw records to a list with the 3 fields mentioned above as columns:

Time	user_name	user_principal_name	user_id
2021-04-01 17:19:35.532 +00:00	Luis	luis@pymtechlabs.com	1c587fa4-0dbb-472c-bdc8-5477beefb3a9
2021-04-01 17:19:34.798 +00:00	-	-	-
2021-04-01 17:19:34.728 +00:00	Luis	luis@pymtechlabs.com	1c587fa4-0dbb-472c-bdc8-5477beefb3a9
2021-04-01 17:19:34.643 +00:00	-	-	-
2021-04-01 17:18:41.393 +00:00	Luis	luis@pymtechlabs.com	1c587fa4-0dbb-472c-bdc8-5477beefb3a9

Some records do not contain any information. It would be nice to eliminate them from the search. Use the following filter:

```
user_name: *
```



Don't forget to hit `Update` after entering your filter.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

>	2021-04-01 16:04:54.156 +00:00	Janet Van Dyne	jvandyne@pymtechlabs.com	76362af6-e38a-41e7-adab-e21ad7e23a20
>	2021-04-01 16:04:54.123 +00:00	Janet Van Dyne	jvandyne@pymtechlabs.com	76362af6-e38a-41e7-adab-e21ad7e23a20
>	2021-04-01 02:00:21.839 +00:00	Hank Pym	admin@pymtechlabs.com	675be0f4-2486-4443-bef6-d37d9043ae99
>	2021-03-31 22:39:02.496 +00:00	Hank Pym	admin@pymtechlabs.com	675be0f4-2486-4443-bef6-d37d9043ae99
>	2021-03-31 21:38:06.509 +00:00	Hank Pym	admin@pymtechlabs.com	675be0f4-2486-4443-bef6-d37d9043ae99
>	2021-03-31 20:37:52.483 +00:00	Hank Pym	admin@pymtechlabs.com	675be0f4-2486-4443-bef6-d37d9043ae99
>	2021-03-31 20:17:44.901 +00:00	Luis	luis@pymtechlabs.com	1c587fa4-0dbb-472c-bdc8-5477beefb3a9
>	2021-03-31 19:46:25.741 +00:00	Luis	luis@pymtechlabs.com	1c587fa4-0dbb-472c-bdc8-5477beefb3a9
>	2021-03-31 19:46:25.489 +00:00	Luis	luis@pymtechlabs.com	1c587fa4-0dbb-472c-bdc8-5477beefb3a9
>	2021-03-31 19:46:24.326 +00:00	Luis	luis@pymtechlabs.com	1c587fa4-0dbb-472c-bdc8-5477beefb3a9

We now have a long list of records with repeated names. In our situation, the list is short enough to figure out the unique names. However, what if you had a much longer list of users? Let's jump to the visualization tab to create a table of unique usernames.

2. Create a table of unique user names

   This question will be answered in the Visualize tab

   Jump to the `Visualize` tab in Kiabana and select `Create visualization`

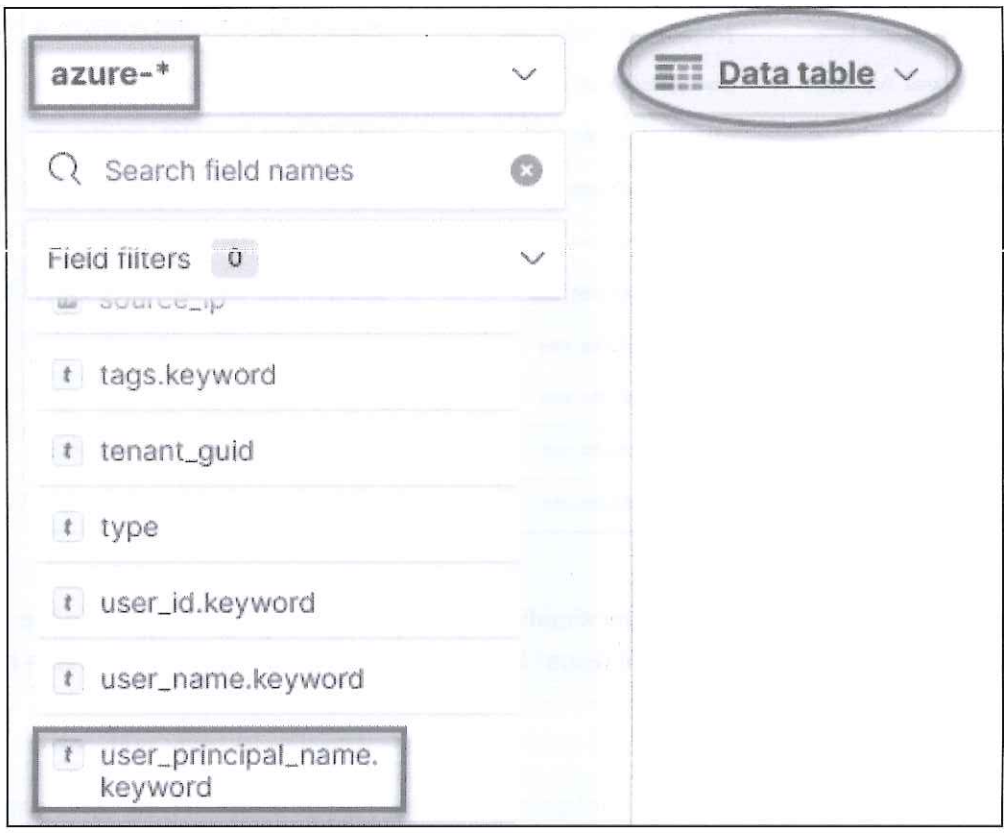


   Choose `Lens` as it's the easiest way to create a new visualization.



   Be sure to be on the correct index: `azure-*` or the field filters menu will be empty.

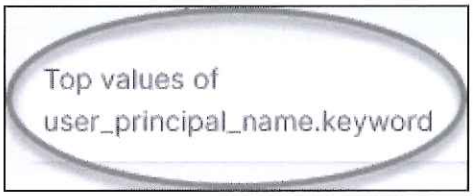
 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



Change your graph type to `Data table` and drag&drop `user_principal_name.keyword` to the middle of your screen.

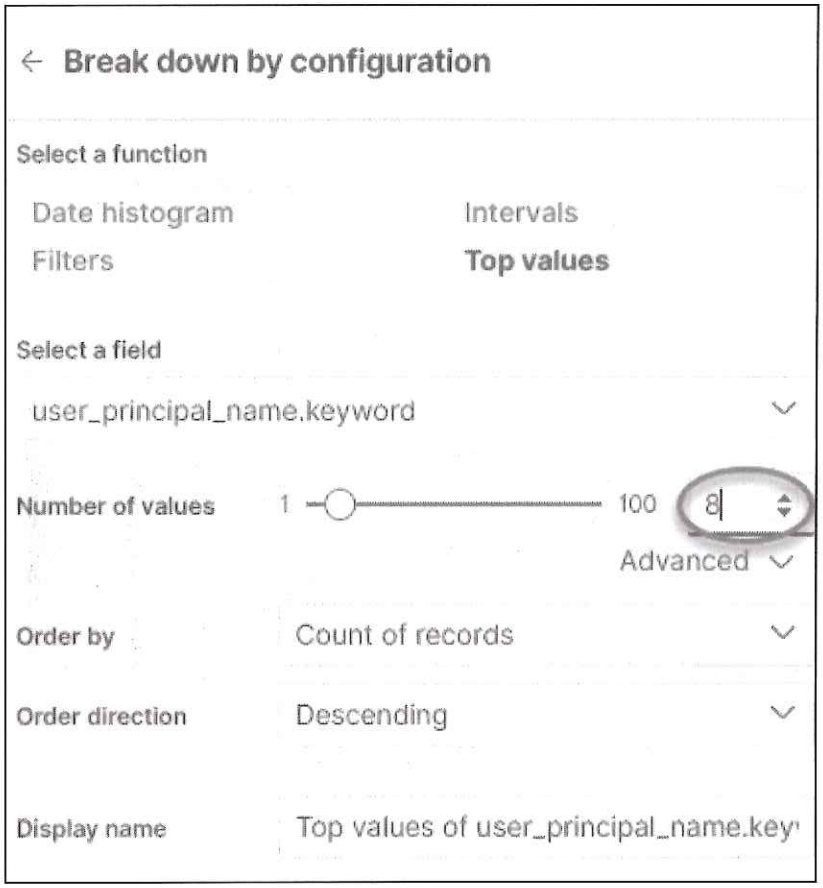
We now get a table but there is a field called `Other` that's hiding valuable information. We need to allow more rows in our table.

On the right of your screen, select `Top values of user_principal_name.keyword`



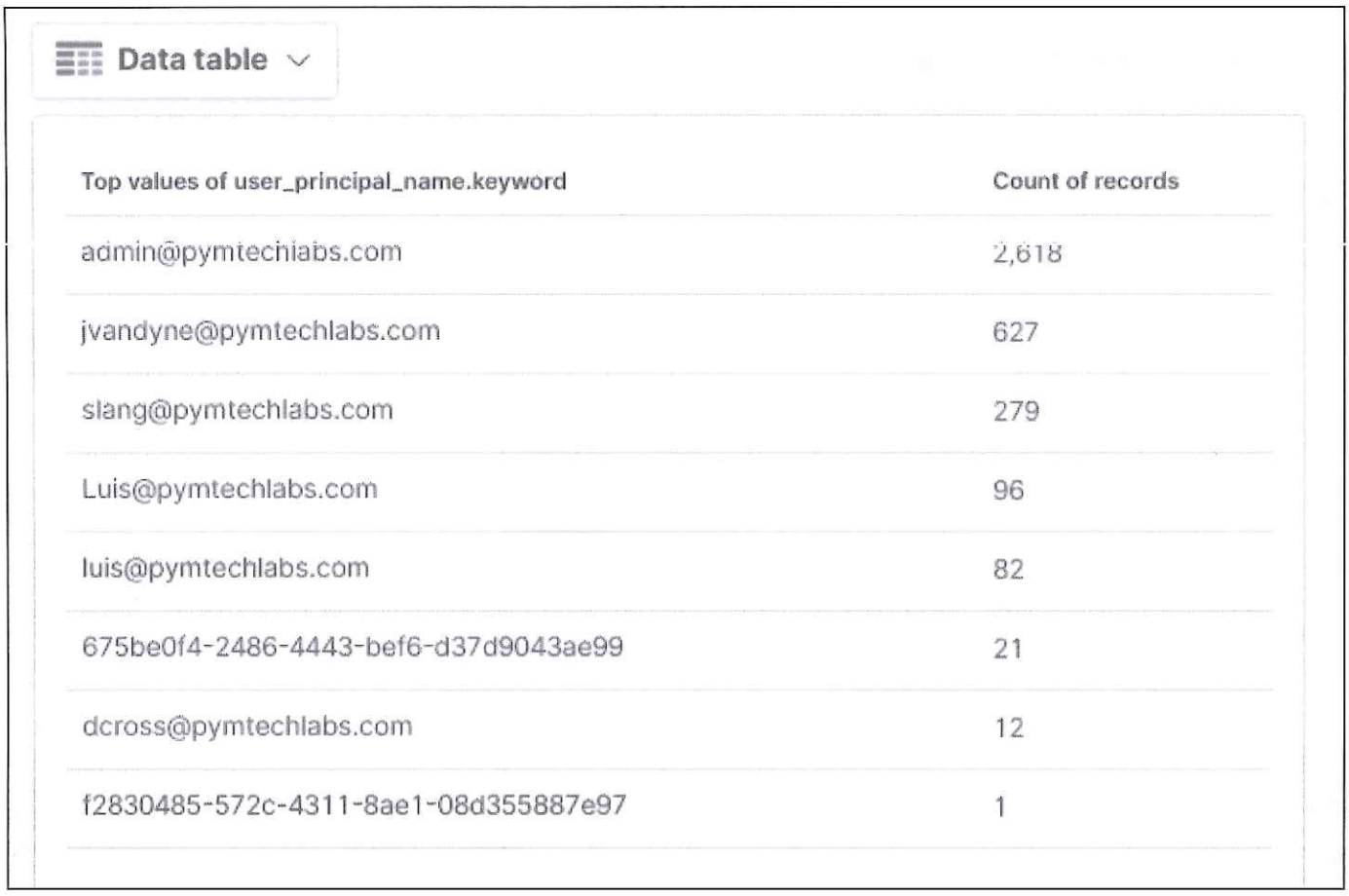
You will now get a menu where you can add more rows.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



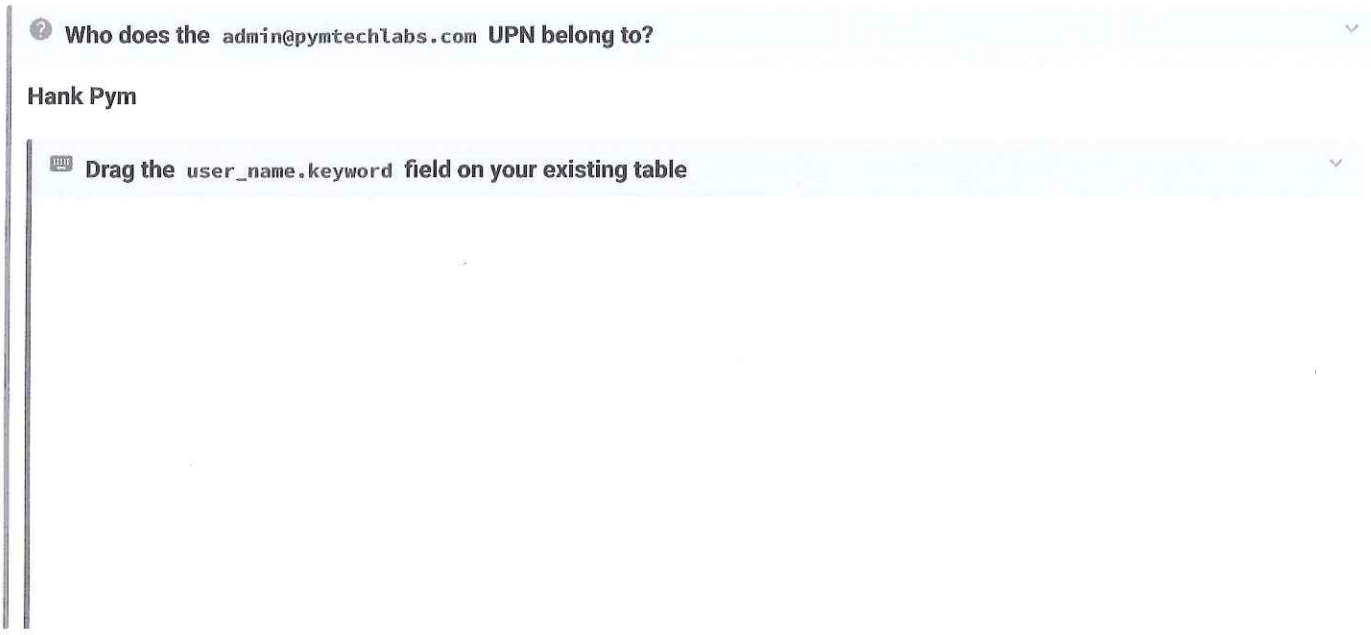
You now have a table that shows you the unique UPNs for Pymtechlabs as well as the number of occurrences each UPN appears in the logs.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



Note that luis is spelled once with a lowercase `l` and once with an uppercase `I`. It has no special meaning other than to point the inconsistencies between different log schemas.

3. Question about the admin UPN



https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Top values of user_principal_name.keyword	Top values of user_name.keyword	Count of records
admin@pymtechlabs.com	Hank Pym	1,036
jvandyne@pymtechlabs.com	Janet Van Dyne	627
slang@pymtechlabs.com	Scott Lang	279
luis@pymtechlabs.com	Luis	82
675be0f4-2486-4443-bef6-d37d9043ae99	675be0f4-2486-4443-bef6-d37d9043ae99	21
dcross@pymtechlabs.com	Darren Cross	12
f2830485-572c-4311-8ae1-08d355887e97	f2830485-572c-4311-8ae1-08d355887e97	1

You will notice that some GUIDs sneaked into the `user_principal_name` field. The GUID ending in `ae99` belongs to Hank Pym (admin@pymtechlab.com) and the one ending in `7e97` belongs to Scott Lang (slang@pymtechlabs.com). There is no clear explanation as to why these bits of data appear inconsistently like that.

Discover the machines in Pymtechlabs

There is no simple query to discover the names of the machines in Pymtechlabs. However, remember that virtual machines belong to the `Microsoft.Compute` provider. Every log entry contains the name of the resouce that's being operated on. This information is contained in the field `resource_id`.

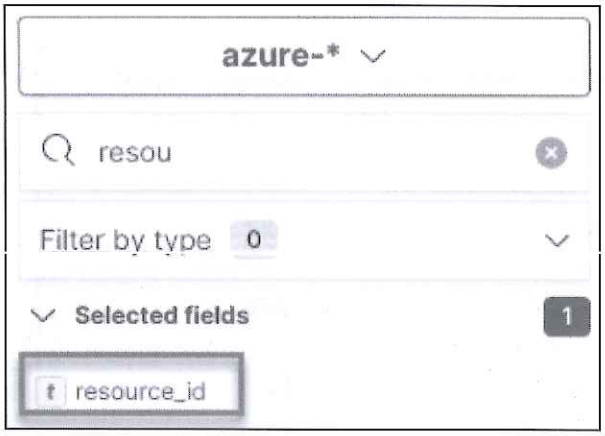
Use the Discover tab for this question

When you select the Discover tab (after completing your work in the Lens tab), you will get a message indicating that you have unsaved changes. Just select `Confirm`.

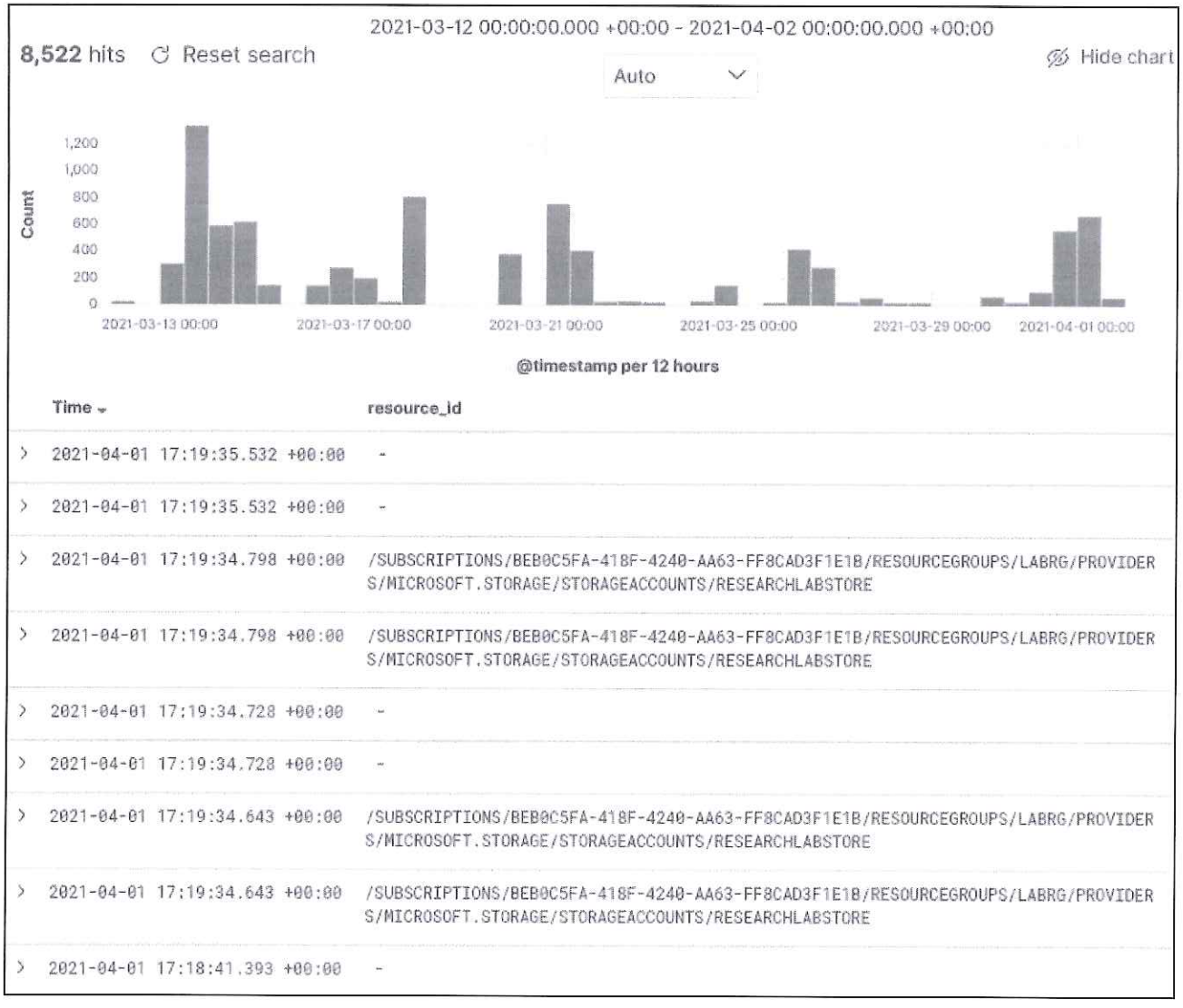
Once you are back in the Discover tab, if there is any remaining filter, be sure to remove it.

In the discover tab, select the field `resource_id`.

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon



You will get a table that shows every resource found in the logs as well as a lot of blank lines.



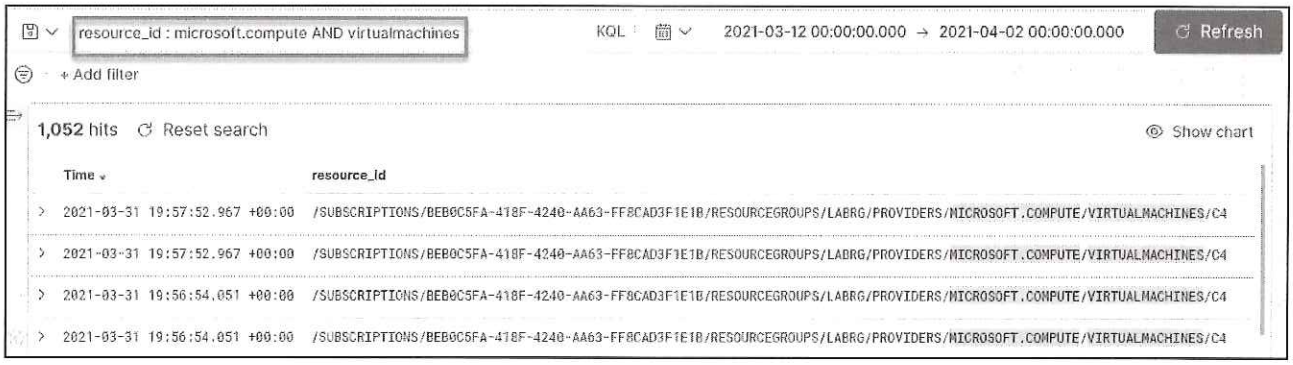
Time	resource_id
2021-04-01 17:19:35.532 +00:00	-
2021-04-01 17:19:35.532 +00:00	-
2021-04-01 17:19:34.798 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/RESEARCHLABSTORE
2021-04-01 17:19:34.798 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/RESEARCHLABSTORE
2021-04-01 17:19:34.728 +00:00	-
2021-04-01 17:19:34.728 +00:00	-
2021-04-01 17:19:34.643 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/RESEARCHLABSTORE
2021-04-01 17:19:34.643 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/RESEARCHLABSTORE
2021-04-01 17:18:41.393 +00:00	-

1. Filter for virtual machines

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Write a filter to limit the search to virtual machines

```
resource_id : microsoft.compute AND virtualmachines
```



2. Get a list of unique machines

Use the Visualize tab for this question

Use the same process as in the previous question to create a table of unique values using the `resource_id.keyword` field.

What are the names of the machines in Pymtechlabs?

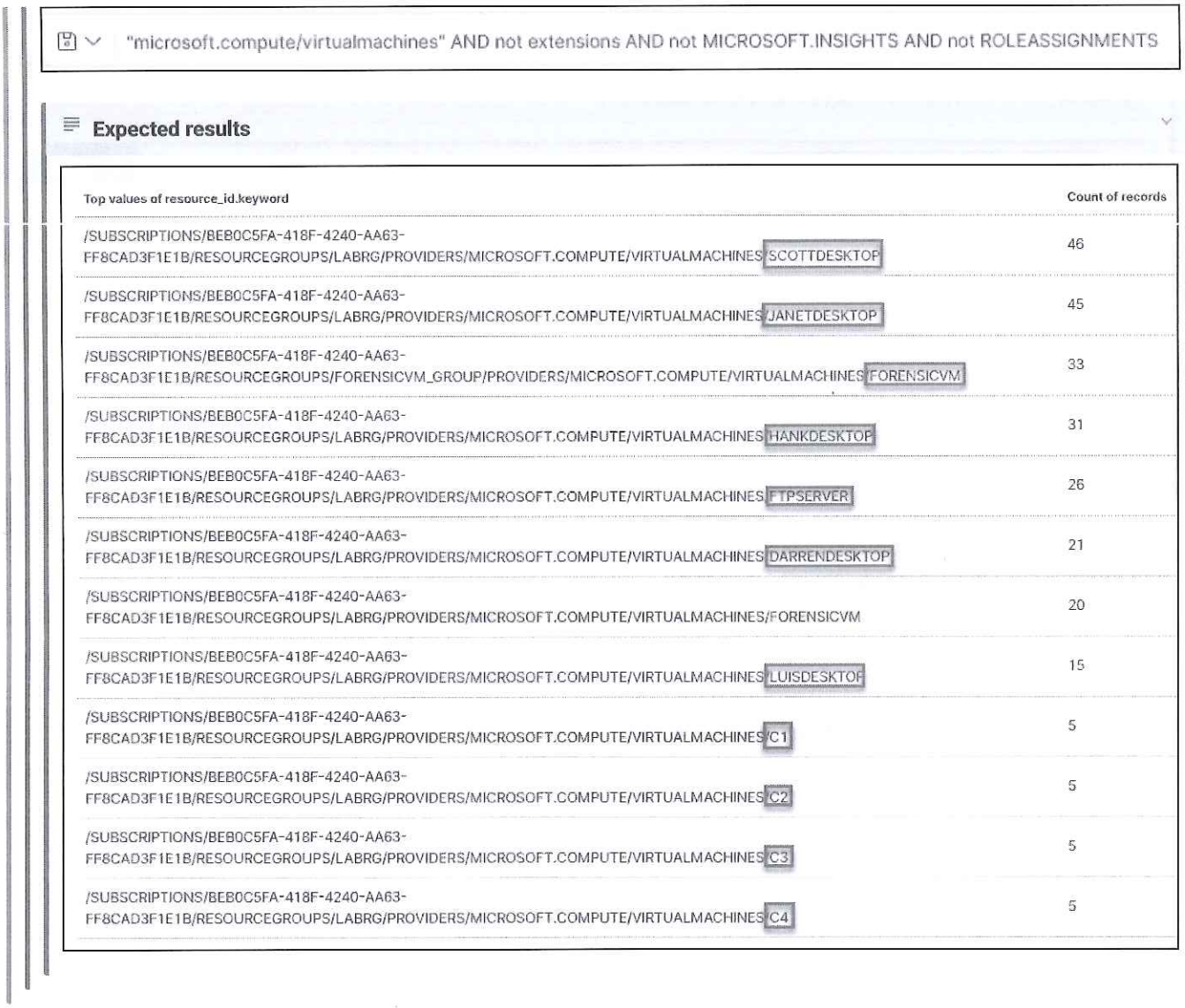
- hankdesktop
- scottdesktop
- janetdesktop
- darrendesktop
- luisdesktop
- ftpserver
- forensicvm
- c1
- c2
- c3
- c4

There is a lot of noise we need to filter

```
resource_id : microsoft.compute AND virtualmachines AND not extensions AND not MICROSOFT.INSIGHTS AND
not ROLEASSIGNMENTS AND not DISKS
```

Also, don't forget to expand the number of rows in your table.

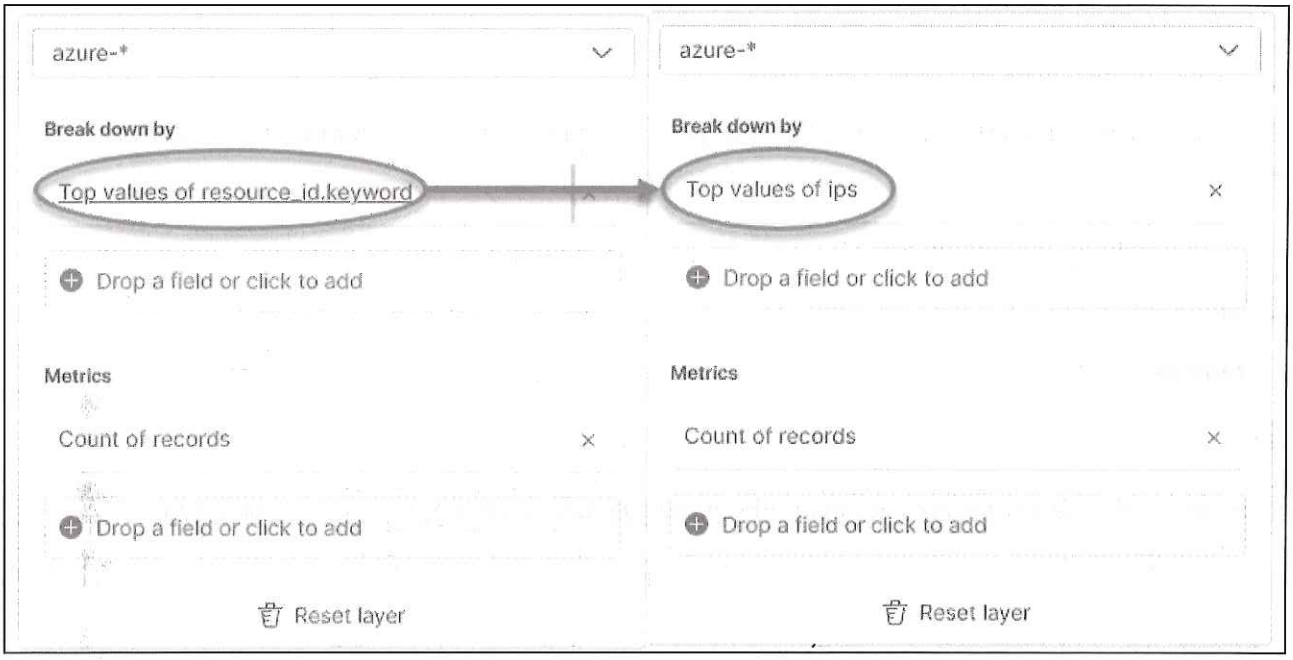
© 2021 Pierre Lidome, David Cowen, and Josh Lemon



Discover the "normal" IPs Pymtechlabs employees may be using to access cloud resources

We have a table with our unique VM names. If we just replace `resource_id.keyword` with `ips` we will get the answer we are looking for. Be sure to leave the noise filter on and don't forget to add rows to your table.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



What IP addresses did you find?

- 45.41.180.139
- 45.56.183.51
- 45.41.180.209
- 85.206.166.82
- 45.132.115.50
- 45.41.180.195
- 154.6.28.254

Any IP strike you as different?

- 85.206.166.82
- 154.6.28.254

Why are these IPs different?

- `85.206.166.82` : will be part of a future lab
- `154.6.28.254` : this is a Microsoft cloud address.
  It's important to keep the noise filter as Azure performs 100s of internal operations which generate log entries. These operations have internal Microsoft IP addresses associated with them.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Bonus Lab Content: Import data into SOF-ELK

In lab 1.1, we ingested the Microsoft Unified Access Log (UAL) into SOF-ELK. The UAL is exported as a single file which makes the process very simple. Unfortunately, that's not the case for Azure logs.

Log on to the SOF-ELK VM with the credentials

- Username: ***elk_user***
- Password: ***forensics***

You may log on to the console, however it's recommended to log in via SSH.

The audit log has been downloaded and archived in the file `/home/elk_user/lab-3.1_source_evidence.zip` .

The data is contained in a series of files called `PT1H.json` which are deeply nested. Feel free to explore if you would like to.

1. Extract the data with the commands:

```
cd ~
unzip lab-3.1_source_evidence.zip
```

2. Combine these PT1H.json files into a single file:

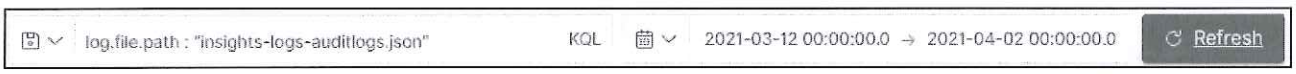
```
cd /home/elk_user/lab-3.1_source_evidence
find ./insights-logs-auditlogs/ -type f -name PT1H.json -exec cat {} + |tee insights-logs-
auditlogs.json
```

```
drwxrwxr-x 3 elk_user elk_user     58 Apr  1 13:02 insights-logs-auditlogs
-rw-rw-r-- 1 elk_user elk_user 774372 Apr  3 20:04 insights-logs-auditlogs.json
[elk_user@sof-elk lab-3.1_source_evidence]$
```

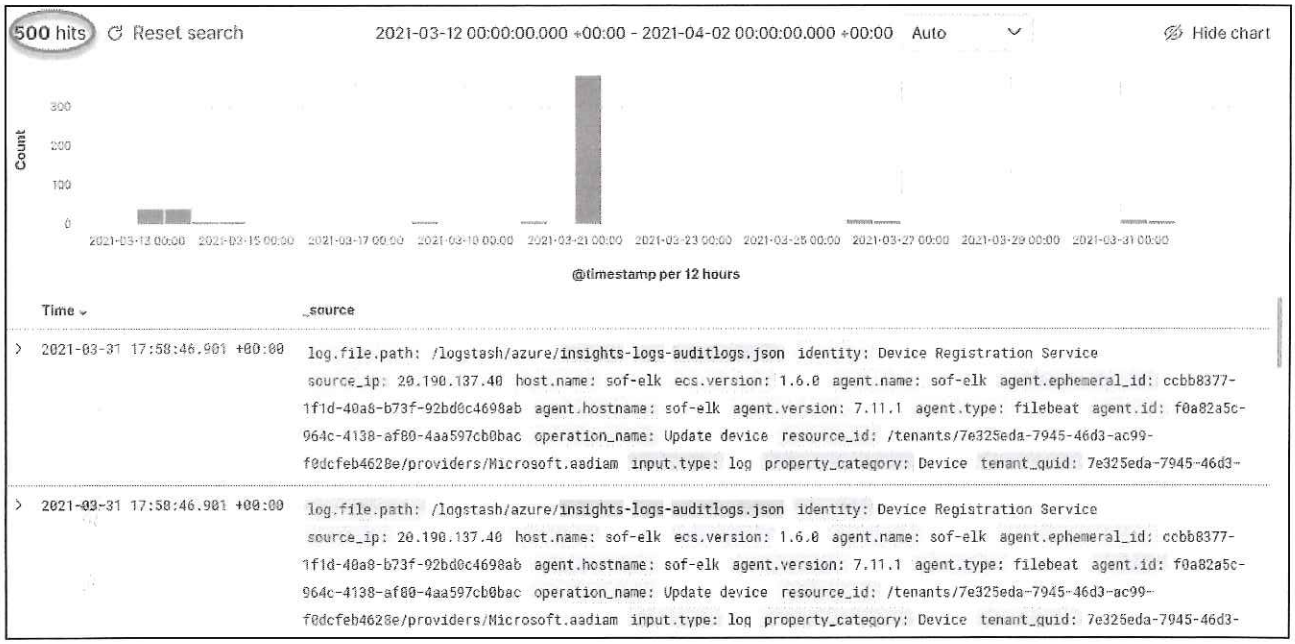
3. Copy the file to the correct logstash directory so it can be ingested into SOF-ELK:

```
cp insights-logs-auditlogs.json /logstash/azure
```

You can now check in Kibana that you have events from that log (give SOF-ELK a couple minutes to ingest all the data).



© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Key Takeaways

- Pymtechlabs has 5 users
- Pymtechlabs has 11 virtual machines
- Normal IPs for Pymtechlabs appear to be in the 45.x.x.x subnet

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Lab 3.2: AAD Password Spray Attack

Objectives

- Become familiar with the Azure Active Directory (AAD) logs
- Search logs for anomalous activity
- Visualize a password spray attack

Preparation

For this lab, you will need to:

1. Set your timeframe to `2021-03-12 00:00 to 2021-04-02 00:00 UTC`
2. Set your index to `Azure-*`
3. Be on the Kibana's Discovery tab

> **Note**
>
> The screenshots will show results that include the bonus section of lab 3.1. If you didn't complete that section, your results will be slightly different.

Lab Content

To search for possible AAD password spray attacks, we will look for clusters of failed logins.

1. Select log source

> **Which log source would show user logins?**
>
> `insights-logs-signinlogs.json`

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Create a filter to limit your searches to this log source



Instead of a filter, you could use a search query. However, it's nicer to have less clutter on the search bar.

2. Narrow down the search

Per the sign-in logs schema, the field `ResultType` reflects the result of the sign-in operation, success or failure. The field `ResultSignature` contains the error code, if any, for the sign-in operation. In practice, the sign-in logs provides the error code in the `ResultType` field and the `ResultSignature` seems to always contain the word "None". Azure is such a fast changing environment that the documentation is not always up-to-date.

In SOF-ELK, we mapped the error code to the field `result_type` .

In addition, no documentation has been found with possible error code values. Through observation, we know about the following values:

- 0 : success
- 50074: MFA failed
- 50126: Failed password
- 50140: Interrupted due to "Stay signed in?" message

Pymtechlabs uses multiple factor authentication. Therefore, when dealing with a password spray attack we would expect the authentication to fail at the first level.

First step, select the relevant field. Which ones would you select?

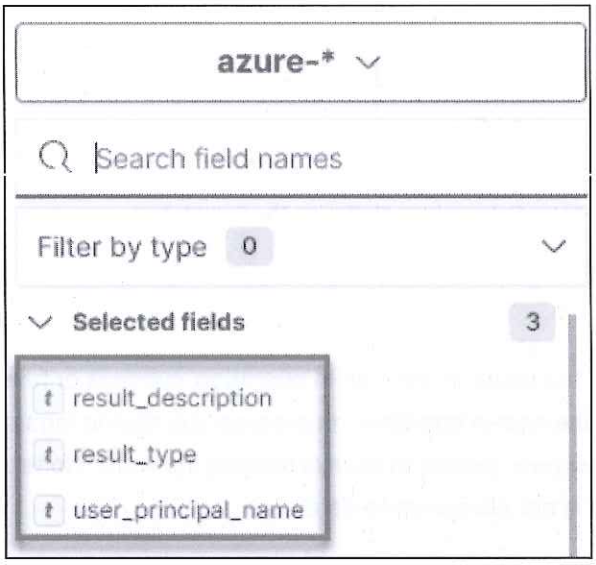
a. user_principal_name

b. result_type

c. result_description

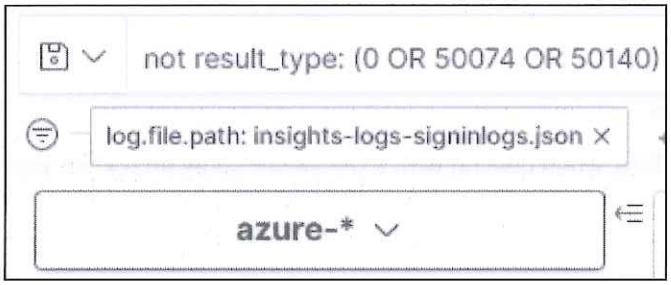
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

d. Optional: authentication_details (will use up a lot of real estate on your screen)

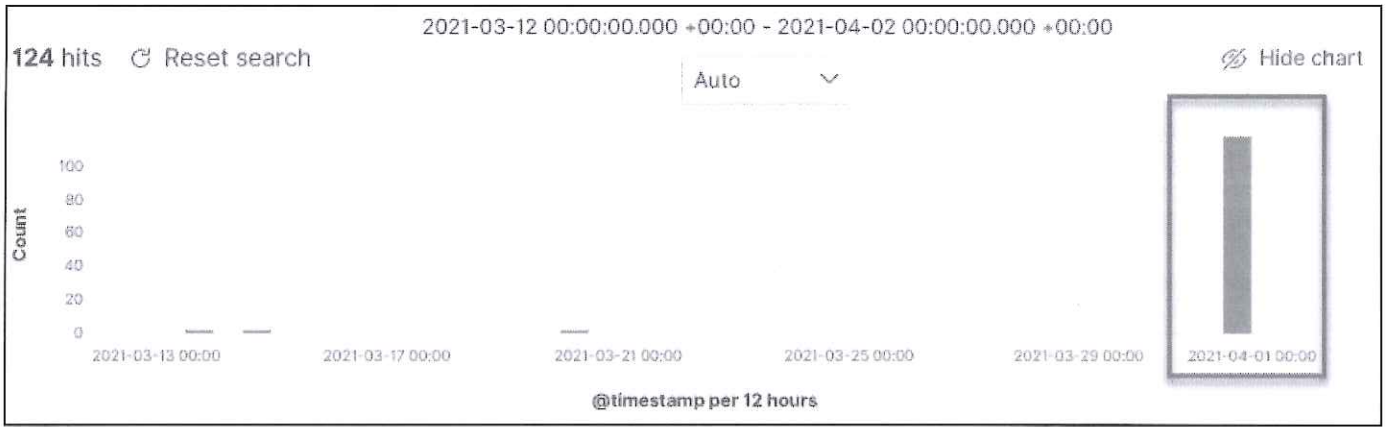


Now that we have all login events, what filter would you write to only see the failed password events?

```
not result_type: (0 OR 50074 OR 50140)
```



We now have a list of all the failed password attempts. In itself, this doesn't prove a password spray attack. However, Kibana gives a graph of the events over time.

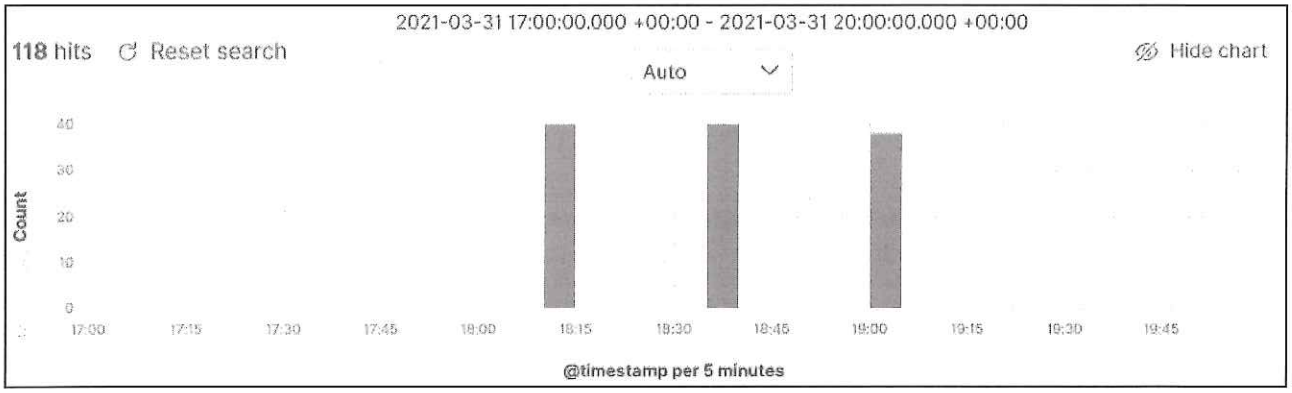


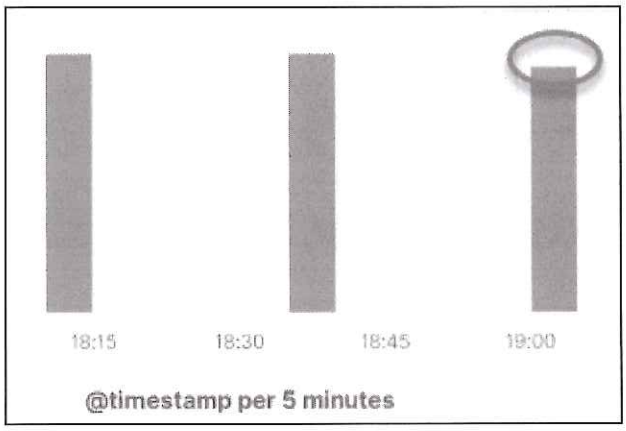
https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

You will notice a few events here and there followed by a huge spike on 2021-04-01 (time is approximate at this scale, we will need to narrow it down in the next step).

3. Investigate the failed login spike

   We need to narrow down our search by changing the timeframe.

> **Change your timeframe to** `2021-03-31 17:00 - 2021-03-31 20:00`
>
> 
>
>
> Notice that by narrowing down the timeframe, the resolution changed to 5 minutes. You could narrow down the timeframe some more and go down to a 1 minute resolution but that's not necessary in this case.
>
> With this 5 minutes resolution, you can clearly see 3 clusters of failed logins.

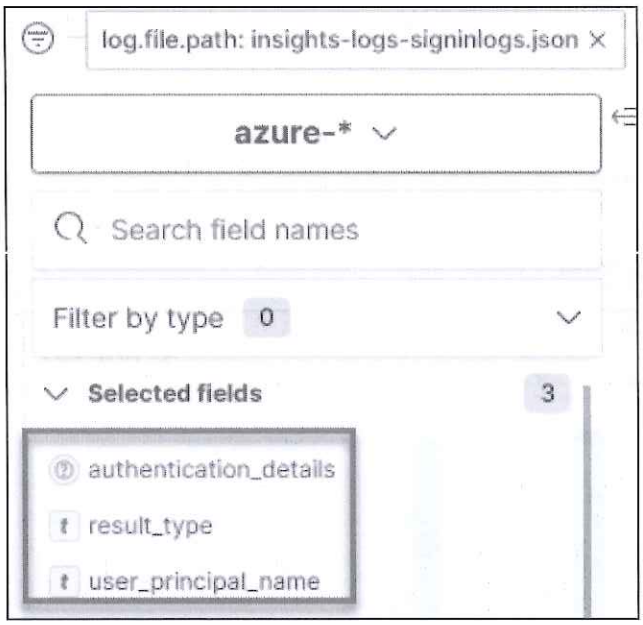
> **Do you notice anything strange on the 3rd cluster?**
>
> 
>
>
> It looks like there is one less failed login on the 3rd cluster. It could be that the bad actor simply tried fewer passwords or it could be something much more concerning...On to the next step.

4. Any successful login during this time?

   The last thing we want to see is a successful login in the middle of a password spray attack. Let's investigate this possibility.

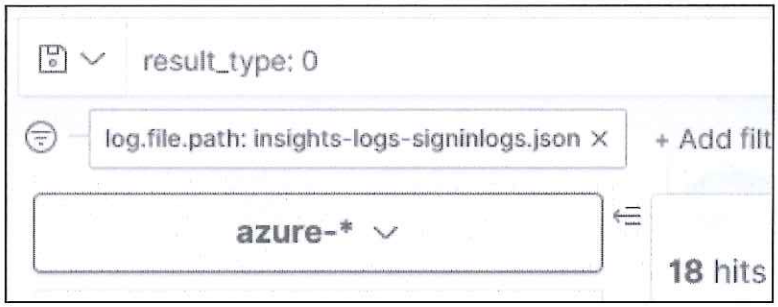
   Before you proceed change your filter to show `user_principal_name`, `result_type`, `authentication_details`

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



What filter would you write to test for this possibility?

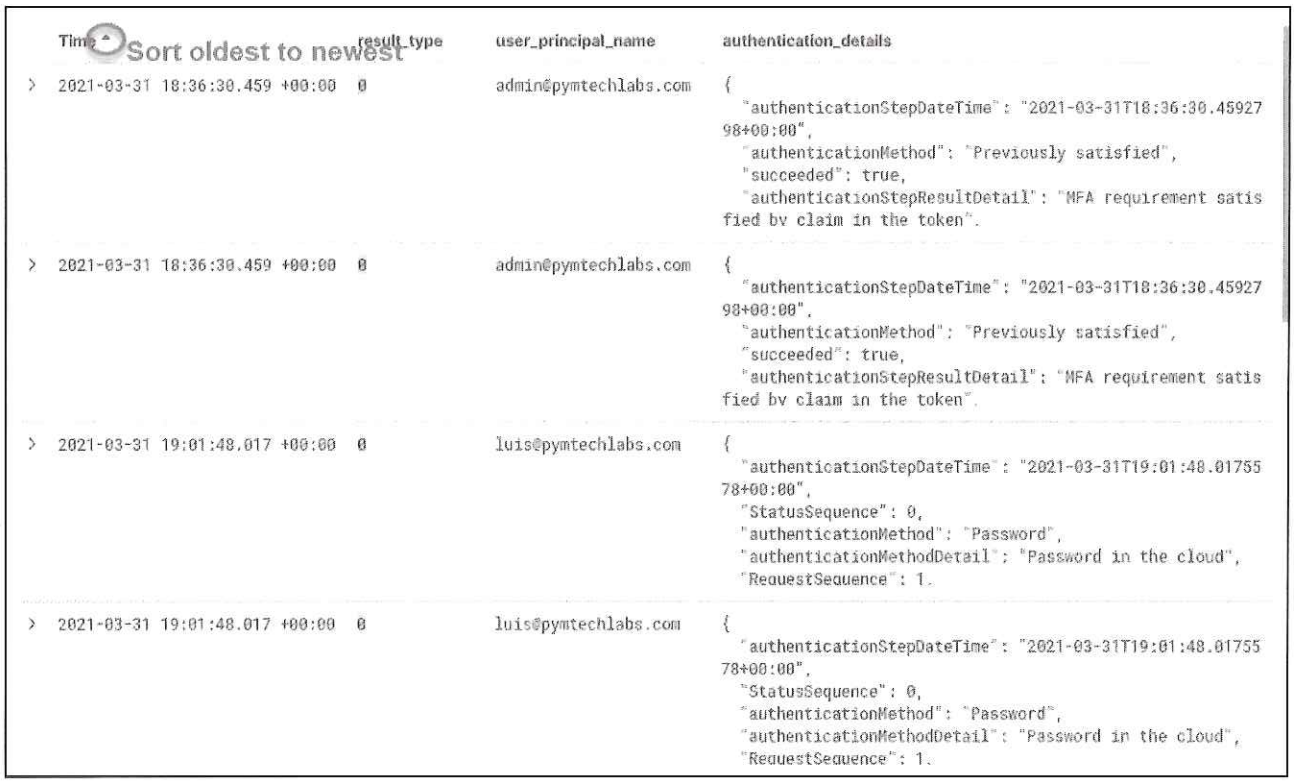
```
result_type: 0
```



Be sure to keep the same narrow timeframe and sort the results from oldest to newest

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24



Time (Sort oldest to newest)	result_type	user_principal_name	authentication_details
2021-03-31 18:36:30.459 +00:00	0	admin@pymtechlabs.com	{ "authenticationStepDateTime": "2021-03-31T18:36:30.4592798+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "MFA requirement satisfied by claim in the token".
2021-03-31 18:36:30.459 +00:00	0	admin@pymtechlabs.com	{ "authenticationStepDateTime": "2021-03-31T18:36:30.4592798+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "MFA requirement satisfied by claim in the token".
2021-03-31 19:01:48.017 +00:00	0	luis@pymtechlabs.com	{ "authenticationStepDateTime": "2021-03-31T19:01:48.0175578+00:00", "StatusSequence": 0, "authenticationMethod": "Password", "authenticationMethodDetail": "Password in the cloud", "RequestSequence": 1.
2021-03-31 19:01:48.017 +00:00	0	luis@pymtechlabs.com	{ "authenticationStepDateTime": "2021-03-31T19:01:48.0175578+00:00", "StatusSequence": 0, "authenticationMethod": "Password", "authenticationMethodDetail": "Password in the cloud", "RequestSequence": 1.

The first event is Hank Pym logging in at the same time as the attack (coincidence and nothing to do with our investigation). However, the events at `2021-03-31 19:01:48.017` shows Luis successfully logged in with the correct password. This is becoming really concerning. It's not conclusive yet (one more step)!

Bonus question: how is a simple password login possible when MFA is enabled?

There are two possibilities:
1. Legacy authentication is enabled on this tenant (example: Activesync) which is something Microsoft is trying hard to obsolete.
2. Luis is part of an AAD Conditional Access rule. It's very typical in corporate environments where some accounts are exempted from MFA. Not a good practice, but sometimes necessary.

5. Examine the event's details

We need to make sure that the event we found doesn't represent a legitimate login. Before we call the user to confirm, let's check where this login originated from.

Do you see an IP address that could be out of the ordinary?

Open the event and check the IP address: 85.206.166.82 This IP address is from Lithuania and is very different from the 45.x.x.x IP addresses we saw in the first lab. It also doesn't belong to Microsoft.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

source_ip	85.206.166.82

There is a very strong possibility that we have a serious situation on our hands!

Key Takeaways

- Luis@pymtechlabs.com has very likely been compromised
- 85.206.166.82 is a likely the attacker's IP address
- We must now investigate what actions were taken with this compromised account

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Lab 3.3: Tracking Resource Creation

Objectives

- Review for the process to narrow log data
- Review the VM creation process
- Continue the investigation of a potentially compromised account

Preparation

For this lab, you will need to:

1. Set your timeframe to `2021-03-31 17:00 to 2021-04-02 00:00 UTC`
2. Set your index to `Azure-*`
3. Be on the Kibana's Discovery tab

Lab Content

We have strong suspicions that luis@pymtechlabs.com has been compromised. We should check what operations may have been performed by this account subsequent to the breach.

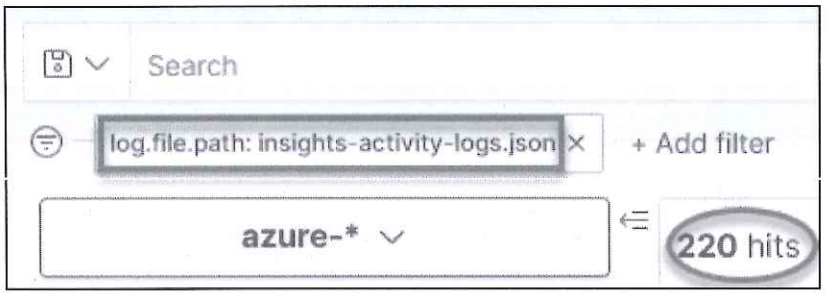
1. Narrow the timeframe

   Since the account was compromised on 2021-03-31, we want to narrow our timeframe to minimize the amount of noise. In Kibana, set your timeframe to `2021-03-31 17:00 to 2021-04-02 00:00 UTC`

2. Narrow the dataset to a specific log

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Which field would you filter for?



Your first instict might be to write a filter such as `user_principal_name: luis@pymtechlabs.com`. However, remember that not every schema includes every type of information. While it would work in this case, it's best to filter on the log type first and then narrow down your search.

3. Look for suspicious activity

To narrow down our search what field would show you activity in the subscription?

`operation_name` and `source_ip`

What do VALIDATE and WRITE indicate to you?

`New resources are being created`

How do we associate this activity with luis@pymtechlabs.com?

Add the filter

```
user_principal_name: luis@pymtechlabs.com AND source_ip: 85.206.166.82
```

Answer

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

	Time ^	operation_name	source_ip
>	2021-03-31 19:30:36.250 +00:00	MICROSOFT.ADDONS/SUPPORTPROVIDERS/LISTSUPPORTPLANINFO/ACTION	85.206.166.82
>	2021-03-31 19:30:36.659 +00:00	MICROSOFT.RECOVERYSERVICES/LOCATIONS/BACKUPVALIDATEFEATURES/ACTION	85.206.166.82
>	2021-03-31 19:30:37.599 +00:00	MICROSOFT.RECOVERYSERVICES/LOCATIONS/BACKUPVALIDATEFEATURES/ACTION	85.206.166.82
>	2021-03-31 19:30:39.505 +00:00	MICROSOFT.ADDONS/SUPPORTPROVIDERS/LISTSUPPORTPLANINFO/ACTION	85.206.166.82
>	2021-03-31 19:30:46.055 +00:00	MICROSOFT.RESOURCES/DEPLOYMENTS/VALIDATE/ACTION	85.206.166.82
>	2021-03-31 19:30:49.535 +00:00	MICROSOFT.RESOURCES/DEPLOYMENTS/VALIDATE/ACTION	85.206.166.82
>	2021-03-31 19:30:55.839 +00:00	MICROSOFT.RESOURCES/DEPLOYMENTS/VALIDATE/ACTION	85.206.166.82
>	2021-03-31 19:30:58.279 +00:00	MICROSOFT.RESOURCES/DEPLOYMENTS/VALIDATE/ACTION	85.206.166.82
>	2021-03-31 19:30:58.649 +00:00	MICROSOFT.RESOURCES/DEPLOYMENTS/WRITE	85.206.166.82
>	2021-03-31 19:31:02.574 +00:00	MICROSOFT.RESOURCES/DEPLOYMENTS/WRITE	85.206.166.82
>	2021-03-31 19:31:03.269 +00:00	MICROSOFT.NETWORK/PUBLICIPADDRESSES/WRITE	85.206.166.82
>	2021-03-31 19:31:07.224 +00:00	MICROSOFT.NETWORK/PUBLICIPADDRESSES/WRITE	85.206.166.82
>	2021-03-31 19:31:12.446 +00:00	MICROSOFT.NETWORK/NETWORKINTERFACES/WRITE	85.206.166.82
>	2021-03-31 19:31:16.737 +00:00	MICROSOFT.NETWORK/PUBLICIPADDRESSES/WRITE	85.206.166.82
>	2021-03-31 19:31:16.934 +00:00	MICROSOFT.NETWORK/NETWORKINTERFACES/WRITE	85.206.166.82

This is the IP address that we discovered in the previous lab which we found suspicious as it came from a location not normally associated with Pymtechlabs. We now see that the person using the luis@pymtechlabs.com account is creating a bunch of new resources.

4. Time to dig deeper

Filter for virtual machines

```
user_principal_name: luis@pymtechlabs.com AND operation_name: VIRTUALMACHINES AND source_ip: 85.206.166.82
```

What are the names of the virtual machines?

`C1, C2, C3, C4`

Hint: add `resource_id` to see the name of the machines.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Time ^	operation_name	resource_id
2021-03-31 19:31:17.449 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C1
2021-03-31 19:31:21.290 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C1
2021-03-31 19:32:31.399 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C1
2021-03-31 19:41:00.915 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C2
2021-03-31 19:41:04.621 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C2
2021-03-31 19:41:26.108 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C1
2021-03-31 19:41:51.825 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C2
2021-03-31 19:42:36.280 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C1
2021-03-31 19:44:07.990 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C3
2021-03-31 19:44:11.992 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C3
2021-03-31 19:44:52.579 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C3
2021-03-31 19:46:47.390 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C4
2021-03-31 19:46:50.427 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C4

Why would the bad actor create all these VMs. Is there something special about them?

5. VM creation

When a VM is created, there are a large number of operations performed by Azure. Let's look at that sequence of operations for a clue.

This sequence of event is tracked by the field `correlation_guid`. You can pick any of the records to select one of the numbers. For example, we will select the one for the C1 VM:

Time ^	operation_name	source_ip	resource_id
2021-03-31 19:31:17.449 +00:00	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE	85.206.166.82	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/C1

Expanded document — View surrounding documents — View single document

Table JSON

_id	jcSXn3gBt8s3rGNVR7yI
_index	azure-2021.03
_score	-
_type	_doc
@timestamp	2021-03-31 19:31:17.449 +00:00
@version	1
action	Microsoft.Compute/virtualMachines/write
agent.ephemeral_id	76696a5a-9507-4685-9414-165c8cfc5979
agent.hostname	sof-elk
agent.id	ae54f81e-c782-41ff-9f1a-2aafdb0ffb36
agent.name	sof-elk
agent.type	filebeat
agent.version	7.11.1
category	Administrative
correlation_guid	c35f64c5-89ad-4162-9de0-f48105c08120

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Change your search to that number:

```
correlation_guid : "c35f64c5-89ad-4162-9de0-f48105c08120"
```



What are the steps to building a VM?

- Create a deployment with the selected operating system
- Create a network interface
- Assign an IP address (internal and public)
- Create the OS disk
- Create the VM

To gain some real estate, remove `operation_name` and `source_ip` from your selected fields. Add the field `response_body`

Time ^	resource_id	response_body
> 2021-03-31 19:30:58.649 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOF	-
> 2021-03-31 19:31:02.574 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOF	-
> 2021-03-31 19:31:03.269 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOF	-
> 2021-03-31 19:31:07.224 +00:00	/SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOF	{"name":"C1-ip","id":"/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Network/publicIPAddresses/C1-ip","etag":"W/\"050f65e9-d011-423d-a521-f4b48f6ccd0d\"","location":"southcentralus","properties":{"provisioningState":"Updating","resourceGuid":"afde5f41-f54e-4c19-a67d-2cd0b2e8bf88","publicIPAddressVersion":"IPv4","publicIPAllocationMethod":"Dynamic","idleTimeoutInMinutes":4,"ipTags":[]},"type":"Microsoft.Network/publicIPAddresses","sku":{"name":"Basic"}}

You will notice that when some of the steps complete, they provide a pretty verbose message.

From the `response_body` information, what types of VMs were created?

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

```
Standard_NV4as_v4
```


```
{"name":"C1","id":"/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Compute/virtualMachines/C1","type":"Microsoft.Compute/virtualMachines","location":"southcentralus","properties":{"vmId":"4cda4db8-8c3a-48f8-beaa-1bb423f149d1","hardwareProfile":{"vmSize":"Standard_NV4as_v4"},"storageProfile":{"imageReference":{"publisher":"Canonical","offer":"UbuntuServer","sku":"18.04-LTS","version":"latest","exactVersion":"18.04.202103250"},"osDisk":{"osType":"Linux","createOption":"FromImage","caching":"ReadWrite","managedDisk":{"storageAccountType":"Standard_LRS"},"diskSizeGB":30},"dataDisks":[]},"osProfile":{"computerName":"C1","adminUsername":"luis","linuxConfiguration":{"disablePasswordAuthentication":false,"provisionVMAgent":true,"patchSettin
```


Is there anything special about this type of VMs?

These are GPU-enabled VMs. This mean that the bad actor's action on objective is likely to run crypto mining software.

6. Bonus

What query could you use to quickly search for GPU-enable VMs?



Time ▲	response_body
2021-03-31 19:31:21.290 +00:00	{"name":"C1","id":"/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Compute/virtualMachines/C1","type":"Microsoft.Compute/virtualMachines","location":"southcentralus","properties":{"vmId":"4cda4db8-8c3a-48f8-beaa-1bb423f149d1","hardwareProfile":{"vmSize":"Standard_NV4as_v4"},"storageProfile":{"imageReference":{"publisher":"Canonical","offer":"UbuntuServer","sku":"18.04-LTS","version":"latest","exactVersion":"18.04.202103250"},"osDisk":{"osType":"Linux","createOption":"FromImage","caching":"ReadWrite","managedDisk":{"storageAccountType":"Standard_LRS"},"diskSizeGB":30},"dataDisks":[]},"osProfile":{"computerName":"C1","adminUsername":"luis","linuxConfiguration":{"disablePasswordAuthentication":false,"provisionVMAgent":true,"patchSettings":{"patchMode":"ImageDefault"}},"secrets":[],"allowExtensionOperations":true,"requireGuestProvisionSignal":true},"networkProfil
2021-03-31 19:41:04.621 +00:00	{"name":"C2","id":"/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Compute/virtualMachines/C2","type":"Microsoft.Compute/virtualMachines","location":"southcentralus","properties":{"vmId":"70aacd5c-27bf-48f6-b81b-1df26bdb6d98","hardwareProfile":{"vmSize":"Standard_NV4as_v4"},"storageProfile":{"imageReference":{"publisher":"Canonical","offer":"UbuntuServer","sku":"18.04-LTS","version":"latest","exactVersion":"18.04.202103250"},"osDisk":{"osType":"Linux","createOption":"FromImage","caching":"ReadWrite","managedDisk":{"storageAccountType":"Standard_LRS"},"diskSizeGB":30},"dataDisks":[]},"osProfile":{"computerName":"C2","adminUsername":"Luis","linuxConfiguration":{"disablePasswordAuthentication":false,"provisionVMAgent":true,"patchSettings":{"patchMode":"ImageDefault"}},"secrets":[],"allowExtensionOperations":true,"requireGuestProvisionSignal":true},"networkProfil
2021-03-31 19:44:11.992 +00:00	{"name":"C3","id":"/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Compute/virtualMachines/C3","type":"Microsoft.Compute/virtualMachines","location":"southcentralus","properties":{"vmId":"d3612af5-2457-420b-9930-d3445923fc98","hardwareProfile":{"vmSize":"Standard_NV4as_v4"},"storageProfile":{"imageReference":{"publisher":"Canonical","offer":"UbuntuServer","sku":"18.04-LTS","version":"latest","exactVersion":"18.04.202103250"},"osDisk":{"osType":"Linux","createOption":"FromImage","caching":"ReadWrite","managedDisk":{"storageAccountType":"Standard_LRS"},"diskSizeGB":30},"dataDisks":[]},"osProfile":{"computerName":"C3","adminUsername":"luis","linuxConfiguration":{"disablePasswordAuthentication":false,"provisionVMAgent":true,"patchSettings":{"patchMode":"ImageDefault"}},"secrets":[],"allowExtensionOperations":true,"requireGuestProvisionSignal":true},"networkProfil
2021-03-31 19:46:50.427 +00:00	{"name":"C4","id":"/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Compute/virtualMachines/C4","type":"Microsoft.Compute/virtualMachines","location":"southcentralus","properties":{"vmId":"f1956003-b462-4422-b165-79ee8df48094","hardwareProfile":{"vmSize":"Standard_NV4as_v4"},"storageProfile":{"imageReference":{"publisher":"Canonical","offer":"UbuntuServer","sku":"18.04-LTS","version":"latest","exactVersion":"18.04.202103250"},"osDisk":{"osType":"Linux","createOption":"FromImage","caching":"ReadWrite","managedDisk":{"storageAccountType":"Standard_LRS"},"diskSizeGB":30},"dataDisks":[]},"osProfile":{"computerName":"C4","adminUsername":"luis","linuxConfiguration":{"disablePasswordAuthentication":false,"provisionVMAgent":true,"patchSettings":{"patchMode":"ImageDefault"}},"secrets":[],"allowExtensionOperations":true,"requireGuestProvisionSignal":true},"networkProfil

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Key Takeaways

We showed you a step-by-step approach so that you can use the same logic for other investigations. However, if you know what you are looking for, you can quickly search for it. Just be sure to consider the context of the results as it might be perfectly normal for your users to create GPU-enabled VMs (in this example).

- Luis@pymtechlabs.com is definitively compromised
- The bad actors have created VMs for the purpose of crypto mining
- Further investigation is required to make sure the breach is contained

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Lab 3.4: Detecting Data Exfiltration

Objectives

- Obtain storage account access keys
- Discover a log for storage account data transfer
- Compare to a traditional FTP transfer

Preparation

For this lab, you will need to:

1. Set your timeframe to `2021-03-31 17:00 to 2021-04-02 00:00 UTC`
2. Set your index to `Azure-*`
3. Be on the Kibana's Discovery tab

Lab Content

We know that our bad actor has created new VMs for the purpose of mining cryptocurrency. What else could they be up to? A typical action on objective is to exfiltrate data. Let's look for any activity that could indicate such actions.

When thinking about exfiltrating data, we need to consider where the data may be stored. There are two obvious locations:
1. a storage account
2. a disk attached to a VM

The first option is the most interesting from a cloud perspective.

To access a storage account, it's necessary to have access keys. Let's start there.

Clear any filters that you may have from prior labs.

1. Storage account keys

> **What's the service provider for storage?**
>
> `Microsoft.Storage`

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

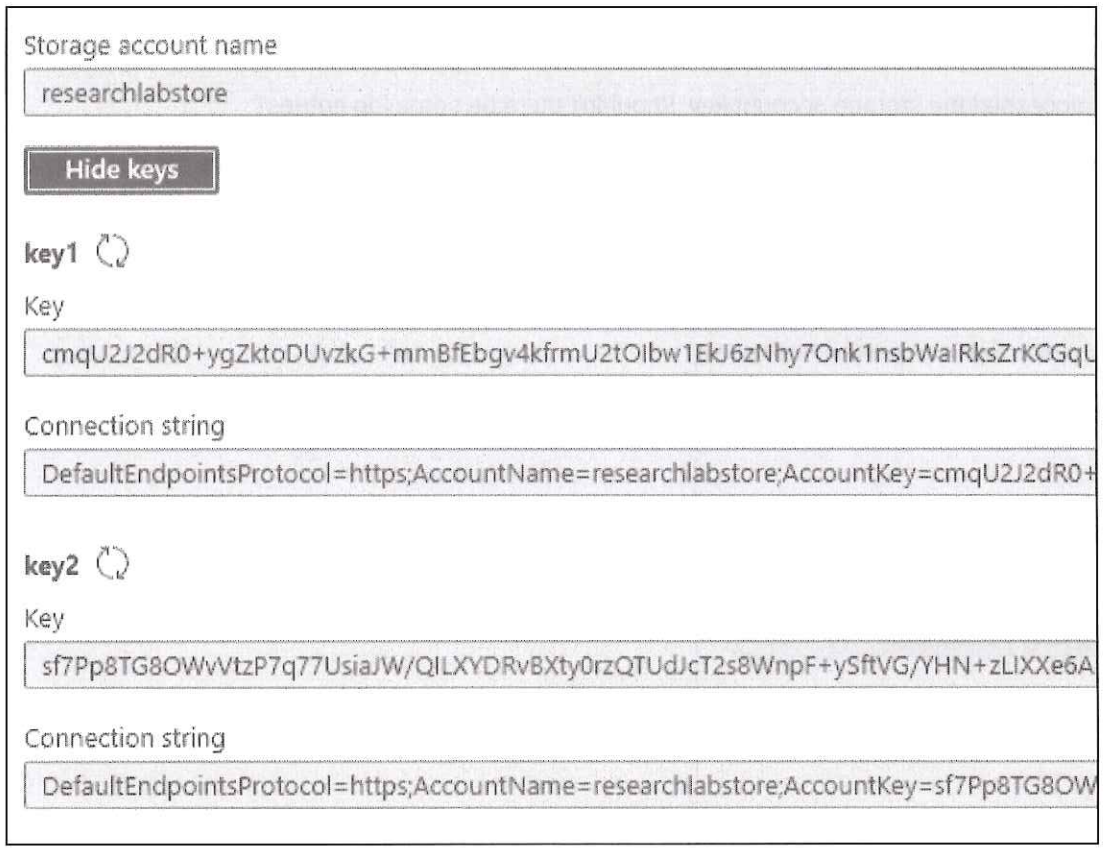
Enter `Microsoft.Storage` as a search term

Time	_source
> 2021-04-01 17:19:34.798 +00:00	scope: /subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Storage/storageAccounts/researchlabstore action: Microsoft.Storage/storageAccounts/listKeys/action operation_name: MICROSOFT.STORAGE/STORAGEACCOUNTS/LISTKEYS/ACTION resource_id: /SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/RESEARCHLABSTORE
> 2021-04-01 17:19:34.643 +00:00	scope: /subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Storage/storageAccounts/researchlabstore action: Microsoft.Storage/storageAccounts/listKeys/action operation_name: MICROSOFT.STORAGE/STORAGEACCOUNTS/LISTKEYS/ACTION resource_id: /SUBSCRIPTIONS/BEB0C5FA-418F-4240-AA63-FF8CAD3F1E1B/RESOURCEGROUPS/LABRG/PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/RESEARCHLABSTORE

Look for events with an `operation_name` of `Microsoft.Storage/storageAccounts/listKeys/action`.

The operation `LISTKEYS/ACTION` indicates that someone looked at the secret keys for the storage account.

In case you are not familiar with the storage account secret keys, this is what they look like in the console:



Yes, the keys are intentionally cut off to prevent anyone hacking my storage account :)

Which storage account was accessed and who accessed it?

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

> `researchlabstore` was accessed by Luis@pymtechlabs.com

If you open the record, you will see the fields `scope` and `resource_id` show that the target is a storage account called `researchlabstore`. The `user_principal_name` field shows that Luis@pymtechlabs.com is the one who performed the LISTKEYS operation.

t	scope	/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Storage/storageAccounts/researchlabstore
IP	source_ip	85.206.166.82
t	tags	process_archive, filebeat, beats_input_codec_plain_applied, azure_json_activity_log, _geoip_lookup_failure
t	type	azure
t	user_principal_name	Luis@pymtechlabs.com

> **Why was Luis able to access the keys?**
>
> Luis was able to access the keys because he had permission at the subscription level.

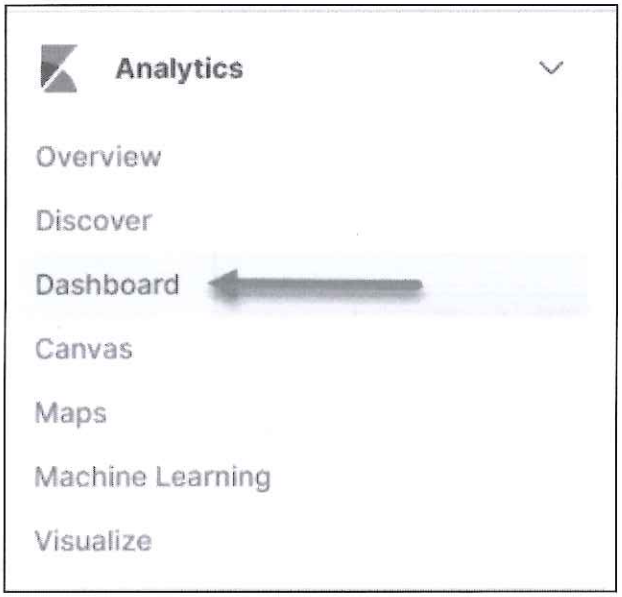
2. Transfering data

   We know that Luis accessed the storage account key. Shouldn't there be some log entries?

   Remember that we are only looking at the activity log and the sign-in logs in the `azure-*` index.

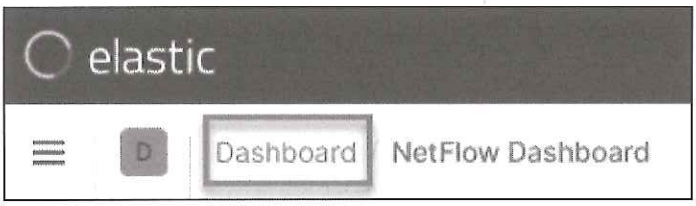
   It's time to look at a different index. If data is going to be transferred out, it would be logical to expect associated network traffic.

   Clear your search filter and switch to the **Dashboard** tab:

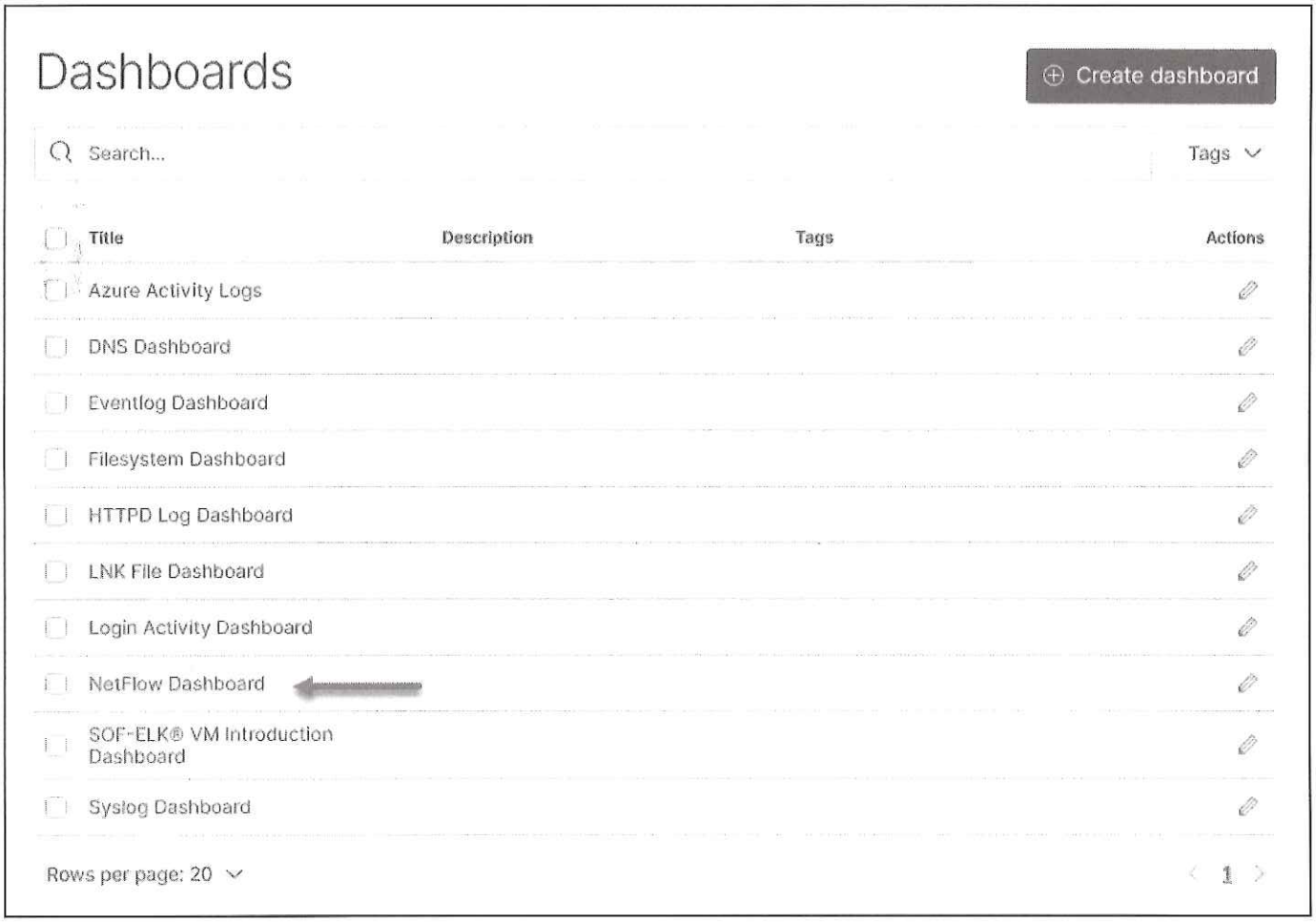


   Click on the word `Dashboard` to get the dashboard menu:

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

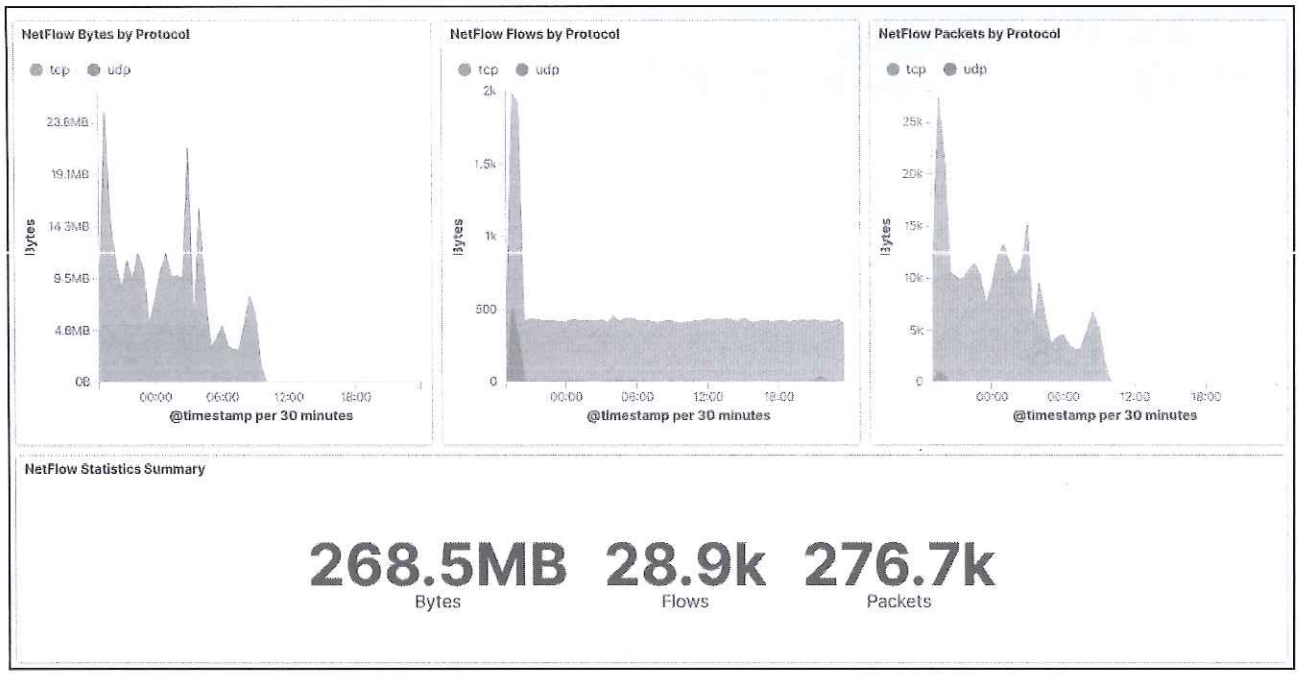


Select the NetFlow dashboard:



During our timeframe, we didn't have much data transferred: only 268.5MB. That being said, if there was data exfiltration, we don't know the size of the files. So far, this is inconclusive.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



Add a filter for our suspect's IP address

```
ips: 85.206.166.82
```



Well that's a bit unexpected: no data exfiltration. The 5 flows are from Luis testing the connection to the cryptomining machines by doing a quick ssh.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

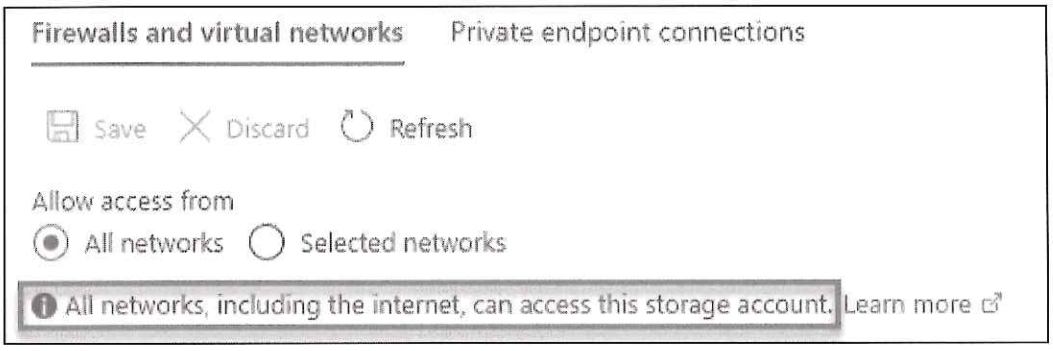
Could data have been exfiltrated to another IP address? To be thorough, look at the destinations in the dashboard (remove the `ips: 85.206.166.82` filter). Go the the panel called `NetFlow Statistics by Destination IP` and click the 3 dots on the top right of the panel to maximize it.

Destination IP	Volume	Packets	Flows
52.252.100.187	77.6MB	20,054	1,042
20.38.105.4	49.5MB	15,181	93
10.1.0.4	41.1MB	82,087	10,654
10.1.0.5	15.4MB	44,798	5,750
52.239.159.84	15MB	8,108	756
52.239.158.234	13.8MB	15,184	1,409
104.214.18.131	12.1MB	27,948	2,166
13.73.242.33	9.5MB	13,602	1,108
20.38.105.6	6.9MB	7,499	750
20.60.140.100	6.3MB	16,861	1,427

If you research all these IPs, you would find that they belong to Microsoft.

Let's step back for a second and think about what a storage account represents. It's storage in the Azure cloud that has its own set of permissions. It's not controlled by the Network Security Group. It doesn't even have an IP address. As such we won't find any data transfer logged in the netflow data.

If you look at the default storage account configuration in the Azure console (network sub-menu), you will see that storage accounts are open to "All networks, including the internet" by default:



3. Where are the logs?

   So, is there really no log of data being transferred from a storage account?

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Actually, there is but it's in preview (Microsoft's equivalent of beta). There are two logs:
- storageread
- storagewrite

We imported the storageread log to the `azure-*` index

Go back to the `Visualize` tab, select `Create visualization`, then `Lens` and make sure your index is set to `azure-*`
Change your graph type to `Data table`
Drag and drop the field called `uri.keyword`
Expand the number of rows

What are the names of the files that were exfiltrated?

- Truth_serum.7z
- Pym_particle.7z
- Quantum_parts_for_sale.7z
- Quantum_tunnel.7z
- Ant_control_helmet.7z
- Quantum_energy.7z
- SHIELD.7z
- Sokovia_Accords.7z
- Quantum_realm.7z
- Avengers_Roster.7z

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Top values of uri.keyword

https://researchlabstore.blob.core.windows.net/secretproject/Truth_serum.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/Pym_particle.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/Quantum_parts_for_sale.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/Quantum_tunnel.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/Ant_control_helmet.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/Quantum_energy.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/SHIELD.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/Sokovia_Accords.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

https://researchlabstore.blob.core.windows.net/secretproject/Quantum_realm.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

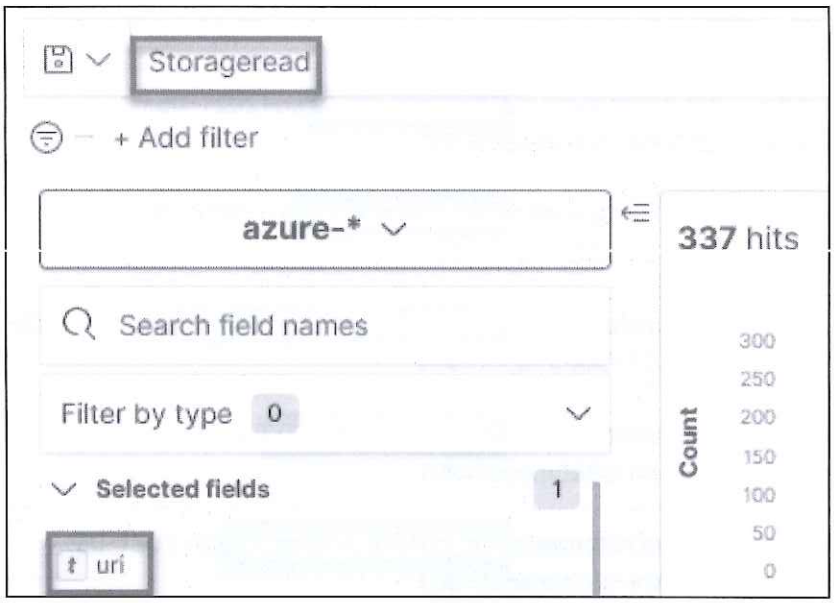
https://researchlabstore.blob.core.windows.net/secretproject/Avengers_Roster.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

What does `secretproject` represent in the uri?

`secretproject` is the name of the container within the `researchlabstore` storage account.

You can verify that by going back to the `Discover` tab and look at the details of one of the records. Use `Storageread` for your search parameter and select the field `uri`

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



Time	uri
2021-04-01 00:04:36.082 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_energy.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
2021-04-01 00:04:31.464 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_realm.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
2021-04-01 00:04:20.878 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_realm.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
2021-04-01 00:04:17.998 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_realm.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
2021-04-01 00:04:17.538 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Avengers_Roster.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
2021-04-01 00:04:16.827 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_realm.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
2021-04-01 00:04:16.256 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_realm.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
2021-04-01 00:04:16.232 +00:00	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_realm.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

t	operation_name	GetBlob
t	ports	9687
t	property_accountname	researchlabstore
t	property_servicetype	blob
t	resource_id	/subscriptions/beb0c5fa-418f-4240-aa63-ff8cad3f1e1b/resourceGroups/labRG/providers/Microsoft.Storage/storageAccounts/researchlabstore/blobServices/default
#	source_ip	85.206.166.83
t	source_port	9687
t	status_text	Success
t	tags	process_archive, filebeat, beats_input_codec_plain_applied, azure_json_storage_log, _geoip_lookup_failure
t	type	azure
t	uri	https://researchlabstore.blob.core.windows.net/secretproject/Quantum_energy.7z?se=2021-05-07T00:01:13Z&sig=XXXXX&sp=rl&sr=c&sv=2020-04-08&timeout=901
t	useragent	Microsoft Azure Storage Explorer 1.18.1, win32, azcopy-node, 2.0.0, win32, AzCopy/10.8.0 Azure-Storage/0.10 (go1.13; Windows_NT)

The detailed record matches everything we would have expected:

- The `operation_name` is `GetBlob` which indicates we downloaded a blob
- The `property_accountname` is `researchlabstore` which is the storage account Luis retreived the keys from
- The `source_ip` is `85.206.166.82` which is our suspicious IP address
- The `status_text` is `success` which indicates a successful data exfiltration
- The `uri` shows the `secretproject` container as well as the file name
- Bonus: we have a `useragent` string that shows us the bad actor used Microsoft Azure Storage Explorer (which is the tool we discussed in class)

Bonus

In the introduction we mentioned that another, more traditional, way to exfiltrate data is from a disk on a VM. Let's examine the logs you can expect if the exfiltration is performed via ftp. There are many paths you can take to search for this information: dashboard, visualize, discover. It's up to you to explore each one.

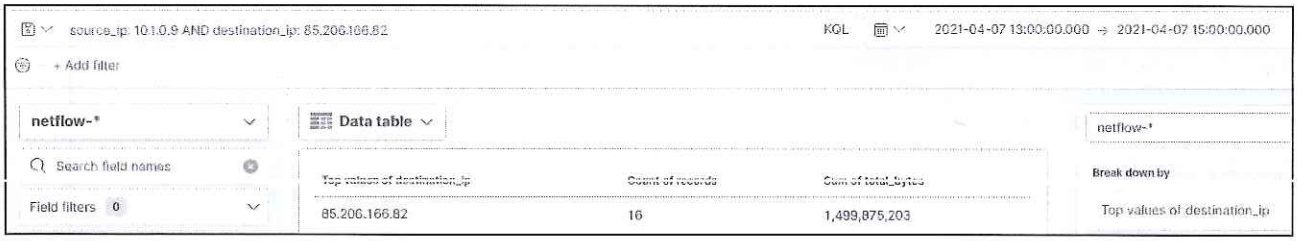
The key elements of your search should be:

Be sure to clear any existing filters and notice the new timeframe

- Timeframe: `2021-04-07 13:00 to 2021-04-07 15:00
- FTP server: `10.1.0.9`
- FTP client: `85.206.166.82`
- Index: `netflow-*`

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

As an example, here is a table (from the `Visualize` tab) showing the data transfer:



Key Takeaways

- Luis was able to retrieve the storage account secret keys because he had access at the subscription level. Whenever possible, limit access to a specific resource group.
- Logging of storage account transfers is very limited and netflow data won't help.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Lab 4.1: GCP IAM and Access Tracking

Objectives

- Understand what is logged within GCP related to user access and what is able to be tracked within the logs.
- How to manipulate GCP IAM and access logs within SOF-ELK.

Background

GCP logs from the Billing, IAM and Resource Manager services have been extracted from the GCP instance that you will use for the rest of the labs in this section. This is an intro to help you understand what user accounts are doing within GCP and how to read some of the logs that you can extract. The logs extracted for this exercise are taken from a specific point in time, in general they aren't very large, however, this may change if you have a very large number of GCP user accounts.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM
3. Access to the SOF-ELK® VM console via the user account `elk_user` and the password `forensics`.
4. Ensure you have completed Lab 0. This is important to ensure the geo tagging for the log data you're about to load into this, and future labs, work correctly.
5. Perform an update of the SOF-ELK configuration by running the following command after you've logged into SOF-ELK:
   `sudo sof-elk_update.sh`
6. Ensure you have loaded the relevant data as described in the next section.
7. Relevant timeframe: `2021-03-15 00:00 to 2021-05-02 00:00 UTC`

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the GCP parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

The GCP JSON logs for this lab have already been exported from Google Logging. To help in keeping the level of data to a reasonable size we have trimmed the data set to only include GCP xxxxxxx Logging. However, there were no other changes made to the JSON that was extracted from GCP so it is still representative of what you'll experience outside of the this course.

The GCP VM Agent Logs have been saved into `/home/elk_user/lab-4.1_source_evidence.zip`.

1. Log on to the SOF-ELK VM with the credentials
   - Username: ***elk_user***
   - Password: ***forensics***

   You may log on to the console, however it's recommended to log in via SSH.
2. Extract the all the `.json` files from the ZIP file above into the their correct LogStash folder for parsing by FileBeats with the following command:

```
cd ~
unzip lab-4.1_source_evidence.zip -d /logstash/gcp/
```

> **Warning**
>
> Do not run this command more than once!

3. Wait 2 minutes for the data to be processed. Once it is complete the data will be available in the `gcp-*` index.

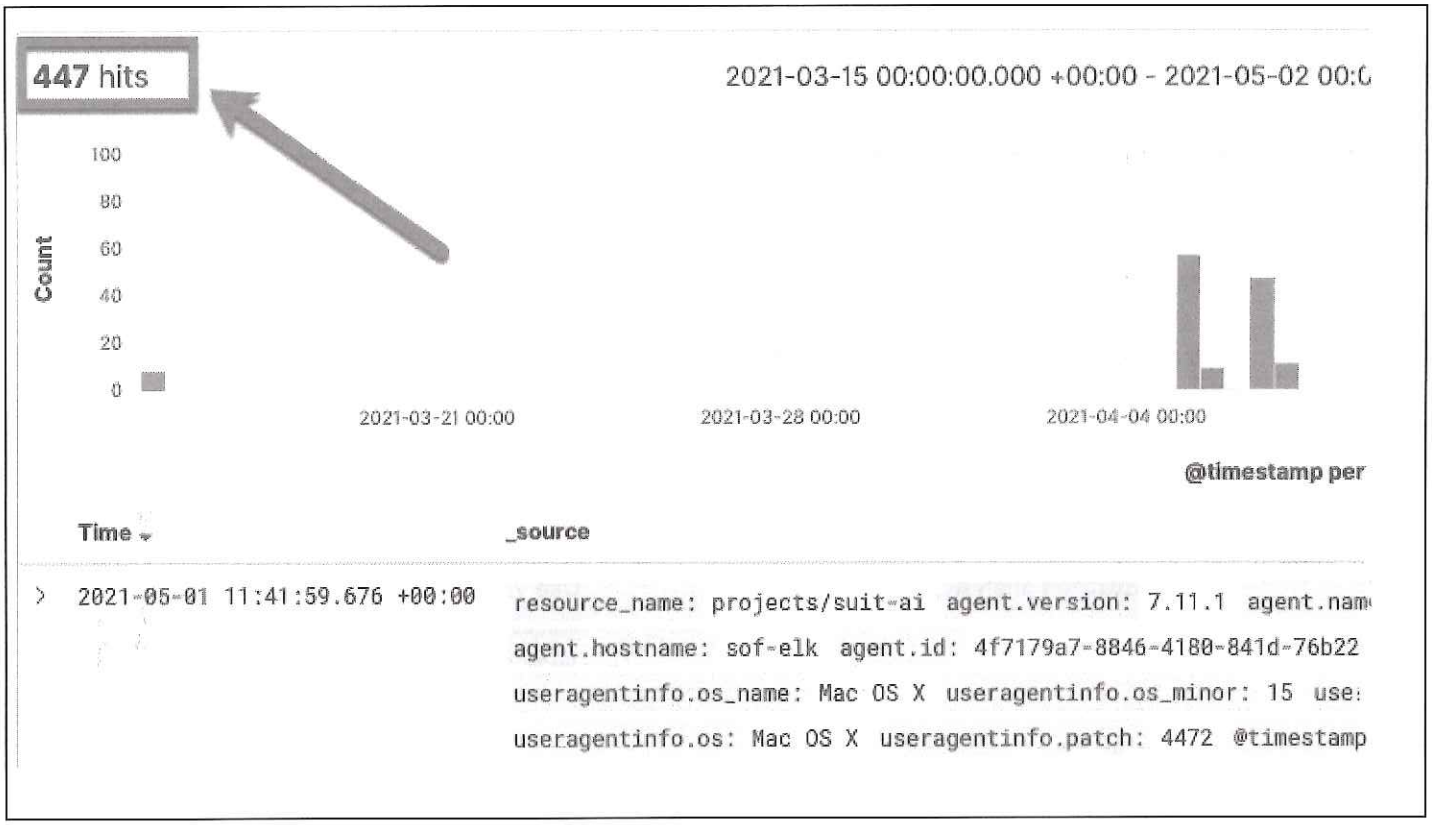
Start in the Discover tab

Before we go too far, let's ensure the date range is correct for the data we'll be using in this lab. Set your search timeframe to `2021-03-15 00:00 to 2021-05-02 00:00 UTC` hit `Update`.

To ensure all your data has loaded correctly, you should now see **447 hits** just above the top right of the histogram.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24



Warning

If you do not see **447 hits** just above the top right of the histogram, you either haven't loaded your data correctly, or you have searches/filters applied that need to be cleared. If you are unable to correct this seek assistance from your instructor before going any further in this lab.

Reviewing Users Within Our Log

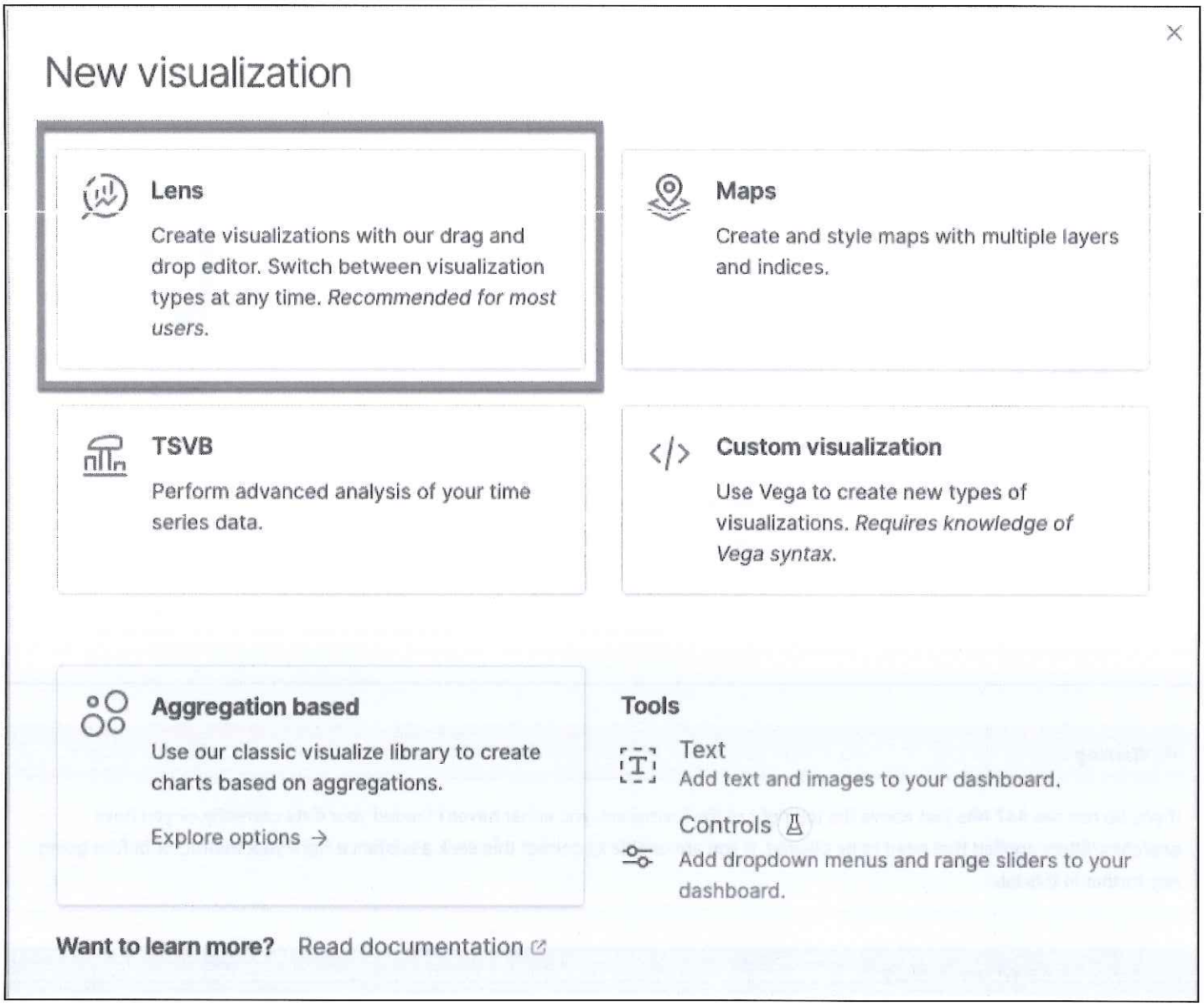
This subsection will be done in the Visualize tab

To start with, let's take a look at the users we have within the logs you have available to search. To do this we will want to generate a summary of all the usernames in the `username` that is parsed out by LogStash.

Move to the `Visualize` tab in Kibana and select `Create visualization`.

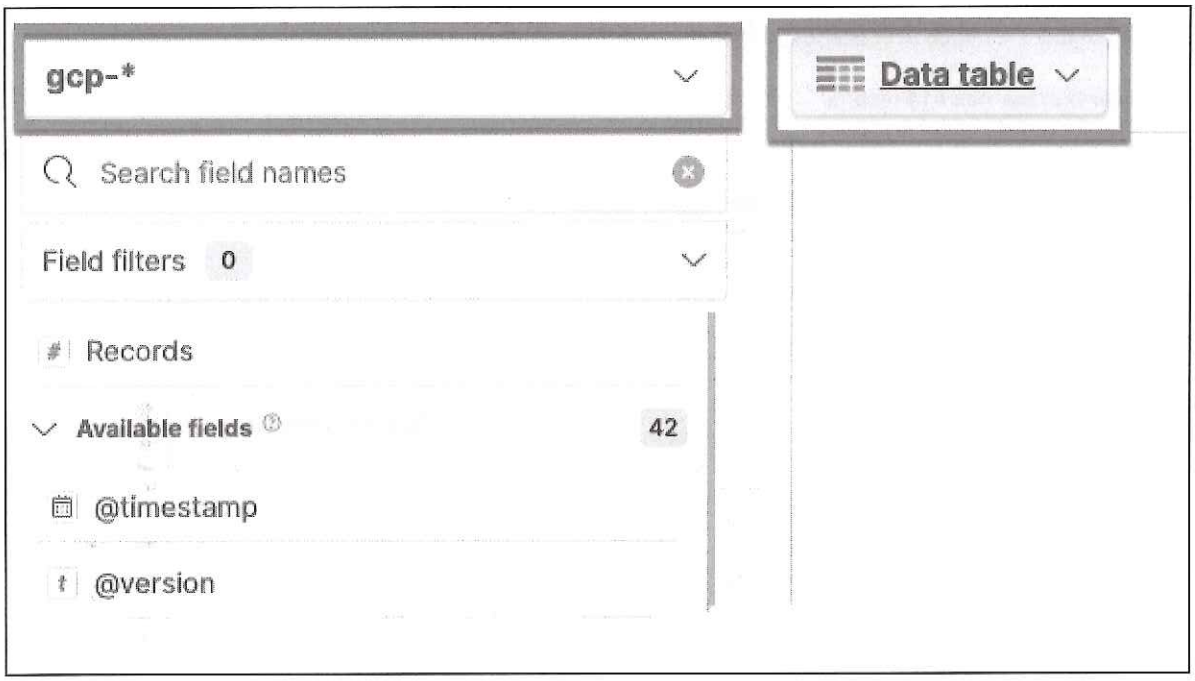
We will use `Lens` as it's the easiest way to create a new visualization.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



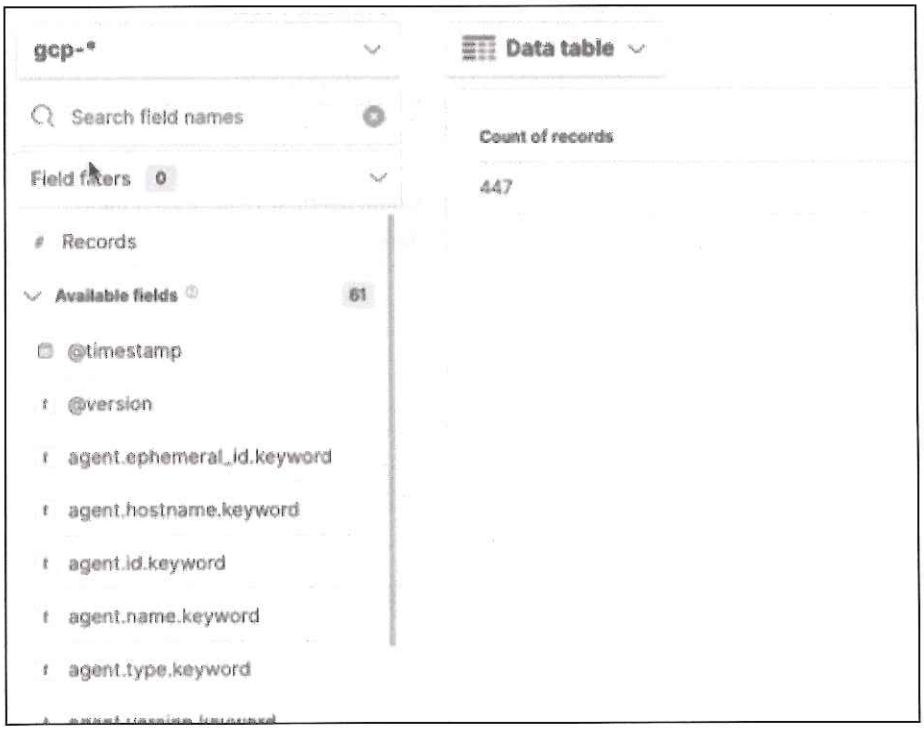
You will need to again move the `index` selector over to `gcp-*` to ensure we are looking at the GCP data. We will also change the graph type to `Data table`

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



The number of available filters may differ after you have performed a `sof-elk_update.sh` *as we continue to parse more fields over time.*

Drag and drop the `username.keyword` field into the table area.

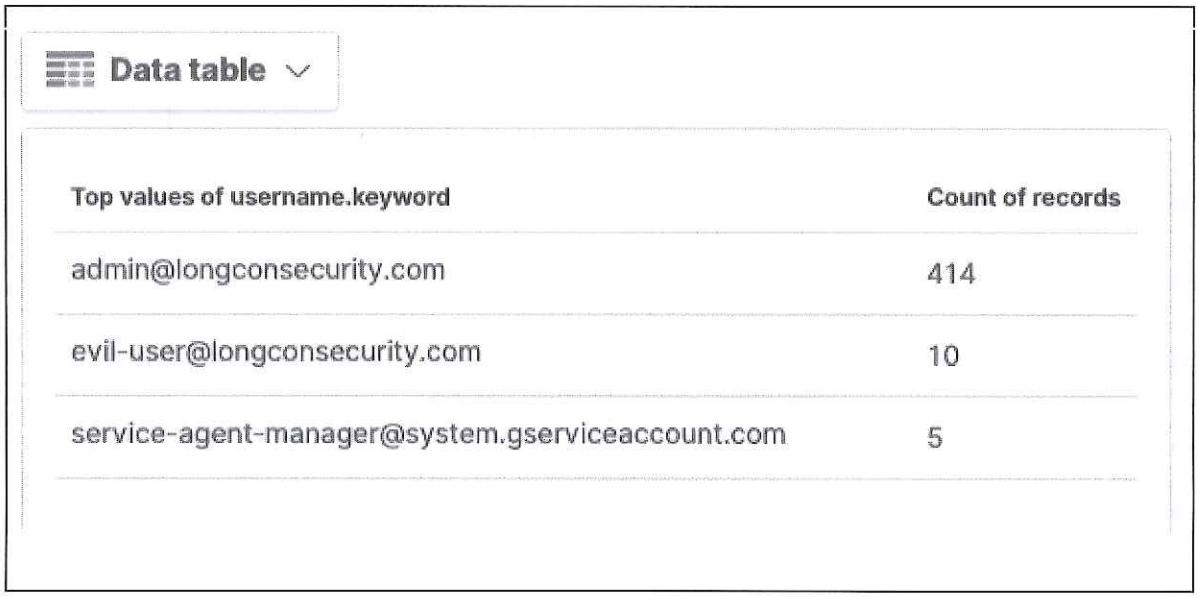


1. Based on the table that is created inside of the Lens Visualize, we can see the users accounts and the number of records available for each user account.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

How many records are there for each user account within the logs you have just summarized with Lens Visualize?

- `admin@longconsecurity.com` has **414** records
- `evil-user@longconsecurity.com` has **10** records
- `service-agent-manager@system.gserviceaccount.com` has **5** records



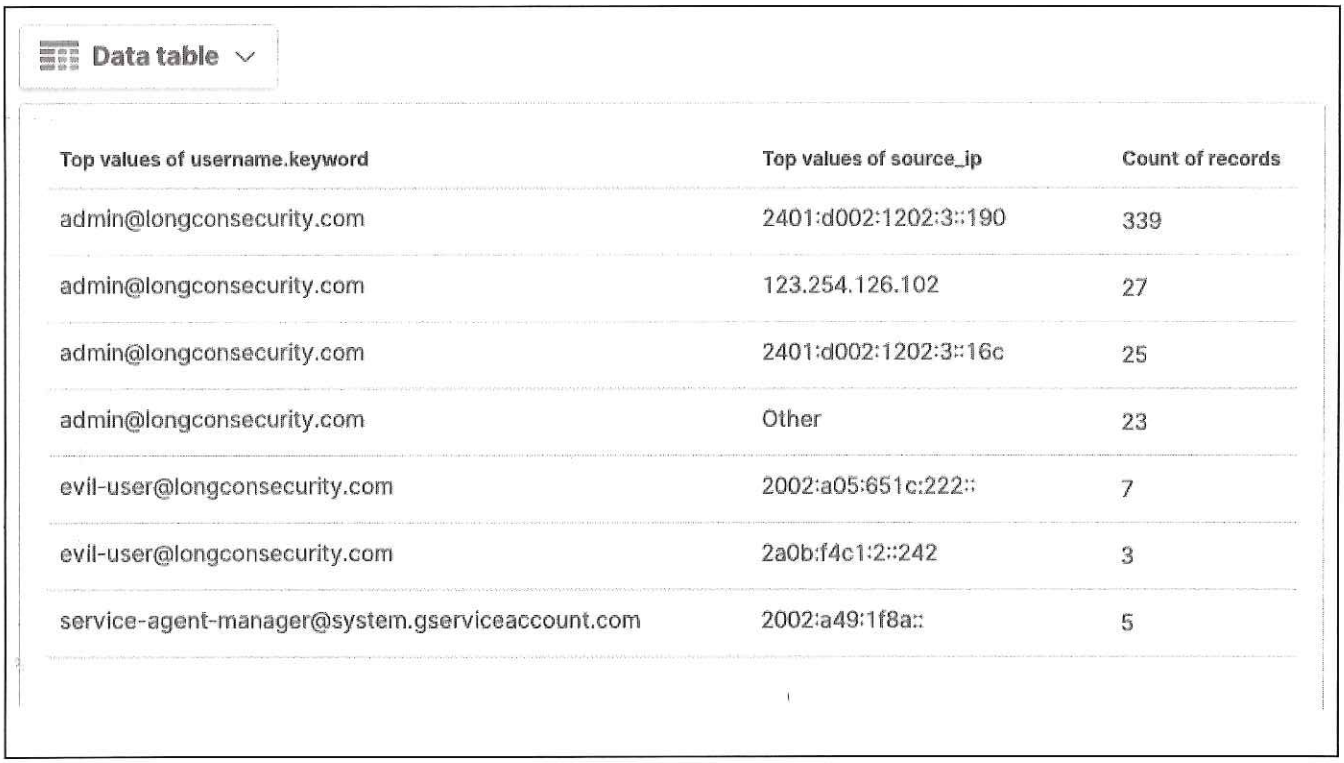
Top values of username.keyword	Count of records
admin@longconsecurity.com	414
evil-user@longconsecurity.com	10
service-agent-manager@system.gserviceaccount.com	5

2. One last thing that maybe of use later on - drag and drop the `source_ip` field into the table as well.

Based on the updated summary table, is there any overlap in the source IP addresses of where the user accounts were being accessed?

No, there doesn't appear to be any overlap in the IP addresses for the different users. Individual users have accessed their account from different locations, but there is no overlap in the source IP addresses for different accounts.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



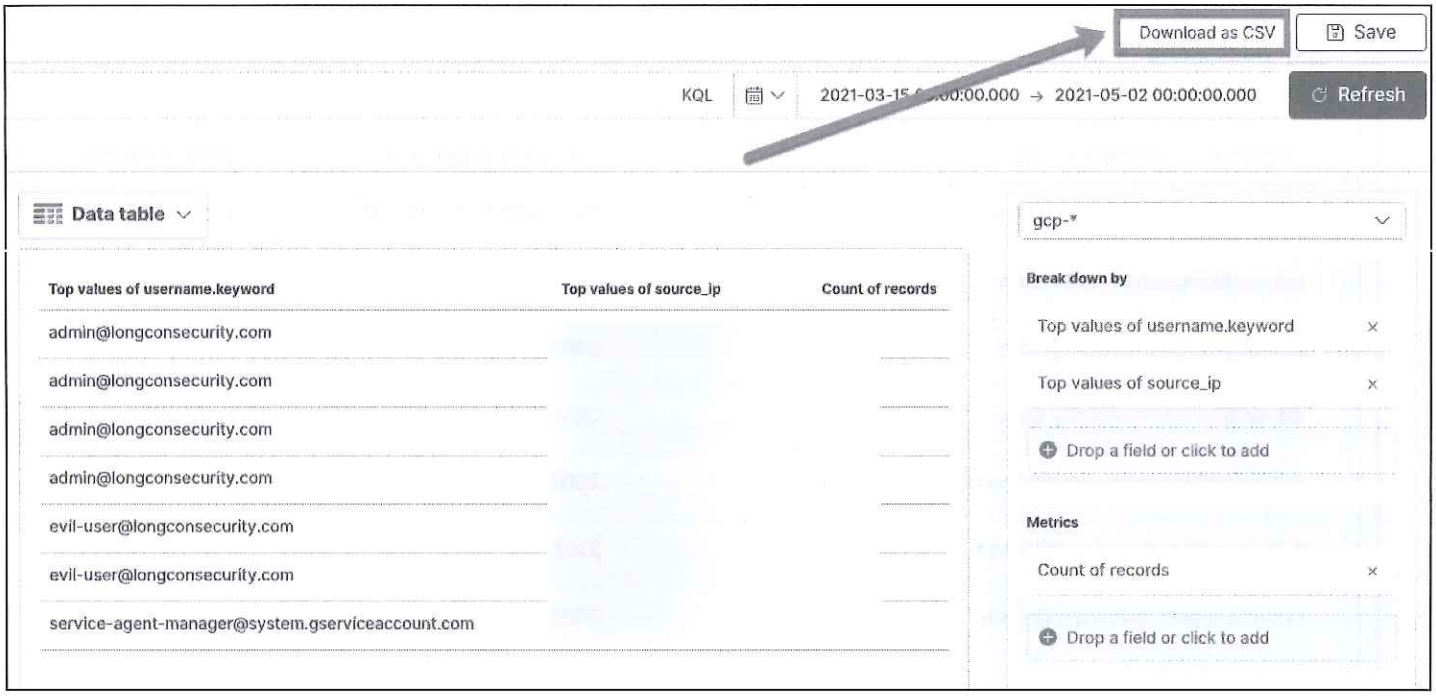
Top values of username.keyword	Top values of source_ip	Count of records
admin@longconsecurity.com	2401:d002:1202:3::190	339
admin@longconsecurity.com	123.254.126.102	27
admin@longconsecurity.com	2401:d002:1202:3::16c	25
admin@longconsecurity.com	Other	23
evil-user@longconsecurity.com	2002:a05:651c:222::	7
evil-user@longconsecurity.com	2a0b:f4c1:2::242	3
service-agent-manager@system.gserviceaccount.com	2002:a49:1f8a::	5

You will notice that there is a mix of both IPv4 and IPv6 addresses as the source IP addresses. This isn't a mistake, it's the legitimate activity of our users in the GCP using native IPv6.

You may want to export the data that you just created to answer the last question. This may become useful later, however, it's also a very common task that you'd want to do when investigating user access so you have a record of where your users were accessing their GCP accounts from.

To export the data from the Visualize Table click on `Download as CSV` in the top right of the screen.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



Now that we have an understanding of the user accounts that are within the logs, let's move back

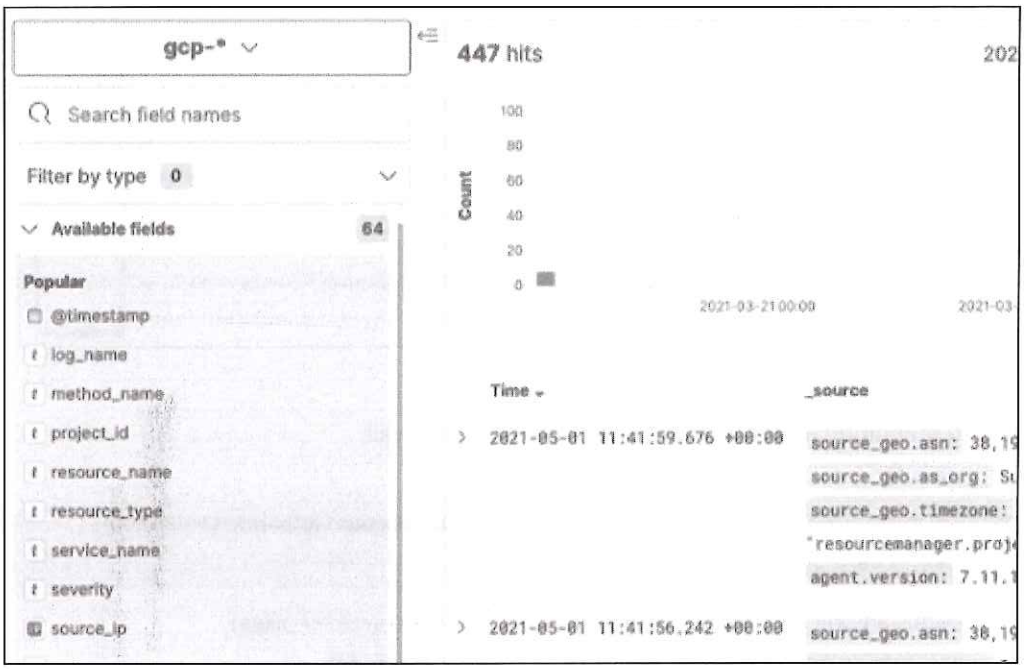
Reviewing User Activity

Move back into the Discover tab

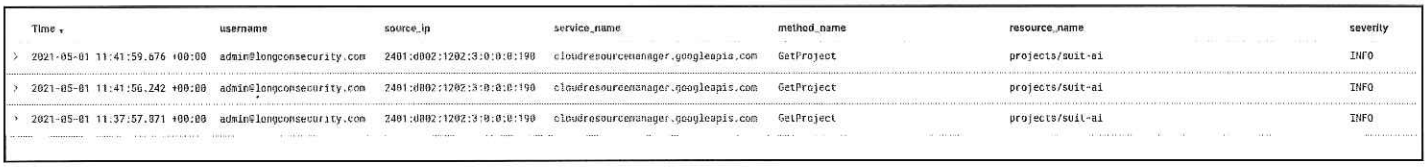
The initial view of the data within the Discovery view of SOF-ELK is very unstructured to begin with. The first few steps in this exercise we will add in specific columns to make the data more useful for reviewing GCP VM Agent Logs. We will want to add in the following column names: - `username` - `source_ip` - `service_name` - `method_name` - `resource_name` - `severity`

To add in these names you can search for them in the field selector under the index drop down menu. When you start typing the field name it will appear for you to select with + that will appear when you hover your mouse over the field name.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Provided you added the fields in the order above, your events in Discovery should now appear similar to the below image.



There are a three different `service_name` items in the logs, let's start with looking at the only the `iam.googleapis.com` log.

1. Run a search for all of the `service_name: iam.googleapis.com` logs and review the output.

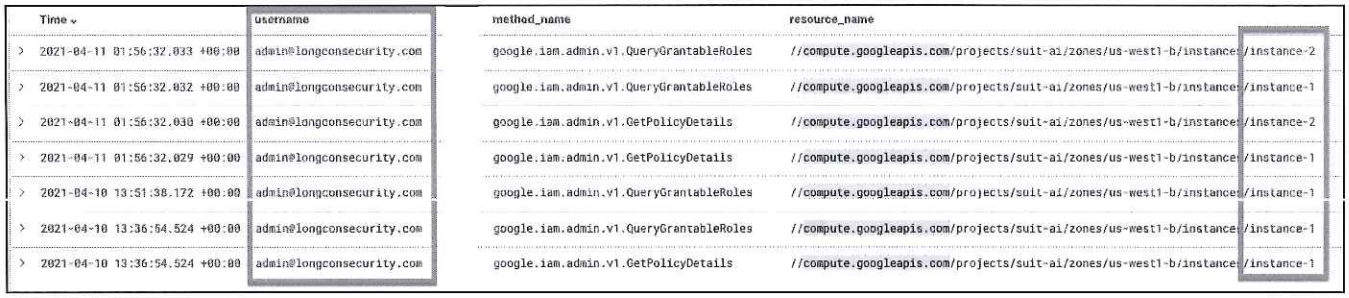
As you scroll through the data you will notice that there are a lot of entries related a `resource_name` that include the term `subnetworks`. These are the VPC resources within GCP that we will look at later in this section of the class.

1. Exclude all the VPC resources from you search by updating you search bar to be: `service_name: iam.googleapis.com AND NOT resource_name : "subnetworks"`. This should now leave you with a more manageable data set to look at.

> **Looking at the IAM events, there are interactions with two (2) VM instances (compute resources). Which user account interacted with them and what were the names of the VM's?**
>
> To answer this question you will need to narrow you search even further by appending `AND resource_name: *compute*` to your current search. This will allow you to only see IAM events that involved the **compute** resource within GCP.
>
> You will see that the `admin@longconsecurity.com` user interacted with two compute resources, they were:
>
> - compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

- compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-2



Time	username	method_name	resource_name
2021-04-11 01:56:32.033 +00:00	admin@longconsecurity.com	google.iam.admin.v1.QueryGrantableRoles	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-2
2021-04-11 01:56:32.032 +00:00	admin@longconsecurity.com	google.iam.admin.v1.QueryGrantableRoles	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1
2021-04-11 01:56:32.030 +00:00	admin@longconsecurity.com	google.iam.admin.v1.GetPolicyDetails	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-2
2021-04-11 01:56:32.029 +00:00	admin@longconsecurity.com	google.iam.admin.v1.GetPolicyDetails	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1
2021-04-10 13:51:38.172 +00:00	admin@longconsecurity.com	google.iam.admin.v1.QueryGrantableRoles	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1
2021-04-10 13:36:54.524 +00:00	admin@longconsecurity.com	google.iam.admin.v1.QueryGrantableRoles	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1
2021-04-10 13:36:54.524 +00:00	admin@longconsecurity.com	google.iam.admin.v1.GetPolicyDetails	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1

2. We can also use the same searching technique to look for other GCP resources as well.

Looking at the IAM events, there are interactions with storage resources. Which user account interacted with them, what storage type was it, and the names storage locations?

You can alter your search from the previous answer to include `storage` this would look like `service_name: iam.googleapis.com AND NOT resource_name : "subnetworks" AND resource_name: *storage*`.

You will again see that the `admin@longconsecurity.com` user interacted with storage `buckets` named:

- confidential_plans
- flight-maps



Time	username	resource_name
2021-04-26 12:54:00.067 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/confidential_plans
2021-04-26 12:54:00.066 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/confidential_plans
2021-04-26 12:00:33.638 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/confidential_plans
2021-04-26 12:00:21.563 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/confidential_plans
2021-04-26 12:00:21.560 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/confidential_plans
2021-04-26 11:22:10.459 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/confidential_plans
2021-04-26 11:22:10.288 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/confidential_plans
2021-04-13 04:14:51.715 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/flight-maps
2021-04-13 01:32:59.865 +00:00	admin@longconsecurity.com	//storage.googleapis.com/projects/_/buckets/flight-maps

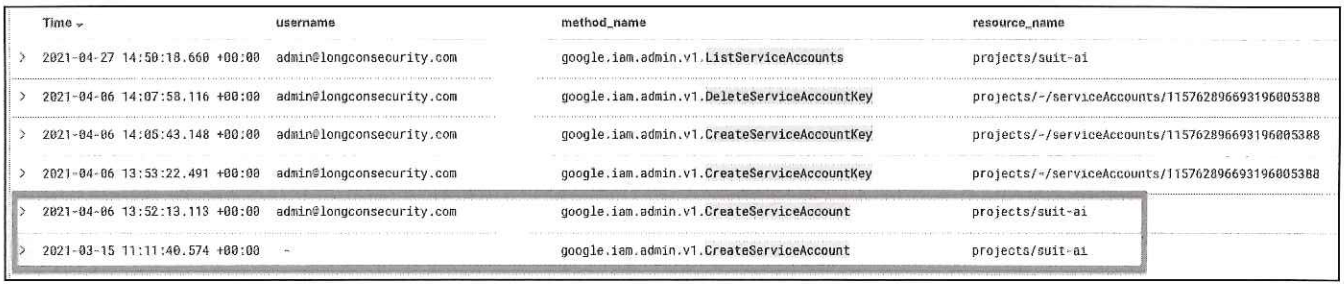
3. Let's move back to our original search so we can see all the IAM events: `service_name: iam.googleapis.com AND NOT resource_name : "subnetworks"` and review Service Account tracking.
4. When you scroll through the IAM logs you will notice there `method_name` items that include the word "service". Let's take a closer look at those events.

Are there any `CreateServiceAccount` events, and if so, what are there `Account_Email` and their `account_ID` values

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Yes, there are two `CreateServiceAccount` events in our logs. To find them you will need to search for `service_name: iam.googleapis.com AND NOT resource_name : "subnetworks" AND method_name : *Service*`.



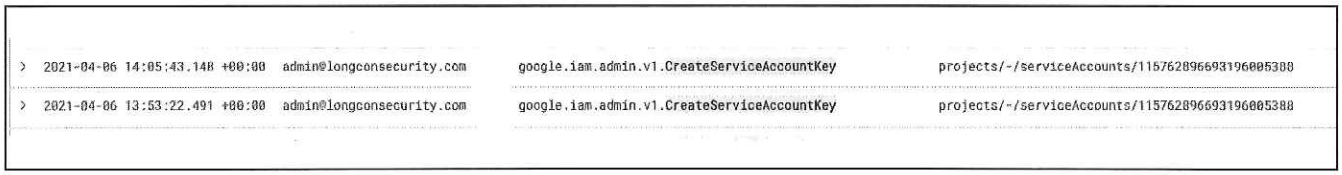
Time	username	method_name	resource_name
2021-04-27 14:50:18.660 +00:00	admin@longconsecurity.com	google.iam.admin.v1.ListServiceAccounts	projects/suit-ai
2021-04-06 14:07:58.116 +00:00	admin@longconsecurity.com	google.iam.admin.v1.DeleteServiceAccountKey	projects/-/serviceAccounts/115762896693196005388
2021-04-06 14:05:43.148 +00:00	admin@longconsecurity.com	google.iam.admin.v1.CreateServiceAccountKey	projects/-/serviceAccounts/115762896693196005388
2021-04-06 13:53:22.491 +00:00	admin@longconsecurity.com	google.iam.admin.v1.CreateServiceAccountKey	projects/-/serviceAccounts/115762896693196005388
2021-04-06 13:52:13.113 +00:00	admin@longconsecurity.com	google.iam.admin.v1.CreateServiceAccount	projects/suit-ai
2021-03-15 11:11:40.574 +00:00	-	google.iam.admin.v1.CreateServiceAccount	projects/suit-ai

To determine the `Account_Email` and their `account_ID` values you need to expand out each event individually. You will find both of these values beside each other.

- `486497620 25-compute@developer.gserviceaccount.com` and `100820242691295494244`
- `sof-elk-srv-account@suit-ai.iam.gserviceaccount.com` and `115762896693196005388`

There are also `CreateServiceAccountKey` events in the previous search that was run, which account were the keys created for?

The two `CreateServiceAccountKey` events both have the `resource name` value of `projects/-/serviceAccounts/115762896693196005388`. So the keys were created against the Service Account with an ID of `115762896693196005388`.



2021-04-06 14:05:43.148 +00:00	admin@longconsecurity.com	google.iam.admin.v1.CreateServiceAccountKey	projects/-/serviceAccounts/115762896693196005388
2021-04-06 13:53:22.491 +00:00	admin@longconsecurity.com	google.iam.admin.v1.CreateServiceAccountKey	projects/-/serviceAccounts/115762896693196005388

You can match this Service Account ID back to the ID's you identified in the previous question. Once you do this it will match to `sof-elk-srv-account@suit-ai.iam.gserviceaccount.com`. Additionally, we can also see the user that create the Service Account Keys, `admin@longconsecurity.com`.

Within GCP logs it's common to find the resource names referenced by their unique ID. This is because you can have resource names with the same text in different projects. For example, you could have two VMs with the "Super Smart VM" sitting in two different projects, but because they would appear in the same logs for the organization, it's always good to be familiar with object IDs.

Filtering Clean Up

Ensure you clear out any filters you may still have applied for this lab, this will ensure your next lab isn't impacted by any filters you used in this lab.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Key Takeaways

- The ability to quickly understand what users are in GCP IAM and access logs.
- Understand that GCP logs don't always include the human readable name given to an object, along with the ability to be able to match a Resource ID back to a human readable name.
- The ability to quickly narrow down IAM logs to search for relevant information related to access or actions performed by a user within GCP.

https://t.me/learningnets

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Lab 4.2: Google VM Logging Agent - Agent Log Analysis

Objectives

- Understand the capabilities of Google Logging Agent.
- Develop an understanding of how to use Google Logging Agent logs within SOF-ELK. _ Understand how to identify different log sources from a host and how they are useful to an investigation.

Background

LongConSecurity have three VM's within a VPC that have GCP's host based Agent Logging installed on them. These were installed with the default commands wihtin GCP and were pushed to the VM's by GCP Monitoring with Google Shell commands.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM
3. Access to the SOF-ELK® VM console via the user account `elk_user` and the password `forensics`.
4. Perform an update of the SOF-ELK configuration by running the following command after you've logged into SOF-ELK:
   `sudo sof-elk_update.sh`
5. Ensure you have loaded the relevant data as described in the next section.
6. Relevant timeframe: `2021-04-10 00:00` to `2021-05-01 00:00` UTC

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the GCP parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

The GCP JSON logs for this lab have already been exported from Google Logging. To help in keeping the level of data to a reasonable size we have trimmed the data set to only include GCP VM Agent Logging. However, there were no other changes made to the JSON that was extracted from GCP so it is still representative of what you'll experience outside of the this course.

The GCP VM Agent Logs have been saved into `/home/elk_user/lab-4.2_source_evidence.zip`.

1. Log on to the SOF-ELK VM with the credentials
   - Username: ***elk_user***
   - Password: ***forensics***

   You may log on to the console, however it's recommended to log in via SSH.
2. Extract the all the `.json` files from the ZIP file above into the their correct LogStash folder for parsing by FileBeats with the following command:

```
cd ~
unzip lab-4.2_source_evidence.zip -d /logstash/gcp/
```

> ⚠ **Warning**
>
> Do not run this command more than once!

3. Wait 2 minutes for the data to be processed. Once it is complete the data will be available in the `gcp-*` index.

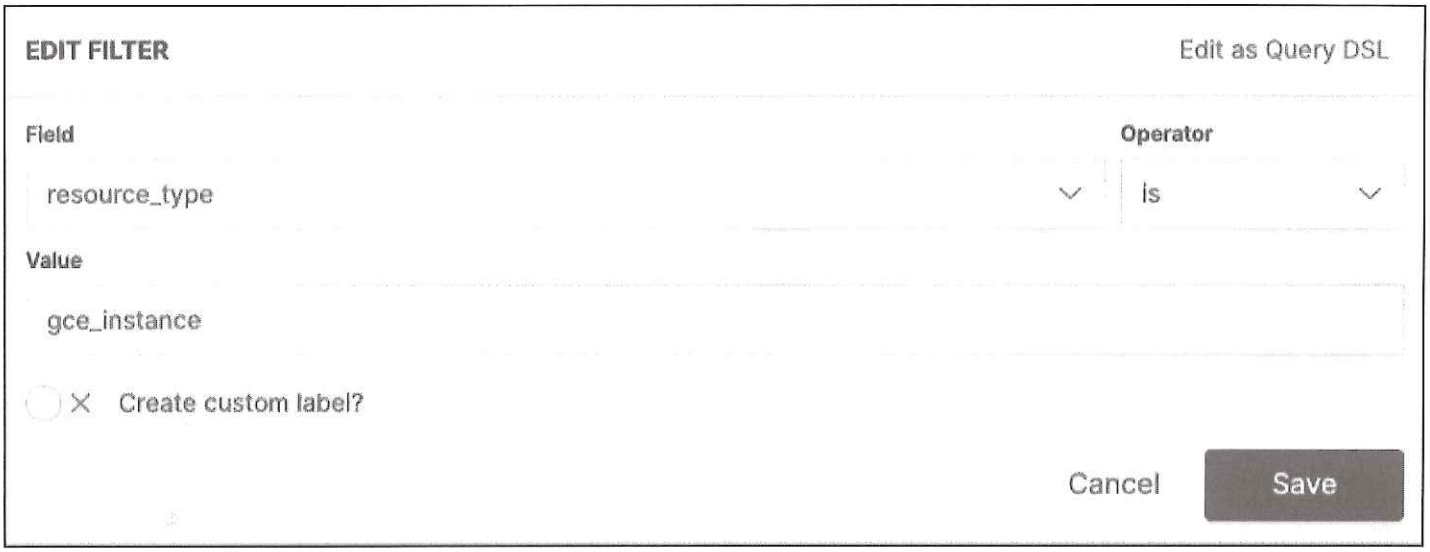
Lab Content

Start in the Discover tab

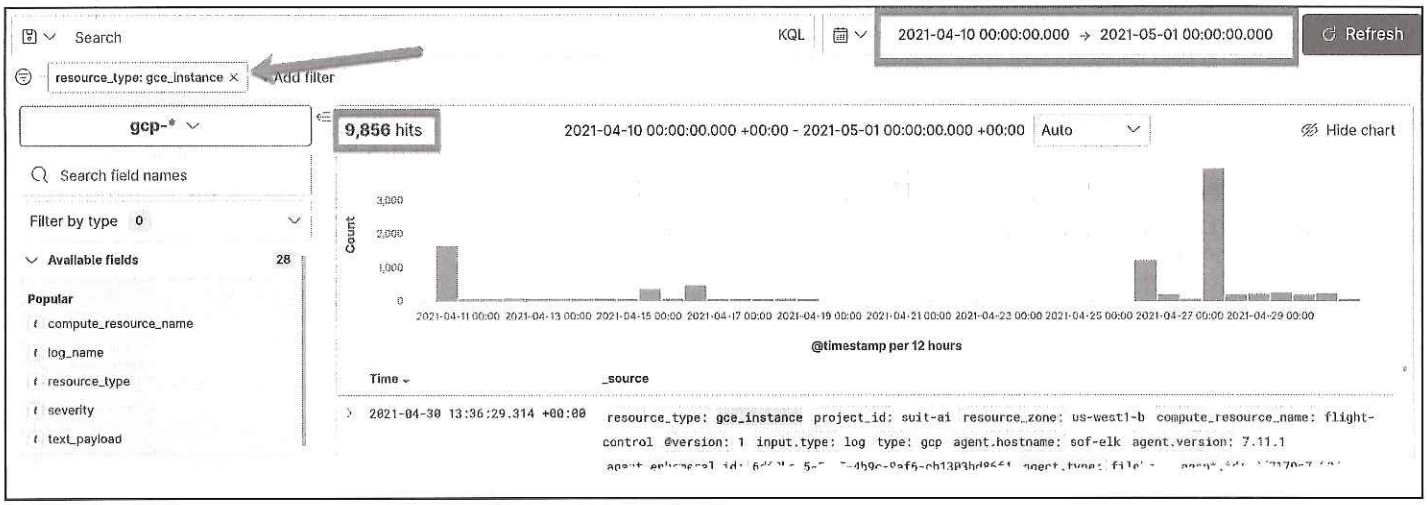
Before we go too far, let's ensure the date range is correct for the data we'll be using in this lab. Set your search timeframe to `2021-04-10 00:00` to `2021-05-01 00:00` UTC hit `Update`. As you may be jumping between different exercises, let's also narrow down the logs we're looking at with "Add filter", select the `Field` to be `resource_type`, set the `Operator` to be `is`, then set the `Value` to be `gce_instance`.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24



Based on this timeframe and filter you just applied, you should see **9,856 hits** or entries in your histogram.

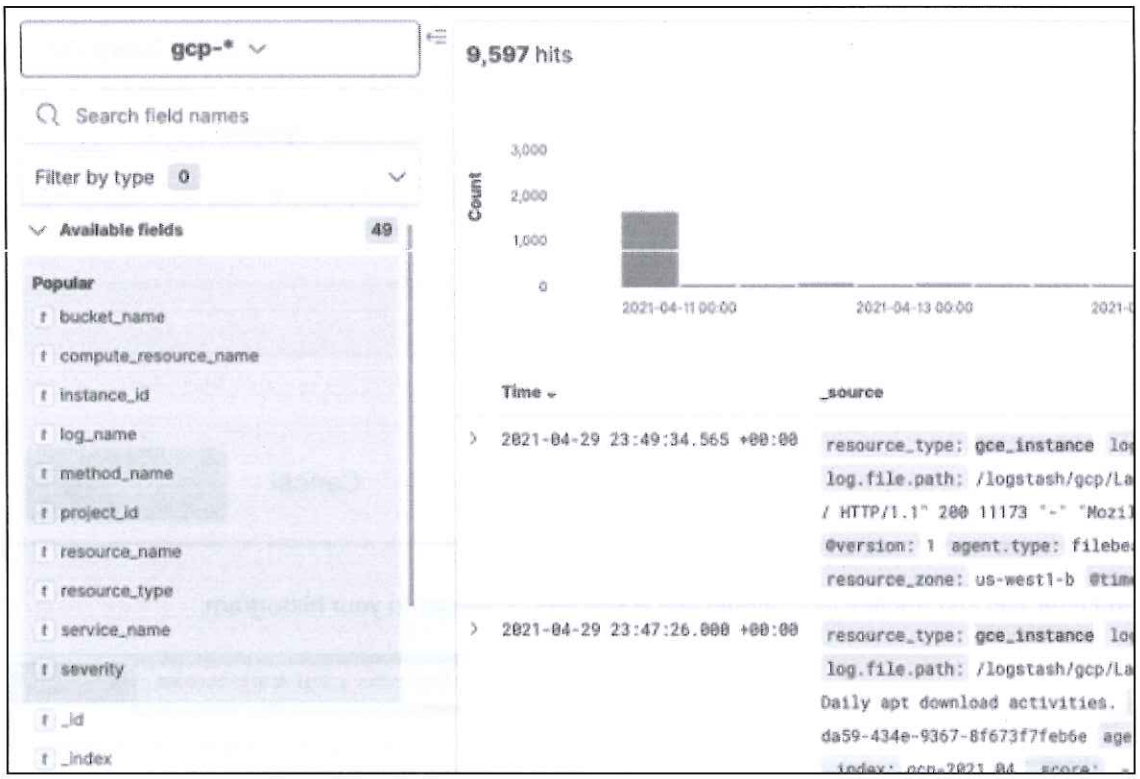


The initial view of the data within the Discovery view of SOF-ELK is very unstructured to begin with. The first few steps in this exercise we will add in specific columns to make the data more useful for reviewing GCP VM Agent Logs. We will want to add in the following column names:

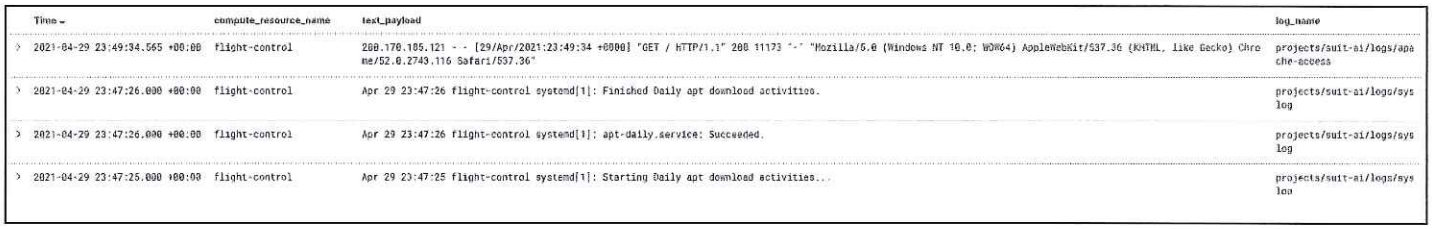
- `compute_resource_name`
- `text_payload`
- `log_name`

To add in these names you can search for them in the field selector under the index drop down menu. When you start typing the field name it will appear for you to select with + that will appear when you hover your mouse over the field name.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



Provided you added the fields in the order above, your events in Discovery should now appear similar to the below image.



Time	compute_resource_name	text_payload	log_name
2021-04-29 23:49:34.565 +00:00	flight-control	200.170.105.121 - - [29/Apr/2021:23:49:34 +0000] "GET / HTTP/1.1" 200 11173 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"	projects/suit-ai/logs/apache-access
2021-04-29 23:47:26.000 +00:00	flight-control	Apr 29 23:47:26 flight-control systemd[1]: Finished Daily apt download activities.	projects/suit-ai/logs/syslog
2021-04-29 23:47:26.000 +00:00	flight-control	Apr 29 23:47:26 flight-control systemd[1]: apt-daily.service: Succeeded.	projects/suit-ai/logs/syslog
2021-04-29 23:47:25.000 +00:00	flight-control	Apr 29 23:47:25 flight-control systemd[1]: Starting Daily apt download activities...	projects/suit-ai/logs/syslog

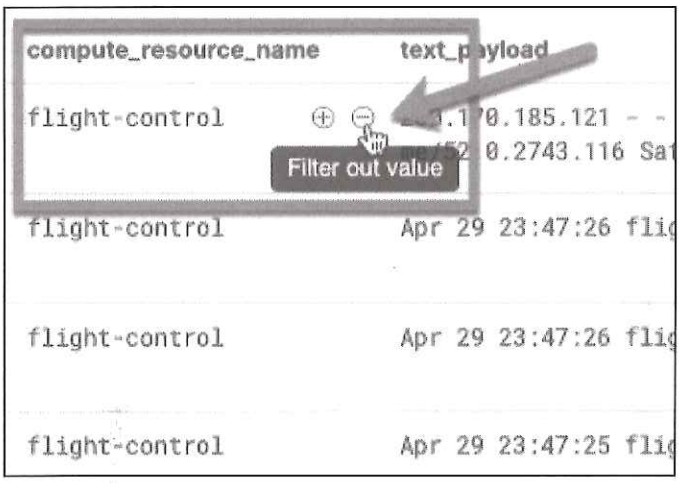
We're now ready to start our GCP VM Agent Logs.

Reviewing Available Logs

1. The logs we collected by the GCP VM Agent can vary depending on what services are running on each VM. Within the log set for this Lab you have three different VM's to explore. Let's start off by simply understanding the logs we have to work with.

> **What are the 'instance IDs' and 'instance names' of the three systems that we have logs for within the data?**
>
> One of the field's we had you add to the Discovery event view earlier will provide you with this information. The `compute_resource_name` is the label given to the VM's by the person that created them.
>
> You can start by recording the names of the systems, then slowly excluding them from the search with a filter.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



This should result in you identifying three system; `flight-control` that has an ID of `6555761934034736853`, `comms-control` that has an ID of `3062874549292210690`, and `instance-1` with an ID of `651533120232493846`.

2. You will also notice from the previous question there were a number of events that did not have an 'instance name' but they did have an 'instance ID'. Within GCP the correct way to refer to a rescues is via its ID. To keep things simple in this Lab we will continue to us the 'instance name' unless we need to review logs that don't contain this field.

> **When did logs start and stop for each of the three systems?**
>
> Logs for `flight-control` started on `2021-04-27 19:33:28.000 UTC` and finished on `2021-04-29 23:49:34.565 UTC`
>
> Logs for `comms-control` started on `2021-04-27 15:29:47.000 UTC` and finished on `2021-04-29 23:37:47.415 UTC`
>
> Logs for `instance-1` started on `2021-04-16 06:40:23.000 UTC` and finished on `2021-04-18 12:47:05.461 UTC`
>
> The most accurate way to search for each of these is using the instance_id for each of the system you identified in the preivous question. An example of this for `instance-1` would be `instance_id : "651533120232493846"`

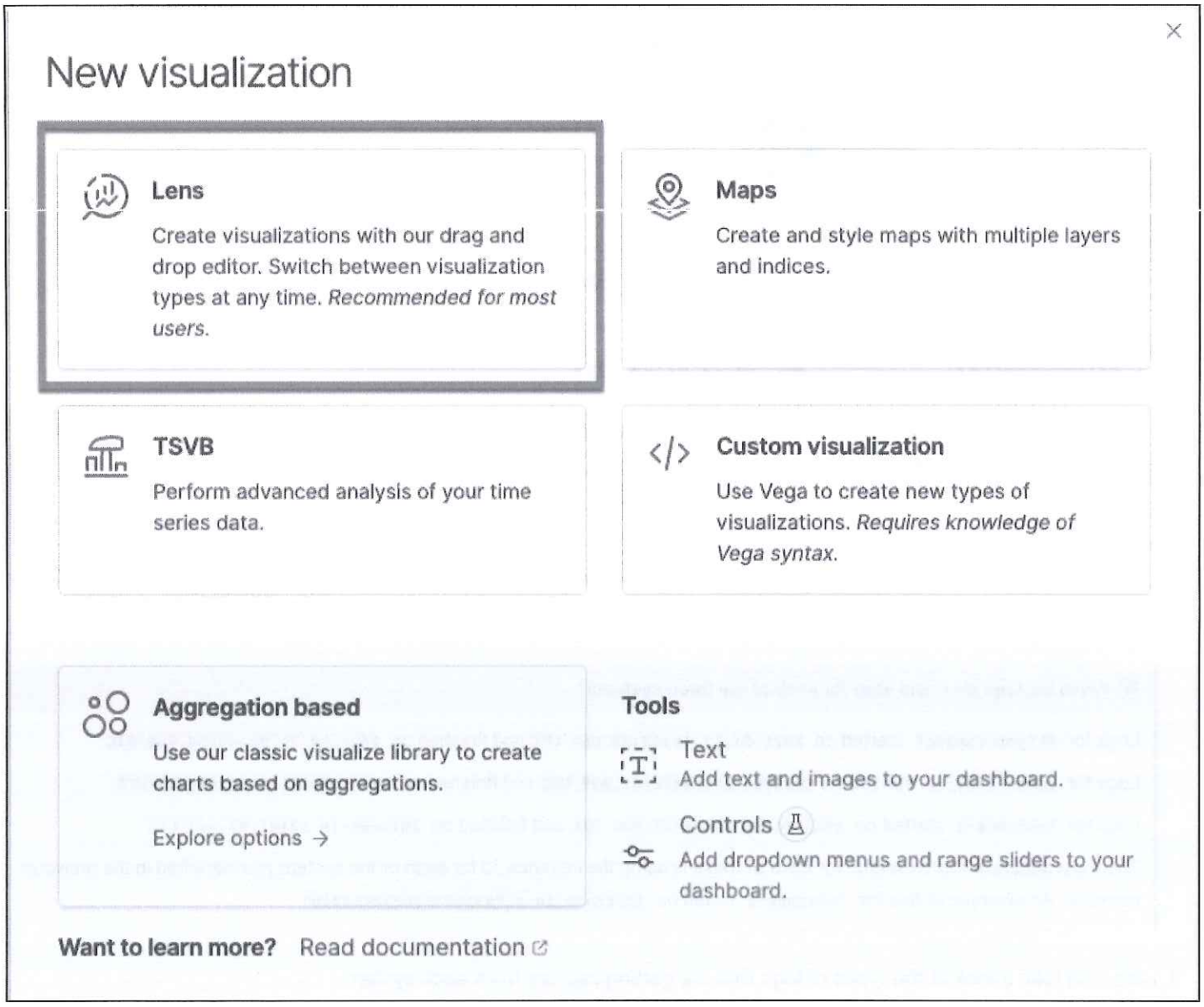
3. Let's now take a look at the types of logs that are getting capture from each system.

This question will be answered in the Visualize tab

Move to the `Visualize` tab in Kiabana and select `Create visualization`.

We will use `Lens` as it's the easiest way to create a new visualization.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

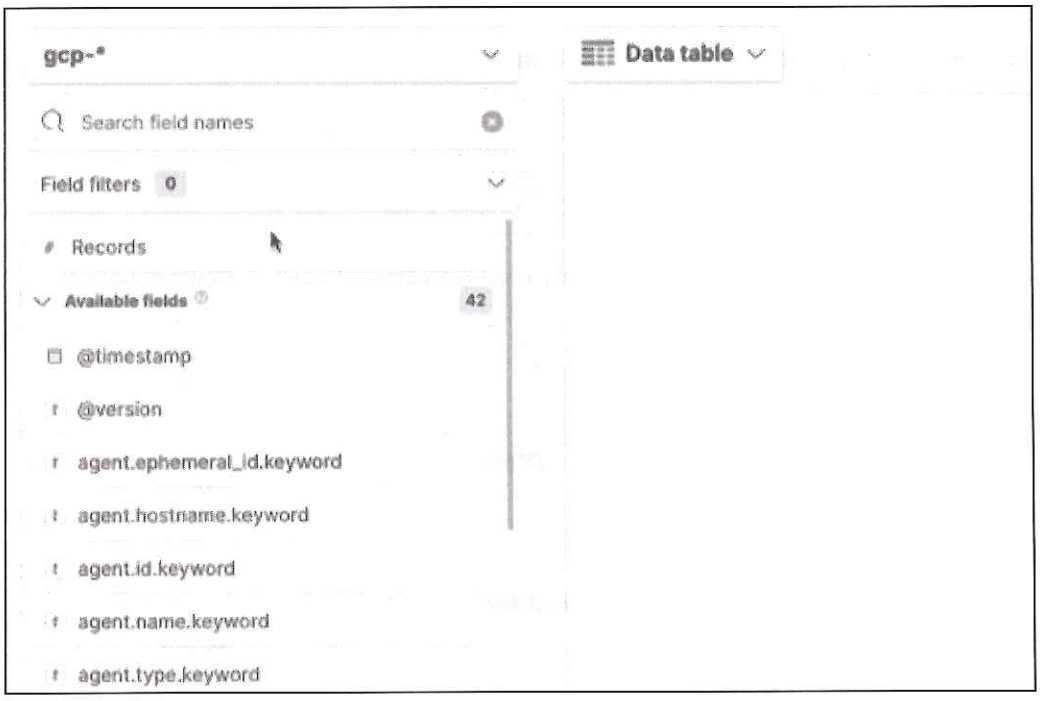


You will need to again move the `index` selector over to `gcp-*` to ensure we are looking at the GCP data. We will also change the graph type to `Data table`

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Drag and drop the `log_name.keyword` field into the table area.



Based on the table that is created inside of the Lens Visualize, we can see there all the log types available.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Top values of log_name.keyword	Count of records
projects/suit-ai/logs/syslog	9,200
projects/suit-ai/logs/apache-access	527
projects/suit-ai/logs/cloudaudit.googleapis.com%2Fdata_access	167
projects/suit-ai/logs/compute.googleapis.com%2Fshielded_vm_integrity	58
projects/suit-ai/logs/GCEGuestAgent	27
Other	49

Of interest to us as investigators are the `projects/suit-ai/logs/syslog`, which are simply the `syslog` output from each VM, and the `projects/suit-ai/logs/apache-access` which are the `apache-access` logs from `Apache2` on the VM's.

1. To further understand which VM's are running Apache2 we could also drag over the `compute_resource_name.keyword`.

What systems were producing `Apache2` logs?

Top values of log_name.keyword ↑	Top values of compute_resource_name.keyword	Count of records
Other	flight-control	16
Other	comms-control	10
projects/suit-ai/logs/apache-access	flight-control	289
projects/suit-ai/logs/apache-access	comms-control	238
projects/suit-ai/logs/syslog	instance-1	3,296
projects/suit-ai/logs/syslog	comms-control	2,998
projects/suit-ai/logs/syslog	flight-control	2,906

We can now see from the table that both the `flight-controller` and `comms-control` systems were logging `apache-access` logs.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

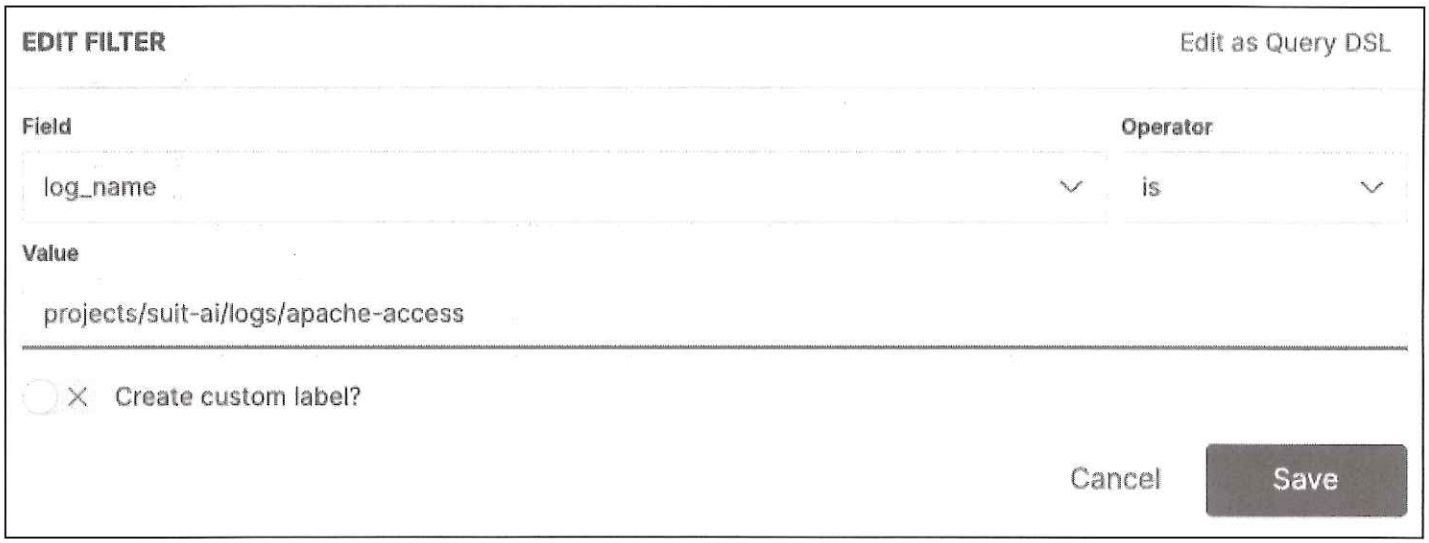
Reviewing Apache Access Logs

1. What was occurring on the systems with Apache Access logs running?

This question will be answered in the Discover tab

Move to the `Discover` tab in Kiabana where we'll run the rest of our searches.

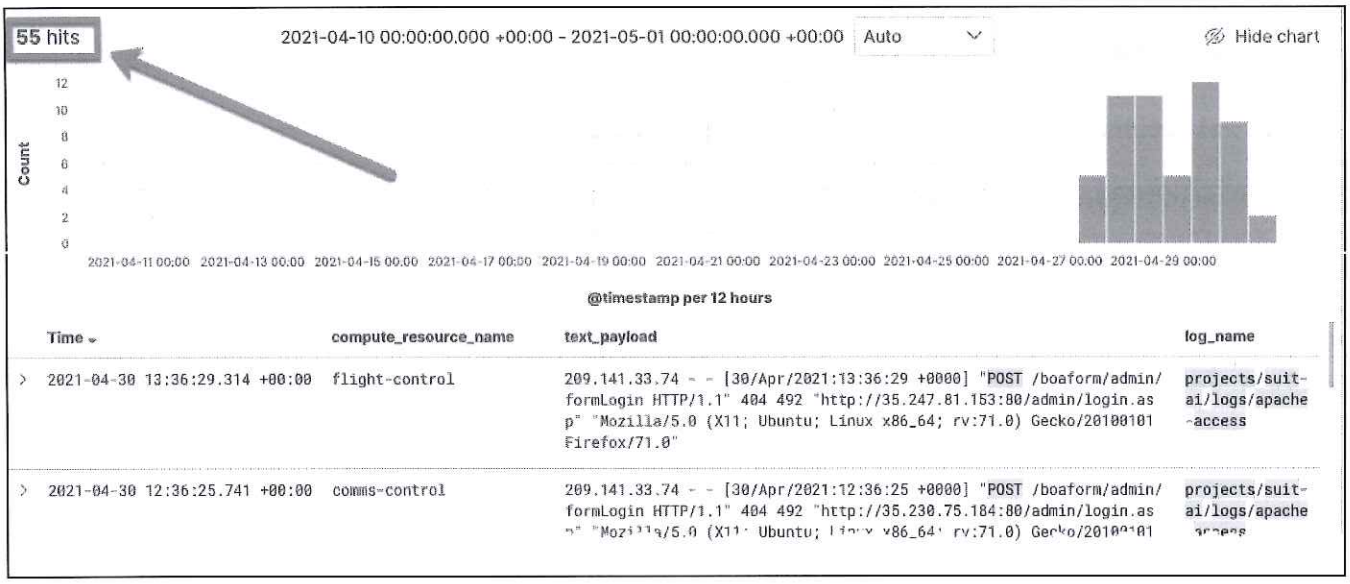
To begin with, let's narrow down our events to only the Apache logs with a filter. You can do this by selecting `log_name` in the `Field`, then `is` in the `Operator`, and `projects/suit-ai/logs/apache-access` in the `Vaule` field.



1. Within these logs there are a number of highly malicious activities occurring.

> **How many `POST` requests occurred in the logs available?**
>
> **55 Events**
>
> Because the logs are streamed to the GCP VM Agent, the data is captured in a single field within the GCP logs, so we cannot break them out. Due to this we have to string search the data we have available, but simply using the term `POST`.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon



How many of the `POST` requests were successfully processed by the Apache server?

8 Events

If you search for `POST AND "200"` you will find there are 8 events that used a `POST` request and received a `200` response from the Apache web server. The `200` response indicates that Apache server successfully processed the request it received.

text_payload

```
172.245.158.3 - - [29/Apr/2021:21:59:28 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Lin
Chrome/81.0.4044.129 Safari/537.36"

172.245.158.3 - - [29/Apr/2021:20:32:53 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Lin
Chrome/81.0.4044.129 Safari/537.36"

45.73.155.207 - - [29/Apr/2021:10:28:30 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Linu
Chrome/81.0.4044.129 Safari/537.36"

34.229.241.170 - - [29/Apr/2021:04:14:20 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Li
Chrome/81.0.4044.129 Safari/537.36"

52.167.54.108 - - [28/Apr/2021:07:17:01 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Lin
Chrome/81.0.4044.129 Safari/537.36"

45.73.155.207 - - [28/Apr/2021:01:46:00 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Lin
Chrome/81.0.4044.129 Safari/537.36"

64.227.106.142 - - [27/Apr/2021:21:25:00 +0000] "POST / HTTP/1.1" 200 3477 "-" "Anarchy99"

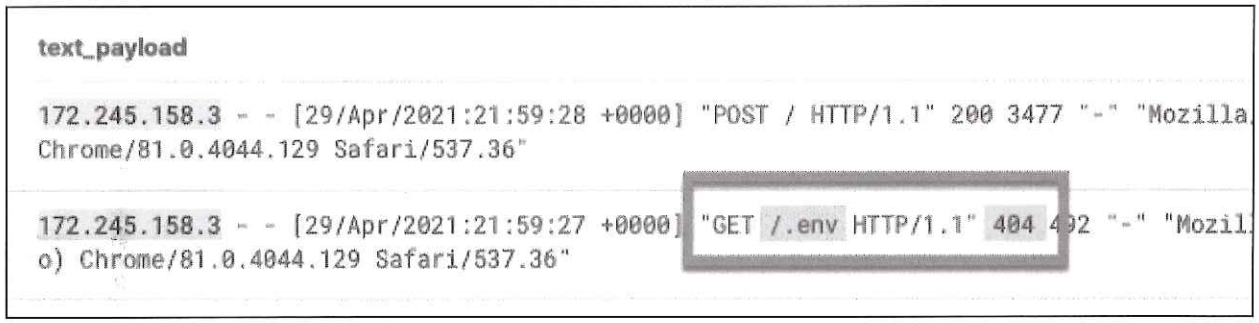
3.84.132.113 - - [26/Apr/2021:18:21:47 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Linu
hrome/81.0.4044.129 Safari/537.36"
```

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

All the IP addresses that managed to issue a `POST` request and get a successful response (`200` response code), also attempted to access another resource on the system, what was it?

`GET /.env`

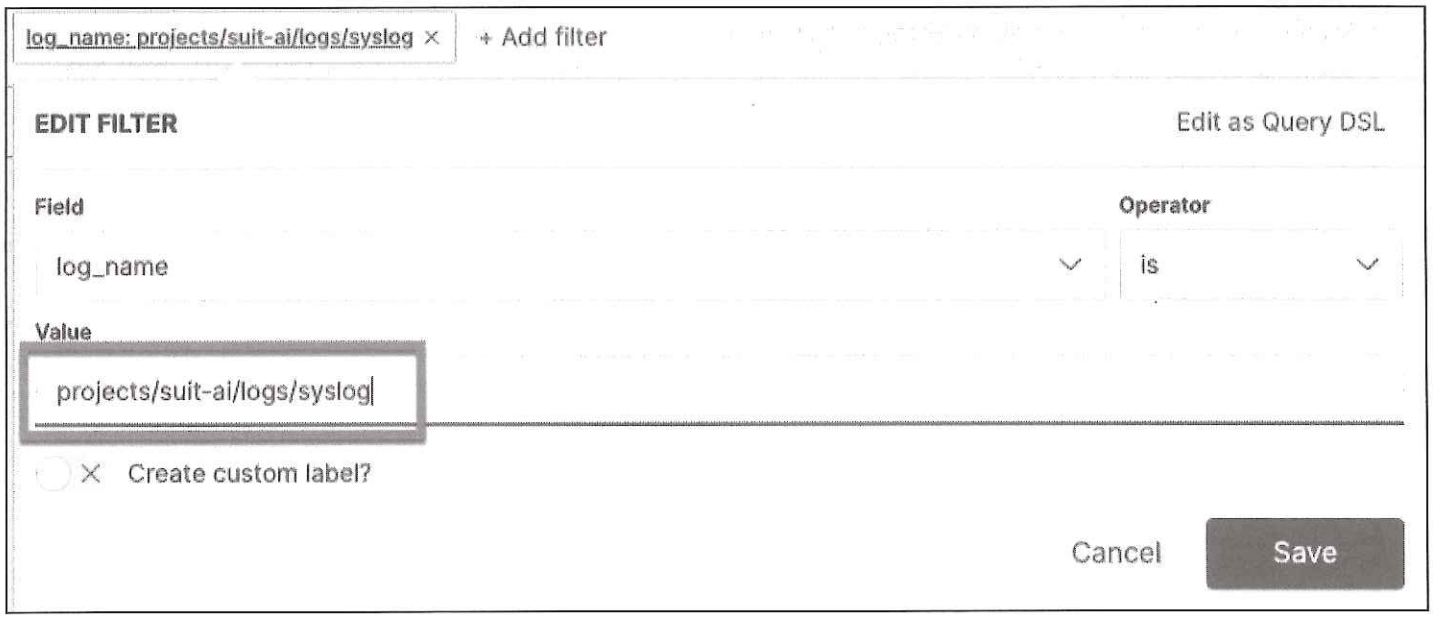
All the IP addresses also attempted, once or more, to access the `/.env` resource on both Apache servers. However, when they attempted this, it was unsuccessful indicated with a `404` response code.



Reviewing SysLog Logs

Before we finish with VM Agent Logs let's take a look at the SysLog logs. These can be some of the most useful messages when investigating a comprise, but also comes with its own frustrations.

Change the `filter` you have applied so that you are filtering all logs based on the `projects/suit-ai/logs/syslog` `Value` , then press `Save` .

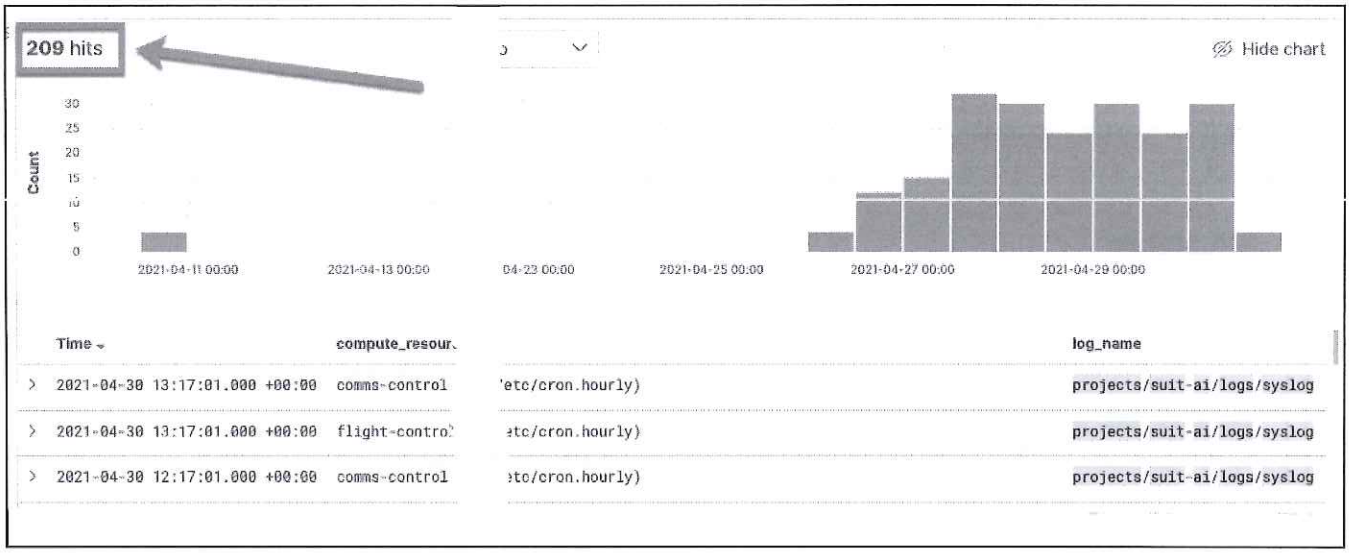


1. Now we have this filter applied let's see what we can find within the SysLog logs.

How many `CRON` logs can you find within the available data set?

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

** 209 Event Logs **



This can be run simply by using a search string of `"CRON"`.

You will notice that some of the earliest events that appear don't have their GCP VM Agent Logs in the `text_payload` field, instead they use the `system_message` field - this field is produced by SOF-ELK's parsers, they are actually in the the GCP JSON field `jsonPayload.message`. We're not really sure what the location of the GCP VM Agent output changed during our log capture, however, this is a good example to understand that GCP can change their logging format.

Can you find any unusual SSH login activity, and if so, why is it unusual?

Simply searching for `SSH` or `SSHD` doesn't return many useful results, in face it looks like there is now SSH logging that is being pushed to SysLog. This is because by default SSH will log to `/var/log/sshd/sshd.log`, which is not captured by GCP's VM Agent. There are ways to force SSH logging into SysLog, or can could also alter GCP's VM Agent config to include the `/var/log/sshd/sshd.log` file.

As a second step we can try to look for authentication events within SysLog. The easiest way to look for these is with the string search `"Started Session"` in the Search Bar.

One the above search is run you should now see **12** login events with both the user names `admin_` and `noname`.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Time	compute_resource_name	text_payload	log_name
2021-04-28 15:39:31.000 +00:00	comms-control	Apr 28 15:39:31 comms-control systemd[1]: Started Session 34 of user noname.	projects/suit-ai/logs/syslog
2021-04-28 10:56:16.000 +00:00	comms-control	Apr 28 10:56:16 comms-control systemd[1]: Started Session 28 of user noname.	projects/suit-ai/logs/syslog
2021-04-28 10:56:01.000 +00:00	comms-control	Apr 28 10:56:01 comms-control systemd[1]: Started Session 27 of user noname.	projects/suit-ai/logs/syslog
2021-04-27 15:44:52.000 +00:00	comms-control	Apr 27 15:44:52 comms-control systemd[1]: Started Session 4 of user noname.	projects/suit-ai/logs/syslog
2021-04-27 15:38:03.000 +00:00	comms-control	Apr 27 15:38:03 comms-control systemd[1]: Started Session 3 of user noname.	projects/suit-ai/logs/syslog
2021-04-27 15:29:47.000 +00:00	comms-control	Apr 27 15:29:47 comms-control systemd[1]: Started Session 1 of user noname.	projects/suit-ai/logs/syslog
2021-04-27 15:06:04.000 +00:00	comms-control	Apr 27 15:06:04 comms-control systemd[1]: Started Session 3 of user admin_.	projects/suit-ai/logs/syslog
2021-04-27 14:53:42.000 +00:00	comms-control	Apr 27 14:53:42 comms-control systemd[1]: Started Session 1 of user admin_.	projects/suit-ai/logs/syslog
2021-04-26 12:23:04.000 +00:00	flight-control	Apr 26 12:23:04 flight-control systemd[1]: Started Session 4 of user admin_.	projects/suit-ai/logs/syslog
2021-04-26 12:15:00.000 +00:00	flight-control	Apr 26 12:15:00 flight-control systemd[1]: Started Session 1 of user admin_.	projects/suit-ai/logs/syslog
2021-04-10 14:09:50.000 +00:00	instance-1	-	projects/suit-ai/logs/syslog
2021-04-10 13:55:33.000 +00:00	instance-1	-	projects/suit-ai/logs/syslog

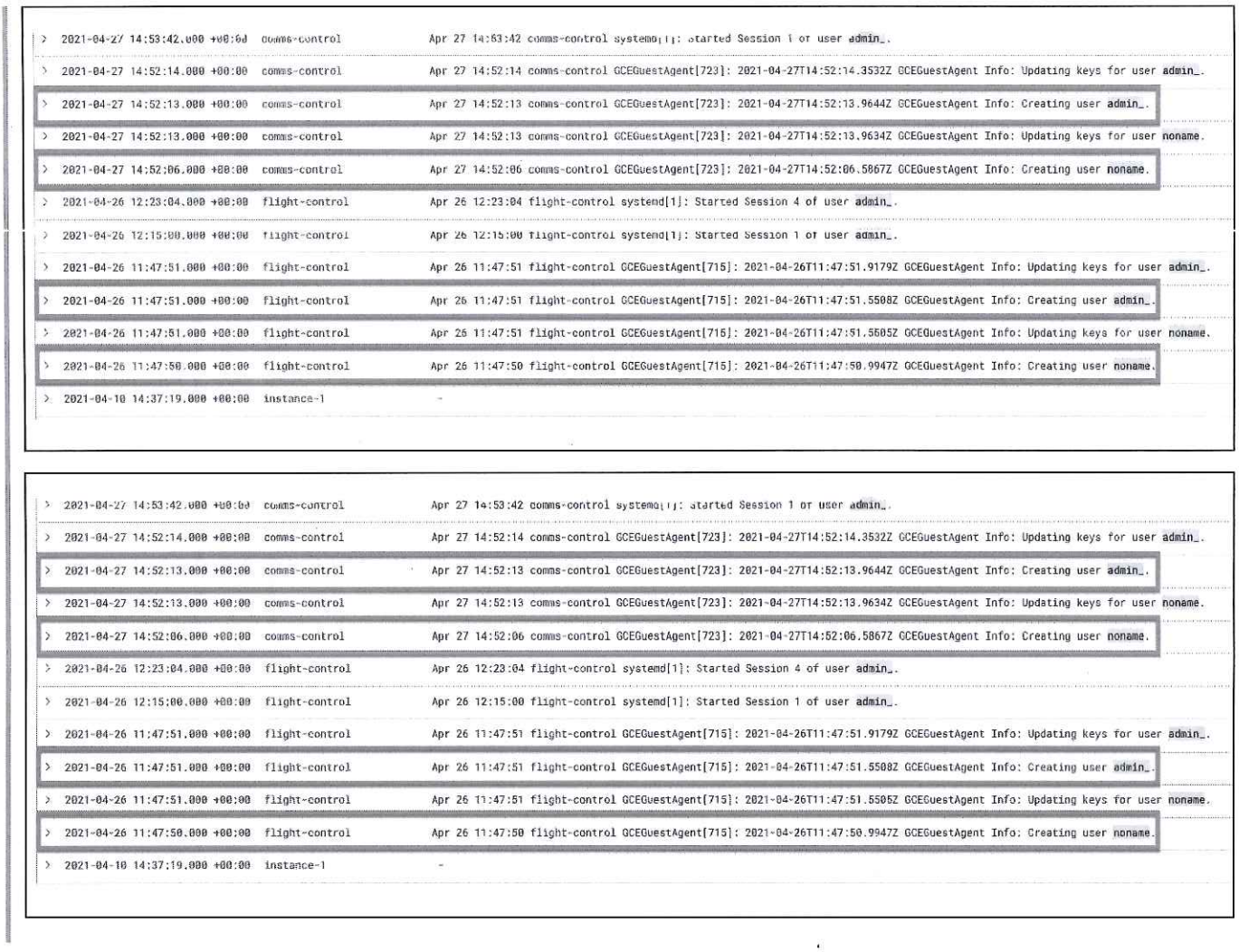
How were the two user accounts created, and when?

If you search for both the user names in the Search Bar `"noname" OR "admin_"` it will give you an overview of activity with those user accounts.

You will notice that both the user accounts were created with the `GCEGuestAgent`, this is the built in GCP agent that looks after integration between a VM and GCP architecture. This agent would have created these user accounts as part of an instruction from the platform, this could be either due to Policy or due to Project wide SSH keys that were implemented by a Policy.

Looking at the logs we can see the accounts were created; on `flight-control` on the `2021-04-26 11:47:50.000 UTC` on `comms-control` on the `2021-04-27 14:52:06.000 UTC` on `instance-1` on the `2021-04-10 13:54:45.000 UTC`

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



2021-04-27 14:53:42.000 +00:00	comms-control	Apr 27 14:53:42 comms-control systemd[1]: Started Session 1 of user admin_.
2021-04-27 14:52:14.000 +00:00	comms-control	Apr 27 14:52:14 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:14.3532Z GCEGuestAgent Info: Updating keys for user admin_.
2021-04-27 14:52:13.000 +00:00	comms-control	Apr 27 14:52:13 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:13.9644Z GCEGuestAgent Info: Creating user admin_.
2021-04-27 14:52:13.000 +00:00	comms-control	Apr 27 14:52:13 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:13.9634Z GCEGuestAgent Info: Updating keys for user noname.
2021-04-27 14:52:06.000 +00:00	comms-control	Apr 27 14:52:06 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:06.5867Z GCEGuestAgent Info: Creating user noname.
2021-04-26 12:23:04.000 +00:00	flight-control	Apr 26 12:23:04 flight-control systemd[1]: Started Session 4 of user admin_.
2021-04-26 12:15:00.000 +00:00	flight-control	Apr 26 12:15:00 flight-control systemd[1]: Started Session 1 of user admin_.
2021-04-26 11:47:51.000 +00:00	flight-control	Apr 26 11:47:51 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:51.9179Z GCEGuestAgent Info: Updating keys for user admin_.
2021-04-26 11:47:51.000 +00:00	flight-control	Apr 26 11:47:51 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:51.5508Z GCEGuestAgent Info: Creating user admin_.
2021-04-26 11:47:51.000 +00:00	flight-control	Apr 26 11:47:51 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:51.5505Z GCEGuestAgent Info: Updating keys for user noname.
2021-04-26 11:47:50.000 +00:00	flight-control	Apr 26 11:47:50 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:50.9947Z GCEGuestAgent Info: Creating user noname.
2021-04-10 14:37:19.000 +00:00	instance-1	-

2021-04-27 14:53:42.000 +00:00	comms-control	Apr 27 14:53:42 comms-control systemd[1]: Started Session 1 of user admin_.
2021-04-27 14:52:14.000 +00:00	comms-control	Apr 27 14:52:14 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:14.3532Z GCEGuestAgent Info: Updating keys for user admin_.
2021-04-27 14:52:13.000 +00:00	comms-control	Apr 27 14:52:13 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:13.9644Z GCEGuestAgent Info: Creating user admin_.
2021-04-27 14:52:13.000 +00:00	comms-control	Apr 27 14:52:13 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:13.9634Z GCEGuestAgent Info: Updating keys for user noname.
2021-04-27 14:52:06.000 +00:00	comms-control	Apr 27 14:52:06 comms-control GCEGuestAgent[723]: 2021-04-27T14:52:06.5867Z GCEGuestAgent Info: Creating user noname.
2021-04-26 12:23:04.000 +00:00	flight-control	Apr 26 12:23:04 flight-control systemd[1]: Started Session 4 of user admin_.
2021-04-26 12:15:00.000 +00:00	flight-control	Apr 26 12:15:00 flight-control systemd[1]: Started Session 1 of user admin_.
2021-04-26 11:47:51.000 +00:00	flight-control	Apr 26 11:47:51 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:51.9179Z GCEGuestAgent Info: Updating keys for user admin_.
2021-04-26 11:47:51.000 +00:00	flight-control	Apr 26 11:47:51 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:51.5508Z GCEGuestAgent Info: Creating user admin_.
2021-04-26 11:47:51.000 +00:00	flight-control	Apr 26 11:47:51 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:51.5505Z GCEGuestAgent Info: Updating keys for user noname.
2021-04-26 11:47:50.000 +00:00	flight-control	Apr 26 11:47:50 flight-control GCEGuestAgent[715]: 2021-04-26T11:47:50.9947Z GCEGuestAgent Info: Creating user noname.
2021-04-10 14:37:19.000 +00:00	instance-1	-

Filtering Clean Up

Ensure you clear out any filters you may still have applied for this lab, this will ensure your next lab isn't impacted by any filters you used in this lab.

Key Takeaways

- Students should understand how GCP VM Agent Logs are recorded and how they can be manipulated to investigate services running on VM's.
- A better understanding of how to identify individual VM's and knowing they are not always named in the logs with human defined names.
- An understanding of how to quickly identify the servers that are producing logs on a VM and how to then drive into those logs for further analysis.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Lab 4.3: Storage Abuse and Exfil

Objectives

- Understand GCP Storage Logging Format
- Understand what to look for when analyzing GCP Storage Logs for misuse.
- Being able to link misuse events back with user accounts to track a timeline of behaviour.

Background

LongConSecurity have received reports that highly confidential data has been taken from their organization. LongConSecurity know that the data only existed in a locked down GCP Bucket, which they believed to be limited to only users with Organization Admins access. All the users with access to this Bucket are trusted and they do no suspect any of them as the source of the data being taken.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM
3. Access to the SOF-ELK® VM console via the user account `elk_user` and the password `forensics`.
4. Perform an update of the SOF-ELK configuration by running the following command after you've logged into SOF-ELK:
   `sudo sof-elk_update.sh`
5. Ensure you have loaded the relevant data as described in the next section.
6. Relevant timeframe: `2021-04-12 00:00 to 2021-04-28 00:00 UTC`

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the GCP parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

The GCP JSON logs for this lab have already been exported from Google Logging. To help in keeping the level of data to a reasonable size we have trimmed the data set to only include GCP Bucket Logs. However, there were no other changes

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

made to the JSON that was extracted from GCP so it is still representative of what you'll experience outside of the this course.

The GCP VM Agent Logs have been saved into `/home/elk_user/lab-4.3_source_evidence.zip`.

1. Log on to the SOF-ELK VM with the credentials
   - Username: ***elk_user***
   - Password: ***forensics***

   You may log on to the console, however it's recommended to log in via SSH.
2. Extract the all the `.json` files from the ZIP file above into the their correct LogStash folder for parsing by FileBeats with the following command:

```
cd ~
unzip lab-4.3_source_evidence.zip -d /logstash/gcp/
```

> ⚠ **Warning**
>
> Do not run this command more than once!

3. Wait 2 minutes for the data to be processed. Once it is complete the data will be available in the `gcp-*` index.

Lab Content

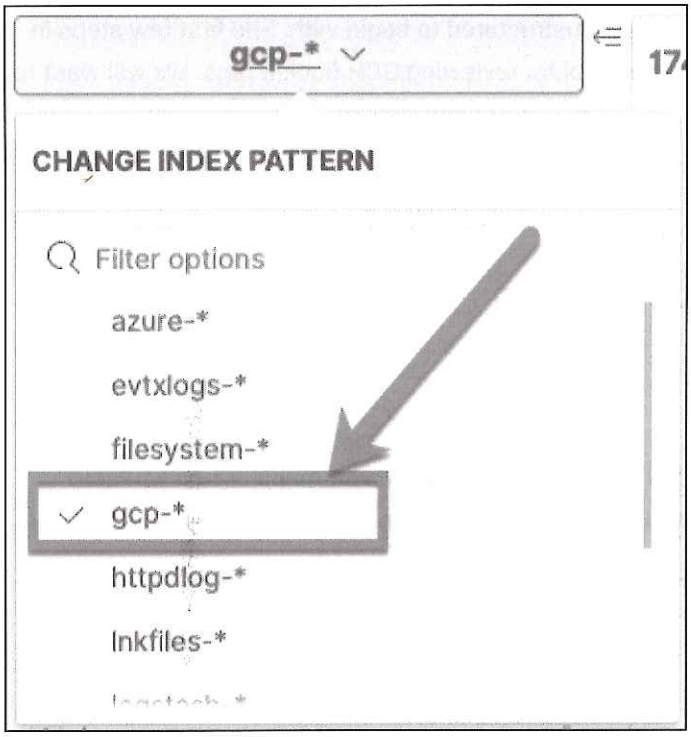
Review the indices in SOF-ELK

Start in the Discover tab

When data is imported in SOF-ELK, it's assigned to a specific index. In this lab, and all other labs within this section, we will be using the `gcp-*` index.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

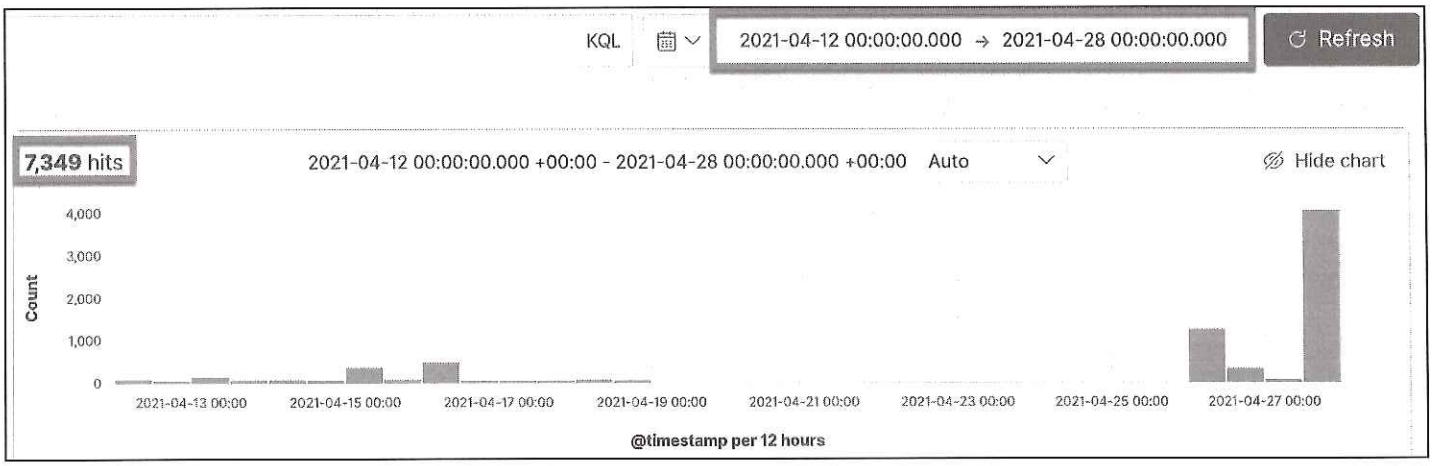
Technet24



This index will contain all of the GCP logs you will investigate in this section of the course, except for Flow data.

Before we go to far, let's ensure the date range is correct for the data we'll be using in this lab. Set your search timeframe to `2021-04-12 00:00 to 2021-04-28 00:00 UTC` hit `Update`. Based on this timeframe you should see **7,349 hits** or entries in your histogram.

> **Notice**
>
> The above "hits" count assumes you have loaded Labs 4.1 and Labs 4.2 already.

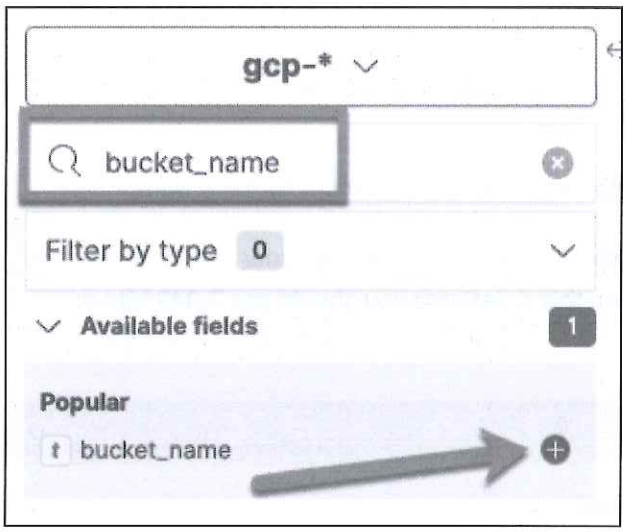


 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

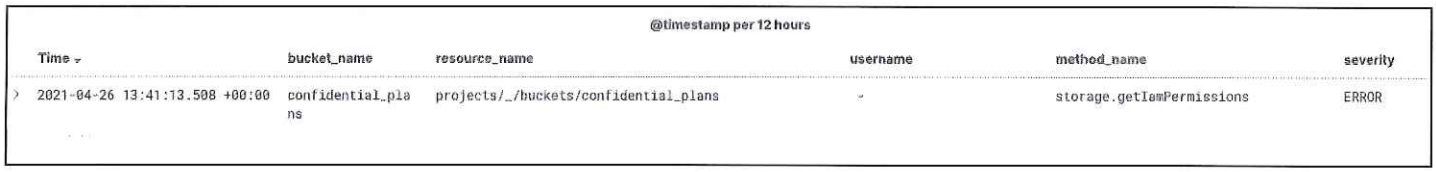
The initial view of the data within the Discovery view of SOF-ELK is very unstructured to begin with. The first few steps in this exercise we will add in specific columns to make the data more useful for reviewing GCP Bucket logs. We will want to add in the following column names:

- `bucket_name`
- `resource_name`
- `username`
- `method_name`
- `severity`

To add in these names you can search for them in the field selector under the index drop down menu. When you start typing the field name it will appear for you to select with + that will appear when you hover your mouse over the field name.



Provided you added the fields in the order above, your events in Discovery should now appear similar to the below image.

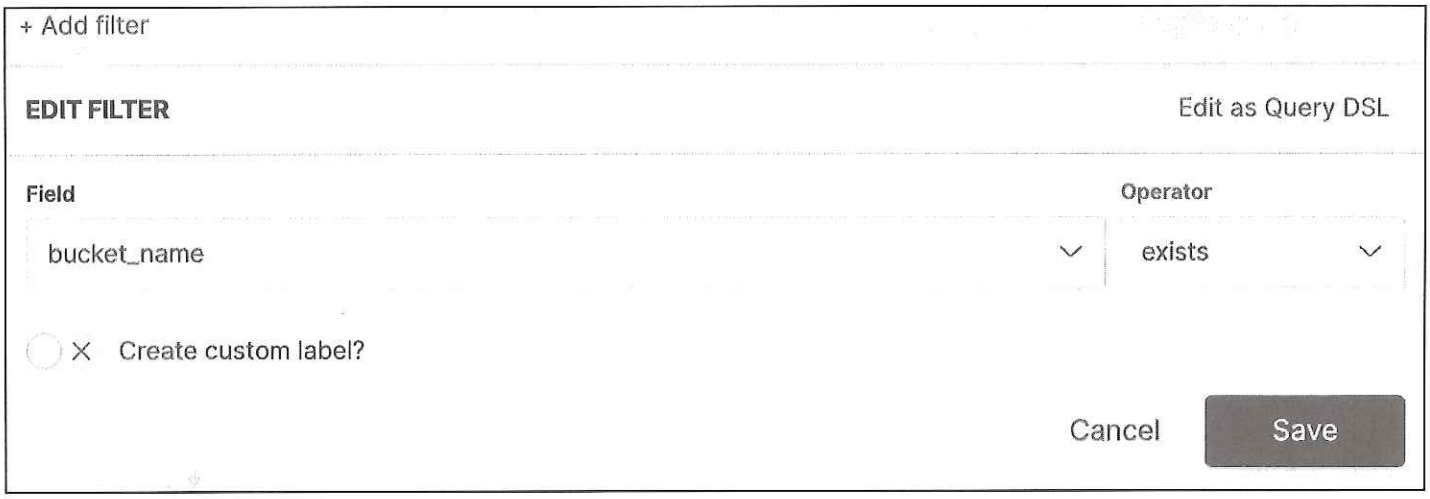


We're now ready to start looking through our GCP Bucket logs.

Discover Unusual Activity in GCP Bucket logs

Let's start by filtering down our log data to only the relevant information for buckets. We can do this with the `Add filter` feature. Let's add a filter that checks that the `bucket_name` field `exists`. This will just show us the GCP Bucket logs.

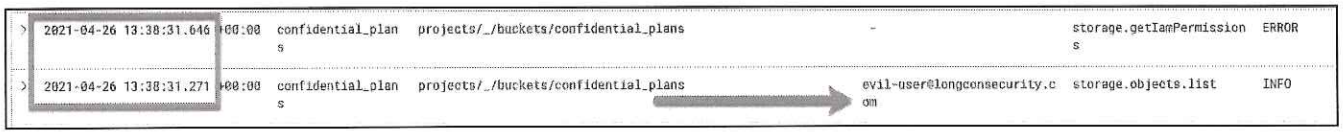
https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



1. Part of reviewing GCP Bucket Logs involves looking for potential failed access to objects or failed permissions to tasks. We're going to see what we can discover when we look for this type of data in the logs.

> **There are two groupings of events in our histogram, using the search field when did the `ERROR` events start and finish?**
>
> You will need to use the search field to look for `severity: "ERROR"`.
>
> You will see **18 hits** for data that matches this search starting from `2021-04-26 13:37:52.405 UTC` and finishing on `2021-04-26 13:41:13.508`

> **Are there any events proceeding these `ERROR` events that involve authenticated user accounts, or account information that we could further investigate?**
>
> You will noticed that immediately before all of these `ERROR` events there is a user account that continually appears `evil-user@longconsecurity.com`



> **What Buckets has the user from the previous question been looking at?**
>
> You will need to use the search field with the user account we identified in the previous question `username: "evil-user@longconsecurity.com"`.
>
> Becasue the amount of data we are analyzing has been trimmed down for the exercise, it is easy to quickly scroll through the events to identify the `bucket_name` 's that appear.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

	bucket_name	resource_name	username
0	confidential_plans	projects/_/buckets/confidential_plans/objects/Suit_CPU_Design.zip	evil-user@longconsecurity.com
9	confidential_plans	projects/_/buckets/confidential_plans	evil-user@longconsecurity.com
0	flight-maps	projects/_/buckets/flight-maps	evil-user@longconsecurity.com
0	flight-maps	projects/_/buckets/flight-maps	evil-user@longconsecurity.com
10	flight-maps	projects/_/buckets/flight-maps	evil-user@longconsecurity.com
0	confidential_plans	projects/_/buckets/confidential_plans	evil-user@longconsecurity.com

The two `bucket_names` that were accessed are; `confidential_plans` and `flight-maps`

What, if any, files were were accessed by the user from the previous questions?

You will need to use the search field and build on the previous searches we've used so far. By adding in the `method_name: "storage.objects.get"` to our search we will see the files that were downloaded by the user.

The overall search should be `username: "evil-user@longconsecurity.com" AND method_name: "storage.objects.get"`.

Once you have run this search you will see there is only 1 file that appears to have been accessed by the user account `evil-user@longconsecurity.com`, that file is listed in the `resource_name` field as `projects/_/buckets/confidential_plans/objects/Suit_CPU_Design.zip`.

bucket_name	resource_name	username	method_name
confidential_plans	projects/_/buckets/confidential_plans/objects/Suit_CPU_Design.zip	evil-user@longconsecurity.com	storage.objects.get

We can also see that this occurred in the `confidential_plans` Bucket.

How did a GCP Bucket Get Exposed

1. In the previous section we discovered that a user account which likely shouldn't have had permission to a Bucket was able to access and download a file. We now need to understand if the logs will show us how this may have occurred.

When was the `Suit_CPU_Design.zip` file first added to the Bucket, and who added it?

You will need to use the search field looking for the file we have previously identified. Your search should be `resource_name : "projects/_/buckets/confidential_plans/objects/Suit_CPU_Design.zip"`

Once this search is completed you will see the earliest event we have for this file is `2021-04-18 14:53:07.306 UTC`.

You will also see that user that appears in this first event is `admin@longconsecurity.com`.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

You'll notice that the first event doesn't contain detail along the lines of "file created", instead you see a `storage.objects.update`. This is how GCP Buckets represent a new or updated item within a Bucket. It is possible the item existed earlier than the time window we are looking at as well, however it would still only show `storage.objects.update`.

Were there any permission changes within the `confidential_plans` Bucket that may explain why it was accessible to other users?

The best way to go looking for this type of data is using the `method_name` to see if there is anything related to a permission change.

Initially you may try looking for `method_name: *IamPermissions` in the search bar. However, you will notice that this returns 38 entries.

You could try to narrow this search down by excluding all the `storage.getIamPermissions` as we aren't interested in when people queried the permissions at this stage, just when they were changed. To do this use this search `method_name: *IamPermissions AND NOT method_name : storage.getIamPermissions`.

You will see one entry. If you expand out the entry you will see there is a `policy_deltas` that lists out the changes made during a `getIamPermissions` event.

t	log.file.path	/logstash/gcp/Lab4.3-GCP_BucketLogs.json
t	log.flags	multiline
#	log.offset	115,979
t	method_name	storage.setIamPermissions
{}	policy_deltas	{ "action": "ADD", "role": "roles/storage.legacyBucketReader", "member": "allUsers" }
t	project_id	suit-ai
t	resource_location	us-west1
t	resource_name	projects/_/buckets/confidential_plans
t	resource_type	gcs_bucket
t	service_name	storage.googleapis.com
t	severity	NOTICE

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

> This shows the `admin@longconsecurity.com` user account set the `confidential_plans` Bucket to allow `allUsers` to access files within the Bucket.

Pivoting on our Findings

1. Based on what we've found so far, can we now pivot on this information to see if anything else has gone wrong with our GCP Buckets?

> **What other Buckets did `admin@longconsecurity.com` create or update?**
>
> The best way to go looking for this is narrowing a search to only ths user you're looking for and to look for both the create and update methods for buckets.
>
> You can use this search: `username:"admin@longconsecurity.com" AND method_name : (storage.buckets.update OR storage.buckets.create)`
>
> Unlike files in a Bucket, Buckets will have the `create` method for them.
>
> You will see two matching buckets, the `confidential_plans` Bucket created on `2021-04-18 12:45:28.808` and the `flight-maps` Bucket with the earliest update time of `2021-04-13 01:41:49.225`.
>
> The `flight-maps` Bucket was created outside of the log data we have available within SOF-ELK.

> **Were there any other permissions applied to any Storage Bucket objects that would have allowed the `allUsers` permission?**
>
> Because the `policy_deltas` file in SOF-ELK is currently an un-indexed field we have to do a simple string search looking for `allUsers` in the search bar.
>
> Running this search we'll find there are in fact **3** resources within the GCP Bucket that have had their permissions all set to `allUsers`.

	Time	bucket_name	resource_name
>	2021-04-26 12:01:39.070 +00:00	confidential_plans	projects/_/buckets/confidential_plans
>	2021-04-18 14:53:07.306 +00:00	confidential_plans	projects/_/buckets/confidential_plans/objects/Suit_CPU_Design.zip
>	2021-04-13 04:01:19.989 +00:00	flight-maps	projects/_/buckets/flight-maps/objects/test-flight/test_flight_route.jpeg

> **Using the same search you just ran for the last question, what `method_name` is used for files within Buckets to set the `allUsers` permission?**
>
> You should see that files within Buckets use the `storage.objects.update` `method_name` when a permission is changed. This should seem familiar now given the same `method_name` is used when adding a file to a Bucket.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

resource_name	username	method_name	severity
projects/_/buckets/confidential_plans	admin@longconsecurity.com	storage.setIamPermissions	NOTICE
projects/_/buckets/confidential_plans/objects/Suit_CPU_Design.zip	admin@longconsecurity.com	storage.objects.update	NOTICE
projects/_/buckets/flight-maps/objects/test-flight/test_flight_route.jpeg	admin@longconsecurity.com	storage.objects.update	NOTICE

Filtering Clean Up

Ensure you clear out any filters you may still have applied for this lab, this will ensure your next lab isn't impacted by any filters you used in this lab.

Key Takeaways

- You should have an understanding that seeing `ERROR` messages within GCP Bucket logs usually indicates unusual requests being made by users who likely don't have permissions to access certain resources.
- Resources that have had the `setIamPermission` applied indicates a change in the permissions on a resource
- An understanding of how to track down permissions changes to files and Buckets when they have been mistakenly exposed.
- Additions and IAM changes to files within Buckets don't have a dedicated "Create" or "IAM Change" type method in the same way that Buckets do.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

Lab 4.4: Google Cloud - Network Forensics

Objectives

- Understand the data that is captured by GCP Flow Logs and how to quickly search for data within them.
- Understand how to import GCP Flow Logs into SOF-ELK and the pre-made dashboard available for searching Flow logs.
- Students will be able to look for malicious network activity within Flow logs and understand the investigation value they can provide.

Background

Inside the GCP instance for LongConSecurity.com there was an unusually large spike in traffic on the evening of the 27th of April 2021 (UTC). The GCP Network Admins have extracted the GCP Flow logs for the VM's that were inside the `default` VPC and provided you with the flow logs just prior and post the large increase in network traffic.

Preparation

To prepare:

1. Make sure your SOF-ELK® VM is running
2. Access Kibana via the IP address shown on the SOF-ELK® VM
3. Access to the SOF-ELK® VM console via the user account `elk_user` and the password `forensics`.
4. Ensure you have completed Lab 0. This is important to ensure the geo tagging for the log data you're about to load into this, and future labs, work correctly.
5. Perform an update of the SOF-ELK configuration by running the following command after you've logged into SOF-ELK:
   `sudo sof-elk_update.sh`
6. Ensure you have loaded the relevant data as described in the next section.
7. Relevant timeframe: `2021-04-27 13:00 to 2021-04-27 21:00 UTC`

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Load Data

In lab 0 you loaded a GeoIP database which means that any new data you import will have IP addresses enriched with geolocation information. For this lab, this extra information will be very useful. As such, we didn't preload the data and you will have the opportunity to see how simple it is to load data into SOF-ELK. Additionally, we are continually making changes to the GCP parsers and because of this we'll get you to update the config files in SOF-ELK before we load this lab's data set.

The GCP JSON logs for this lab have already been exported from Google Logging. To help in keeping the level of data to a reasonable size we have trimmed the data set to only include GCP Bucket Logs. However, there were no other changes made to the JSON that was extracted from GCP so it is still representative of what you'll experience outside of the this course.

The GCP VM Agent Logs have been saved into `/home/elk_user/lab-4.4_source_evidence.zip`.

1. Log on to the SOF-ELK VM with the credentials
   - Username: ***elk_user***
   - Password: ***forensics***

   You may log on to the console, however it's recommended to log in via SSH.
2. Extract the all the `.json` files from the ZIP file above into the their correct LogStash folder for parsing by FileBeats with the following command:

```
cd ~
unzip lab-4.4_source_evidence.zip -d /logstash/nfarch/
```

> ⚠ **Warning**
>
> Do not run this command more than once!

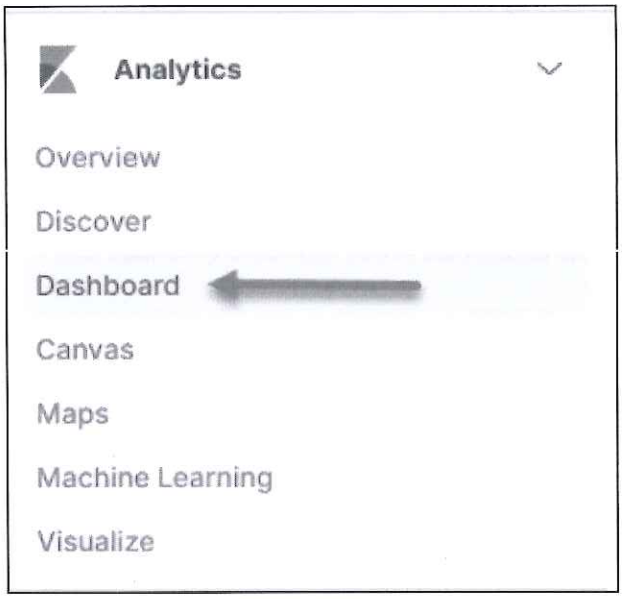
3. Wait 2 - 4 minutes for the data to be processed. Once it is complete the data will be available in the `netflow-*` index.

Lab Content

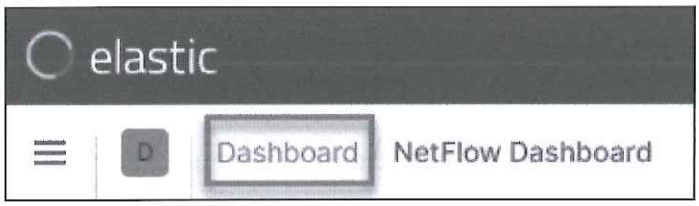
Start in the Dashboard tab

For this lab we're going to work mainly in the NetFlow Dashboard, so you need to ensure you've cleared out any searches you had previously in SOF-ELK and navigate to the **Dashboard** tab:

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

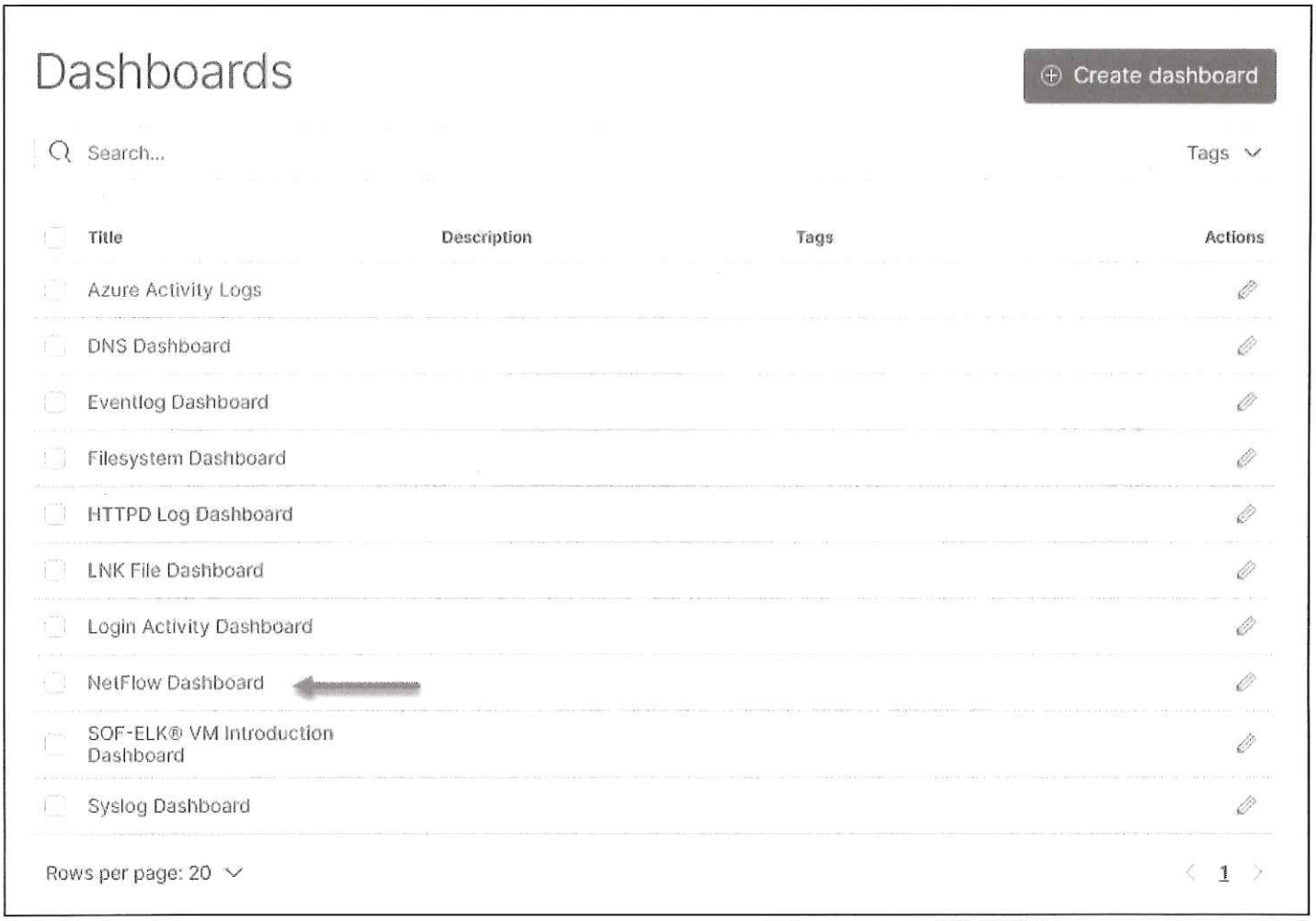


Click on the word `Dashboard` to get the dashboard menu:



Select the **NetFlow** dashboard:

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



Let's ensure we have all the logs loaded correctly, you should see the below results in the top of your NetFlow Dashboard once you filter the time to `2021-04-27 13:00 to 2021-04-27 21:00 UTC`

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



Warning

If you do not see the same data displayed in your SOF-ELK NetFlow Dashboard, you should stop at this point. Either, you are not looking at the correct time frame, or your data hasn't finished loading or hasn't loaded correctly.

Discover The GCP Flow Logs We Have Available

This section is in the Visualize tab

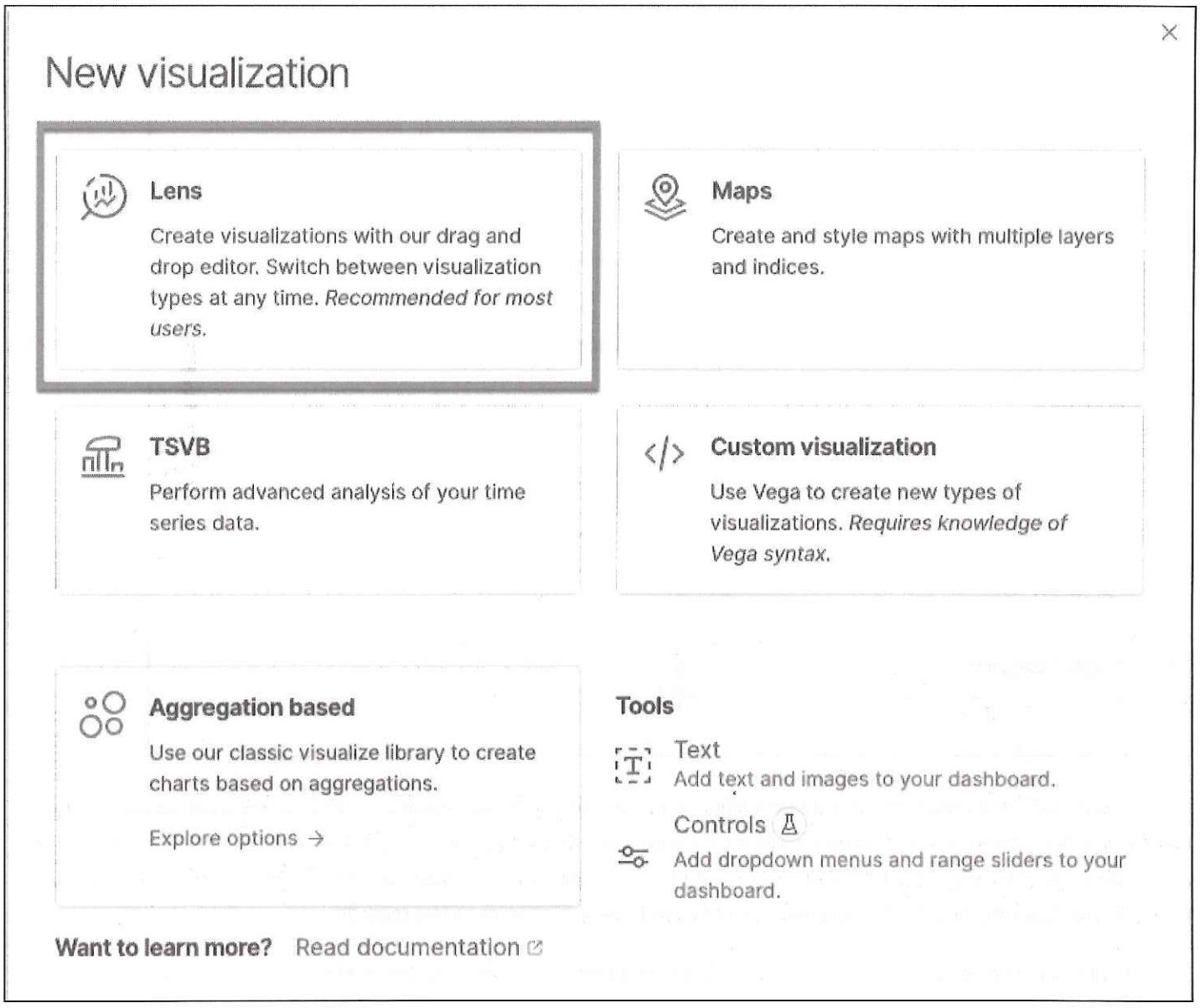
Let's start by understand the GCP Flow Logs that have been loaded, so we know where the logs have come from before we start to dive into them looking for malicious activity.

As the NetFlow Dashboard in SOF-ELK is designed to look at all types of Flow data, it doesn't have Dashboard Widgets that show the VM's or the VPC that the data originated from. We'll need to do this ourselves using the Visualize dashboard.

Move to the `Visualize` tab in Kibana and select `Create visualization`.

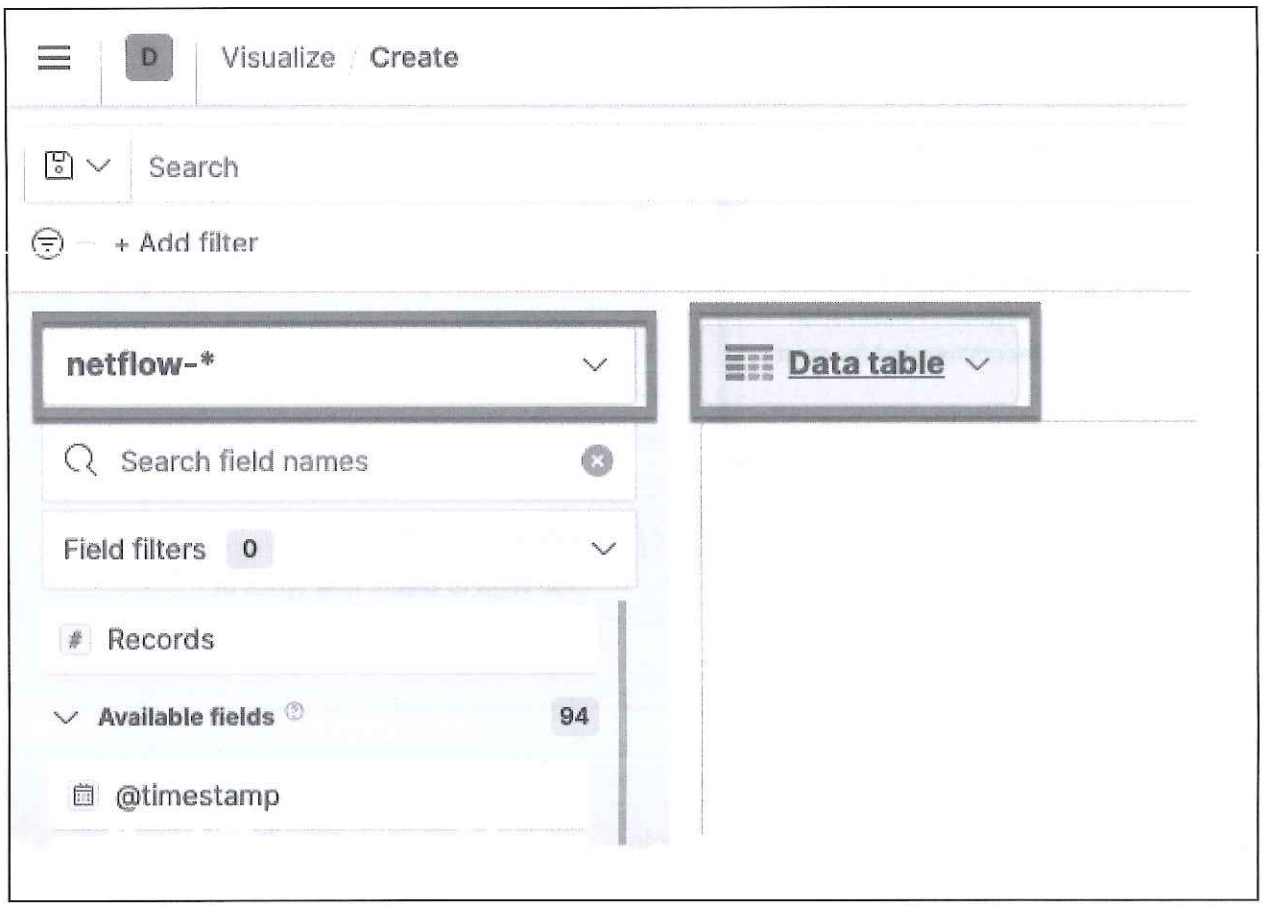
We will use `Lens` as it's the easiest way to create a new visualization.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



You will need to move the index selector over to `netflow-*` to ensure we are looking at the GCP Flow data. We will also change the graph type to `Data table`

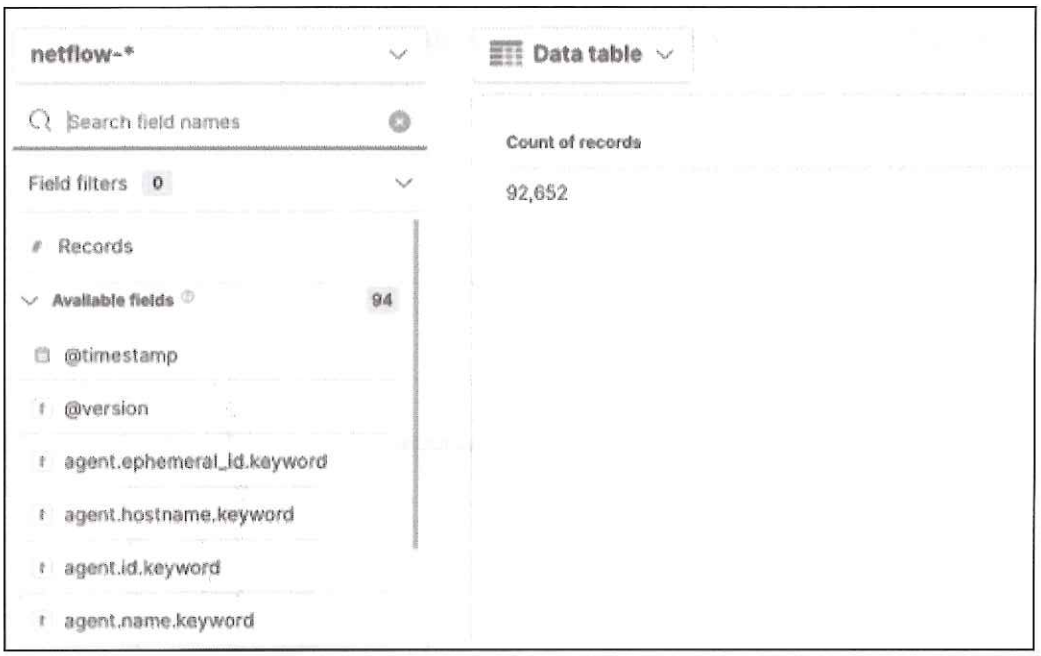
 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



Within each GCP Flow record there is a field called `destination_vm_name.keyword` or `source_vm_name.keyword`, and a record called `destination_vpc_name.keyword` or `source_vpc_name.keyword`. The difference in if there is a the `source_` or `destination_` difference is based on the direction of the traffic. Flow records are not bidirectional, they only record traffic in one direction, so a TCP connection would have have two separate Flow records.

To first understand what data we're looking at, let's just drag into our table vizulization the `destination_vm_name.keyword` field and `destination_vpc_name.keyword` field.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



1. Based on the table we've just created...

> **How many inbound flow records are available for each VM and what is the VPC that these VM's are contained within?**
>
> What this should now allow us to see is that there are three VM's in GCP Flow Logs:
>
> - comms-control = **7,105 records**
> - flight-control = **4,155 records**
> - pcap-capture = **2,991 records**
>
> All of the above VM's are all within the `default` VPC.

Data table

Top values of destination_vm_name.keyword	Top values of destination_vpc_name.keyword	Count of records
comms-control	default	7,105
flight-control	default	4,155
pcap-capture	default	2,991

2. Adding onto the table we just created, add in the `destination_ip` to the table.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon

What are the corresponding internal IP addresses for the VM's we have identified above?

After adding in the `destination_ip` field you should now see the following IP addresses match up with the VM's.

- comms-control = **10.138.0.10**
- flight-control = **10.138.0.8**
- pcap-capture = **10.138.0.9**

Data table

Top values of destination_vm_name.keyword	Top values of destination_vpc_name.keyword	Top values of destinatic
comms-control	default	10.138.0.10
flight-control	default	10.138.0.8
pcap-capture	default	10.138.0.9

This information may seem trivial now, however, it will be useful in the next section when we're looking at all three of the VM's traffic together.

Discover Unusual Traffic In The GCP Flow Logs We Have Available

This section is in the NetFlow Dashboard tab

Noticed

All the screenshots in this section are of widgets within the NetFlow Dashboard. They don't show the whole dashboard, only the widget where the answer would be found. This has been done to make it easier to read.

Now that we know what VM's are within the flow logs, along with the VPC they were contained within, we can now start to dive into the network traffic data. Move back over to the the NetFlow Dashboard where we'll look at the Flow records in more detail.

1. Looking at the top three histogram graphs we can see a visible rise in network traffic.

What VM (instance name and IP) is most likely responsible for the spike in Flow traffic?

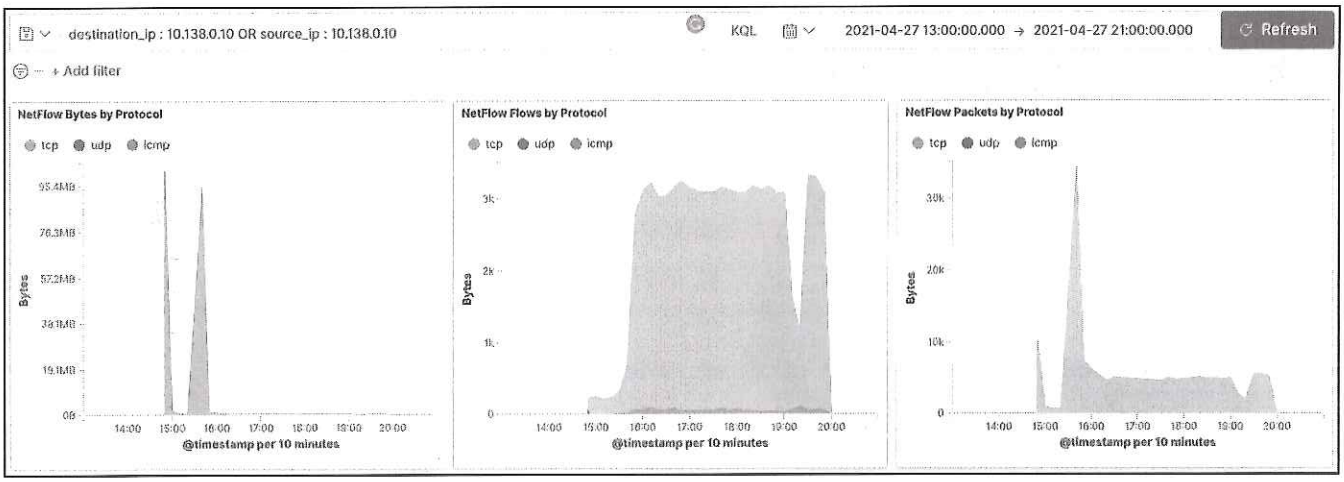
When you filter on the three IP addresses identified above you want to try and include both inbound and outbound traffic for the VM's. The best way to do this is with and `OR` statement in the search field of the Dashboard.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

When you search on IP `10.138.0.10` using `destination_ip : 10.138.0.10 OR source_ip : 10.138.0.10` you can see there is a notable include in traffic based on the top three histogram graphs. This system, which matches back to `comms-control`, appears to be the VM with a very unusually uptick in traffic.

Additionally, this `comms-control` VM appears to have almost 10 times more flow records for the same period of time compared to the other two VM's.

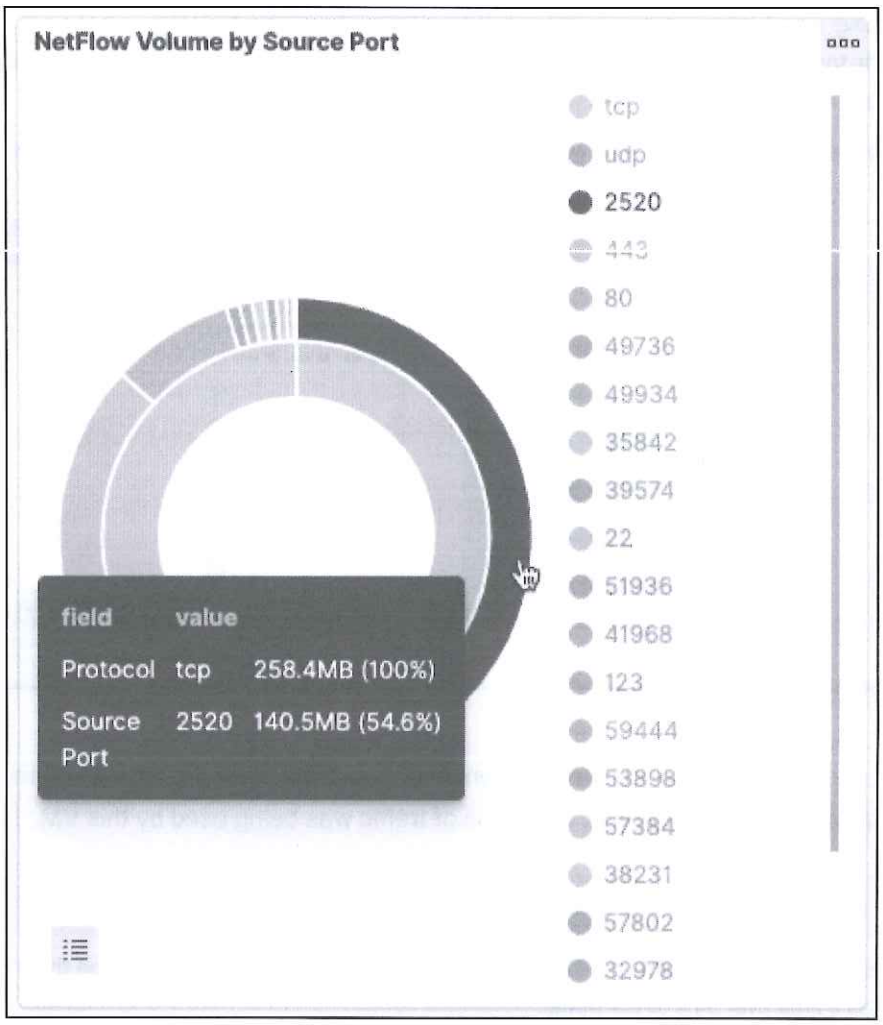


2. Let's start to look at the type of traffic occurring with the VM we just identified. Leave the search filter, mentioned in the above answer, in your search bar so we can start to look at what type of traffic was being used by this VM.

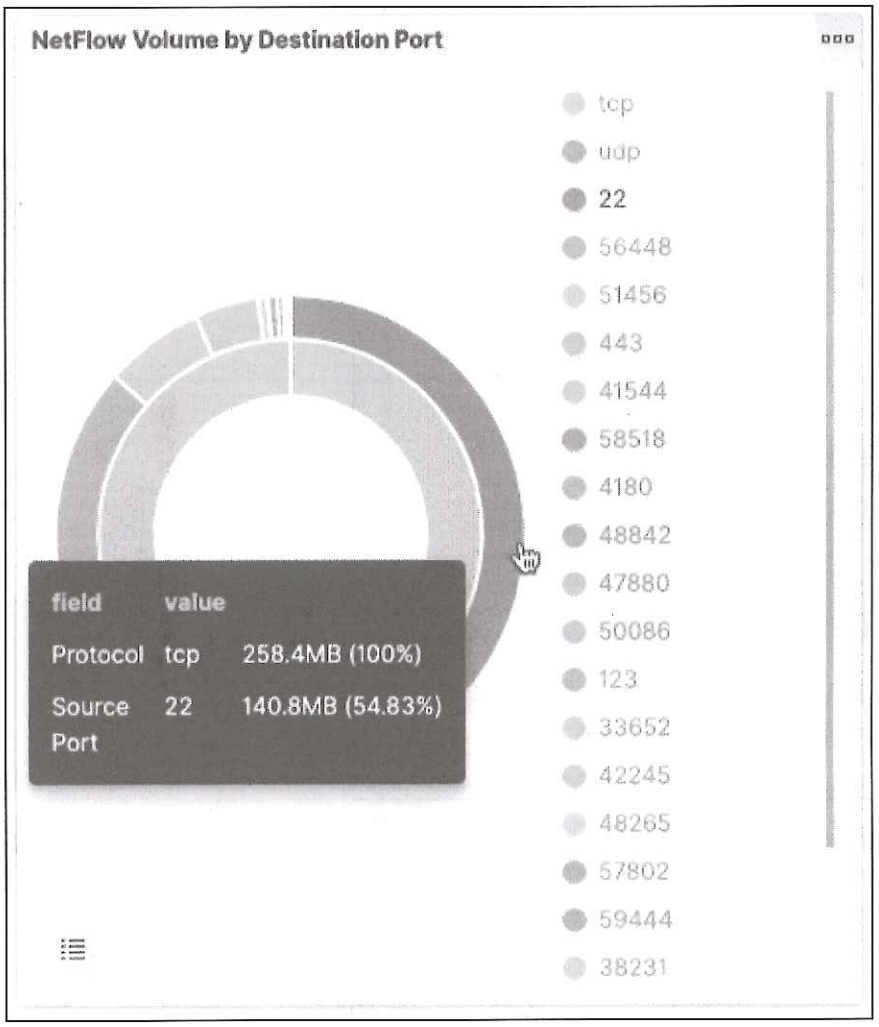
Which traffic type (TCP and Port) appears to be the result of the increased traffic?

When viewing both the `NetFlow Volume by Source Port` and `NetFlow Volume by Destination Port`, we can see there is only slice of the ring graph that consumes a little over 54% of the traffic.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



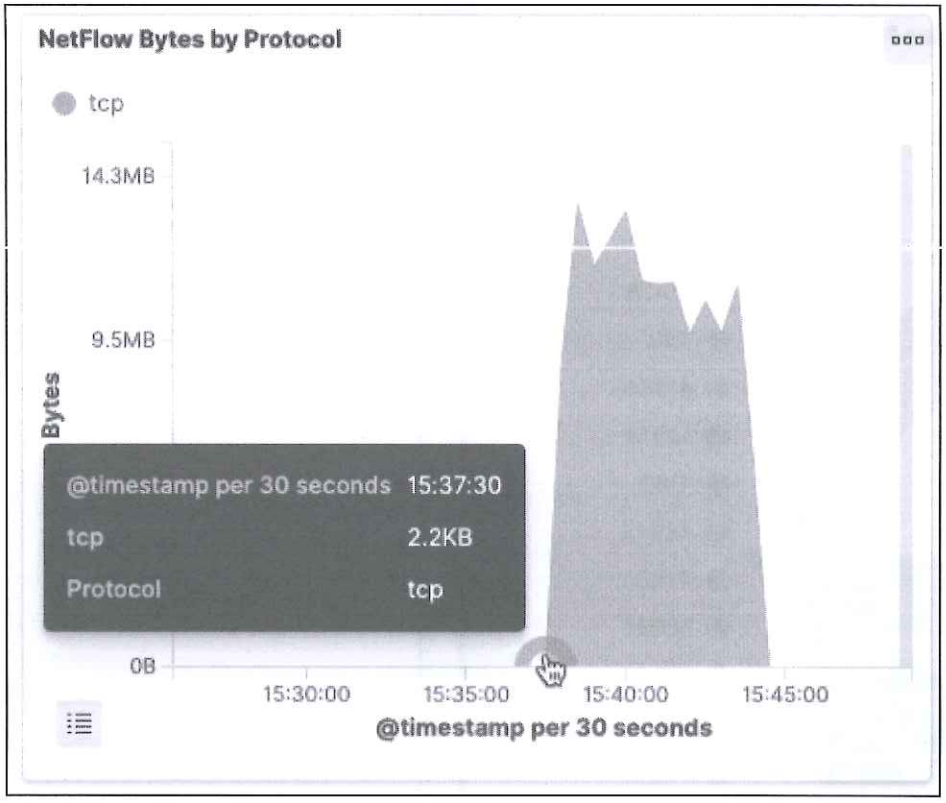
Based on the pie graphs this appears to be:

- Source Port: `TCP 2520`
- Destination Port: `TCP 22`

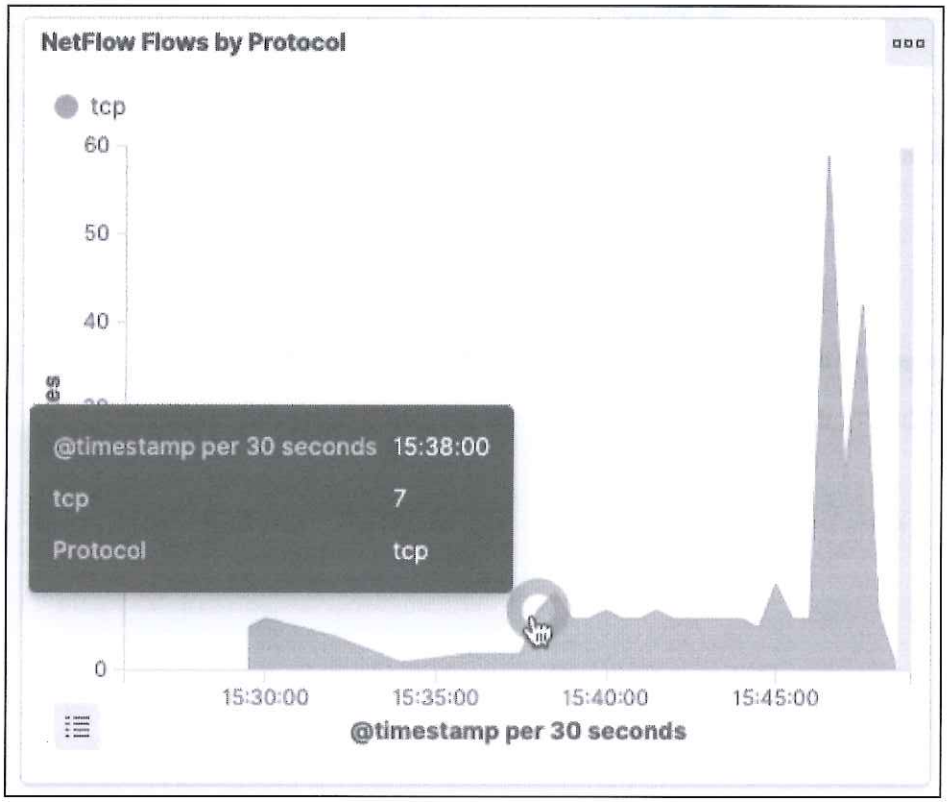
When does the traffic start to significantly increase for the VM and traffic type we've identified?

At approximately 2021-04-27 15:37:30 UTC there was a traffic spice, in terms of the amount of bytes observed.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



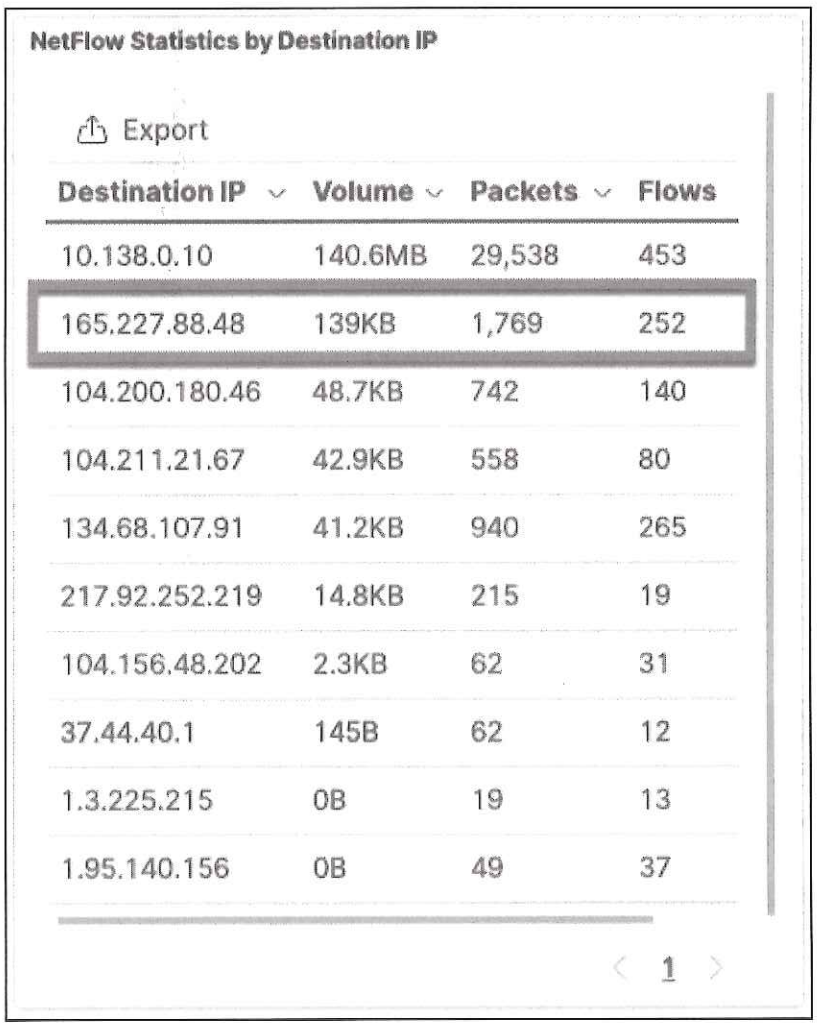
At approximately 2021-04-27 15:38:00 UTC there was a noticeable change in the quality of Flow records produced for outbound TCP 22 traffic.



https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

3. If you altered your search timeframe for the above question, reset it back to `2021-04-27 13:00 to 2021-04-27 21:00 UTC`.

> **There is one external destination IP address that appears to have a lot more TCP 22 traffic than any others within our Flow logs, what is it?**
>
> To narrow down the flow logs to only show outbound TCP 22 you would need to apply the `destination_port : 22 AND aprotocol.keyword : tcp` filter in the search bar.
>
> The IP address `165.227.88.48` appears to communicate a lot more than any of the other IP addresses in our Flow logs.



NetFlow Statistics by Destination IP

Export

Destination IP	Volume	Packets	Flows
10.138.0.10	140.6MB	29,538	453
165.227.88.48	139KB	1,769	252
104.200.180.46	48.7KB	742	140
104.211.21.67	42.9KB	558	80
134.68.107.91	41.2KB	940	265
217.92.252.219	14.8KB	215	19
104.156.48.202	2.3KB	62	31
37.44.40.1	145B	62	12
1.3.225.215	0B	19	13
1.95.140.156	0B	49	37

< 1 >

> As we're only looking for *external* IP addresses we would exclude the hosts own IP addresses of `10.138.0.10`

4. Given we are seeing a lot of outbound traffic TCP 22, let's narrow our search to only show outbound traffic from our suspicious VM.

> **Are there any other unusual outbound connections that we haven't already identified, and why have these not really appeared in our dashboards yet?**

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

If you `Add filter` for `source_ip is 10.138.0.10` we can filter to just look at outbound Flow logs.

Reviewing the dashboards widget for `NetFlow Volume by Destination Port` does show that `TCP 443`, however, when you filter on this traffic type you will notice that the overwhelming majority of this traffic is destine for Google. In fact, it's actually outbound HTTPS traffic from the VM back to Google's GCP. This is normal, and in fact is actually the means for how the logs from Lab 4.2 are produced. So you can exclude this traffic.

If you scroll further down to the individual Flow record entries at the bottom of the NetFlow dashboard, you will notice there are repeated `TCP 22` and `TCP 2222` connections.

NetFlow Discovery

1–50 of 71138

Time	exporter	aprotocol	source_ip	source_port	destination_ip	destination_port	total_bytes
2021-04-27 19:59:55.606Z	10.138.0.10	tcp	10.138.0.10	48706	95.78.102.16	2222	0
2021-04-27 19:59:53.627Z	10.138.0.10	tcp	10.138.0.10	40836	104.211.21.67	22	1,283
2021-04-27 19:59:53.558Z	10.138.0.10	tcp	10.138.0.10	42490	95.78.102.16	22	0
2021-04-27 19:59:53.302Z	10.138.0.10	tcp	10.138.0.10	53992	223.25.244.180	2222	0
2021-04-27 19:59:53.261Z	10.138.0.10	tcp	10.138.0.10	37932	58.200.62.1	2222	0
2021-04-27 19:59:53.046Z	10.138.0.10	tcp	10.138.0.10	60866	222.227.59.253	2222	0
2021-04-27 19:59:52.534Z	10.138.0.10	tcp	10.138.0.10	41570	77.150.54.73	2222	0
2021-04-27 19:59:52.534Z	10.138.0.10	tcp	10.138.0.10	51228	37.136.186.196	22	0
2021-04-27 19:59:52.410Z	10.138.0.10	tcp	10.138.0.10	44442	175.105.210.80	2222	0

The reason that the `TCP 2222` traffic doesn't appear in the ring graphs we've looked at so far, is because the is very little amount of bytes actually transmitted in the `TCP 2222` requests, therefore this is no traffic volume in them. However, they would have produced `SYN TCP` packets on the network which is why that are capture in the Flow logs.

Bonus Questions: What Have You Just Found?

1. Based on what you've observed so far can you identify what may have occurred with the `comms-control` VM.

Based on the traffic you've seen, what are these connection indicative of?

Based on what we have observed in the traffic so far:

- Lots of concurrent connections to `TCP 22`
- Lots of concurrent connections to `TCP 2222`
- A lot of connections that didn't fully establish, based on them containing 0 bytes.
- Connections occuring rapidly
- One connection to an external IP address that contained more traffic than any other connections.

It's likely you are looking at malware traffic that is scanning the internet and has established a C2 connection back to IP `165.227.88.48`.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Can you determine what malware this may be simply from the network traffic?

This is actually a pretty hard question to answer with *only* Flow logs. The best we can do is speculate and collect intel for further analysis of the VM.

If you Google for `malware`, `linux`, `22`, and `2222`, you may come across this story (https://for509.com/uwld7), which seems to match up with the evidence we're seeing in the Flow logs.

Key Takeaways

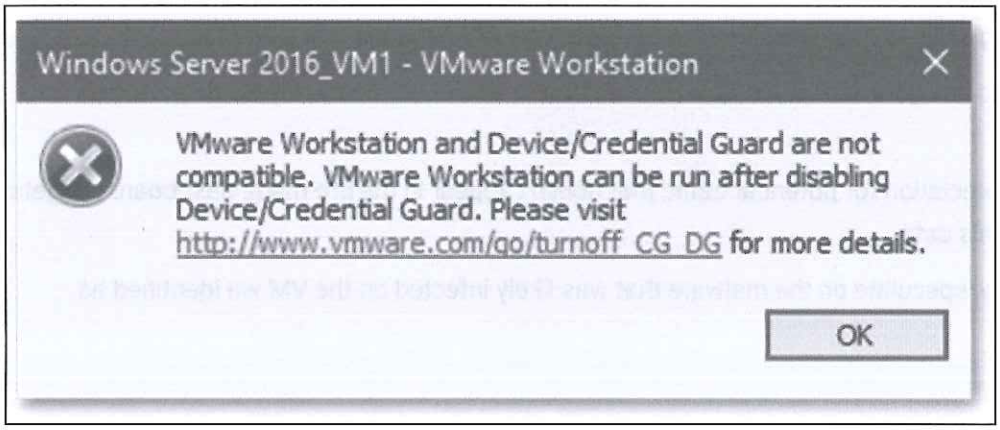
- You should now have a few strong skills to help you identify GCP Flow logs when loaded into SOF-ELK
- Students should now know how to navigate SOF-ELK's NetFlow dashboard to look for unusually traffic patterns originating from GCP VM's
- Students should also have an appreciation for potential traffic that doesn't appear in the pre-made dashboard widgets and now know how to check for this data.
- You should also be able to identify/speculate on the malware that was likely infected on the VM we identified as producing unusual traffic.

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

VMware Workstation/Credential Guard Incompatibility

If your Windows host system has Credential Guard enabled and you attempt to run VMware Workstation, there is an issue that may prevent you from using your VMware in class..

Upon running VMware Workstation, you may encounter a dialog such as below. You will not be able to start the application.



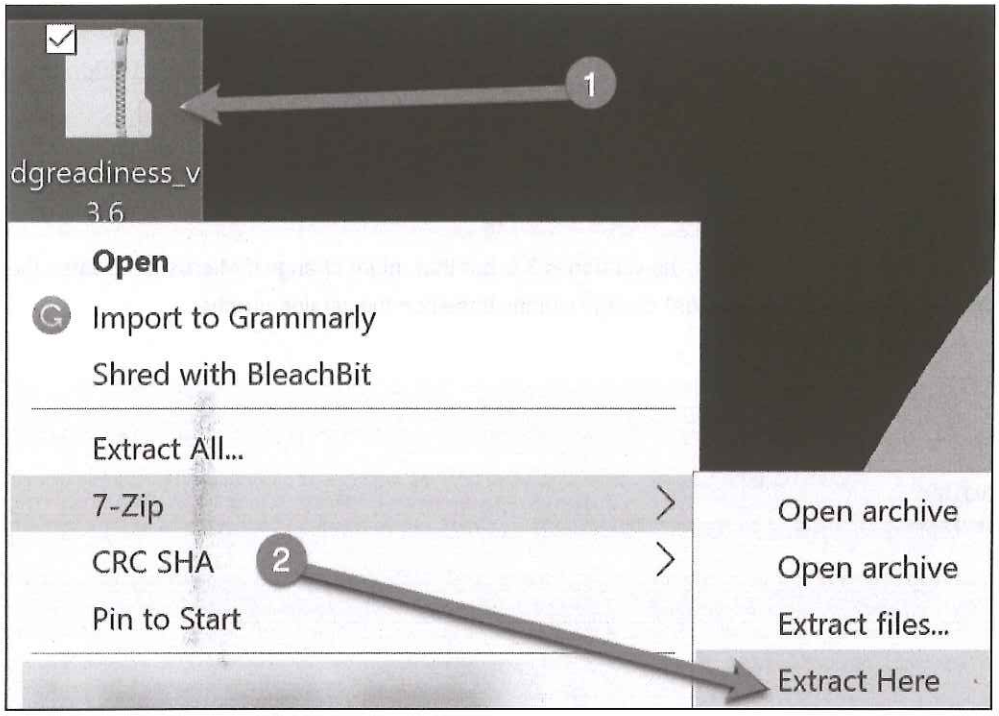
To correct this, take the following steps.

Disabling Credential Guard for Class

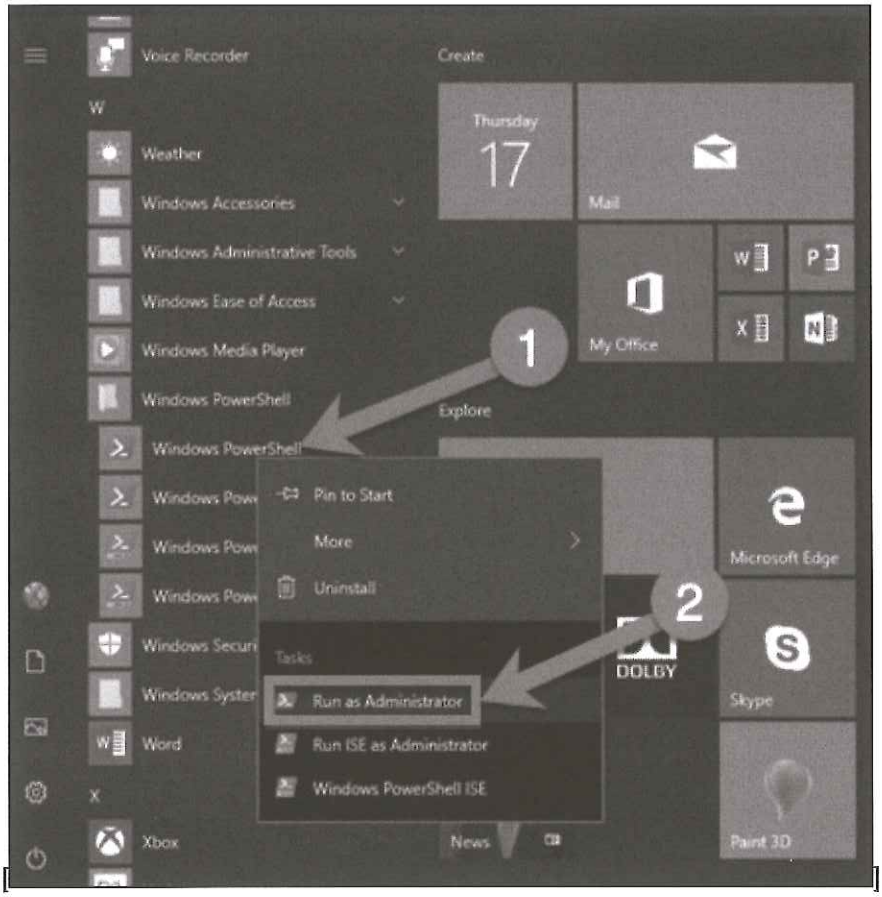
1. From your **host operating system**, Download the "Device Guard and Credential Guard hardware readiness tool" from Microsoft.
2. Move the downloaded zip file to your desktop and extract the zip file to your Desktop.

https://t.me/learningnets

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



3. Run PowerShell as Administrator.



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

4. In the PowerShell window, change the directory to the folder where the script is extracted and run the following PowerShell commands. For example, in the command below, the zip file was extracted to the Desktop folder. You may need to reboot your host system for the changes to take effect.

> **Note:**
>
> The exact version might change over time. In this example, the version is 3.6, but that might change if Microsoft updates the tool. If it does, in each command below, the folder path might change slightly based on the version number.

Command lines

```
cd ~\Desktop\dgreadiness_v3.6\
Set-ExecutionPolicy Unrestricted
```

Expected Results

```
Execution Policy Change
...
Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"):
```

Type `A` and press the Enter/Return key.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Command lines

```
.\DG_Readiness_Tool_v3.6.ps1 -Disable
```

Expected Results

```
Security Warning
...
Do you want to run C:\Users\<%YOUR_USERNAME%>\Desktop\dgreadiness_v3.6\DG_Readiness_Tool_v3.6.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (Default is "D"):
```

Type `R` and press the Enter/Return key.

Expected Results

```
...

################################################################################
Readiness Tool Version 3.4 Release
Tool to check if your device is capable to run Device Guard and Credential Guard
################################################################################
Disabling Device Guard and Credential Guard
Deleting RegKeys to disable DG/CG

...

Disabling Hyper-V and IOMMU
Disabling Hyper-V and IOMMU successful

Please reboot the machine, for settings to be applied.
```

Reboot as directed and your system should be ready for use.

Re-enabling Credential Guard After Class

When class is over, if you no longer need to use VMware Workstation and/or require Credential Guard to be enabled, follow these steps.

1. Run PowerShell as Administrator as shown above.
2. Run the following commands. You may need to reboot your host system for the changes to take effect.

Note:

The exact version might change over time. In this example, the version is 3.6, but that might change if Microsoft updates the tool. If it does, in each command below, the folder path might change slightly based on the version number.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Command lines

```
cd ~\Desktop\dgreadiness_v3.6\
.\DG_Readiness_Tool_v3.6.ps1 -Enable -CG
```

Expected Results

```
Security warning
...
Do you want to run C:\Users\<%YOUR_USERNAME%>\Desktop\dgreadiness_v3.6\DG_Readiness_Tool_v3.6.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (Default is "D"):
```

Type `R` and press the Enter/Return key.

Expected Results

```
################################################################################
Readiness Tool Version 3.4 Release
Tool to check if your device is capable to run Device Guard and Credential Guard
################################################################################
################################################################################
OS and Hardware requirements for enabling Device Guard and Credential Guard
 1. OS SKUs: Available only on these OS Skus - Enterprise, Server, Education, Enterprise IoT, Pro, and
Home
 2. Hardware: Recent hardware that supports virtualization extension with SLAT
To learn more, please visit: https://aka.ms/dgwhcr
################################################################################

Enabling Device Guard and Credential Guard
Setting RegKeys to enable DG/CG
Enabling Hyper-V and IOMMU
Enabling Hyper-V and IOMMU successful
Please reboot the machine, for settings to be applied.
```

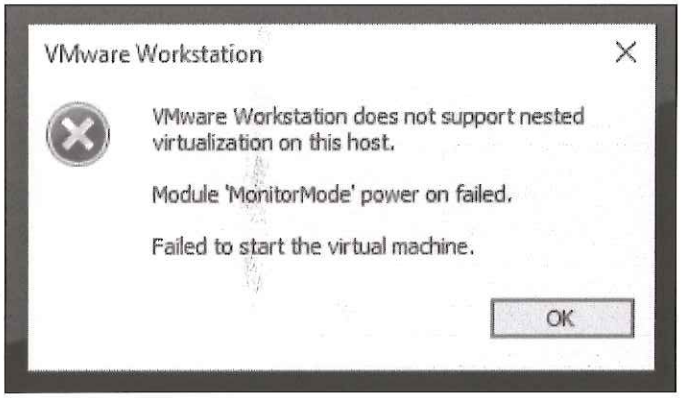
Reboot as directed and your system should be ready for use.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

VMware Workstation/Hyper-V Incompatibility

If your Windows host system has Hyper-V enabled and you are running Windows 10 version 2004, there is an issue that may prevent you from using your class VM(s) in VMware Workstation 15.5.5.

Upon starting your class virtual machine(s), you may encounter a dialog such as below. You will not be able to start the virtual machine.

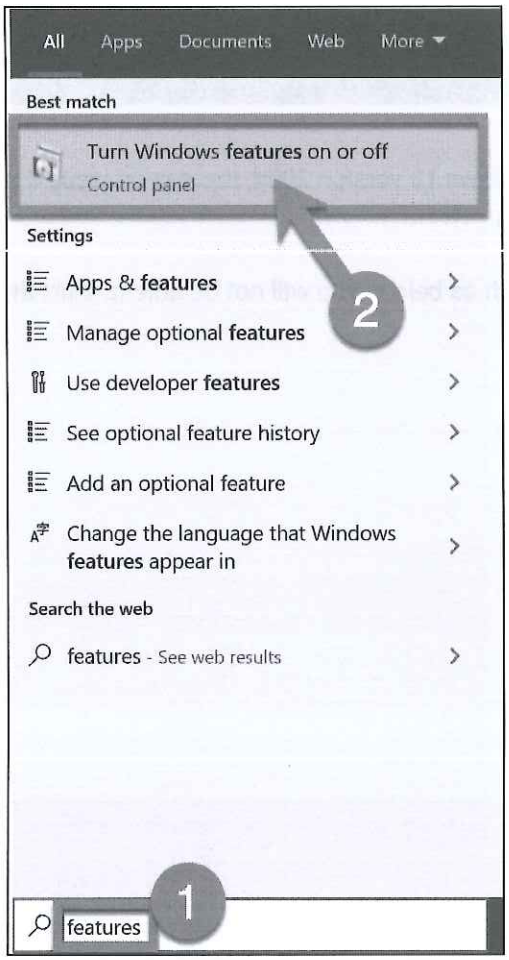


To correct this, take the following steps.

Disabling Hyper-V Features for Class

1. If needed, disable Credential Guard using these instructions
2. Click the Windows button and type `features`. Then click on the result titled `Turn Windows Features on or off`.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon



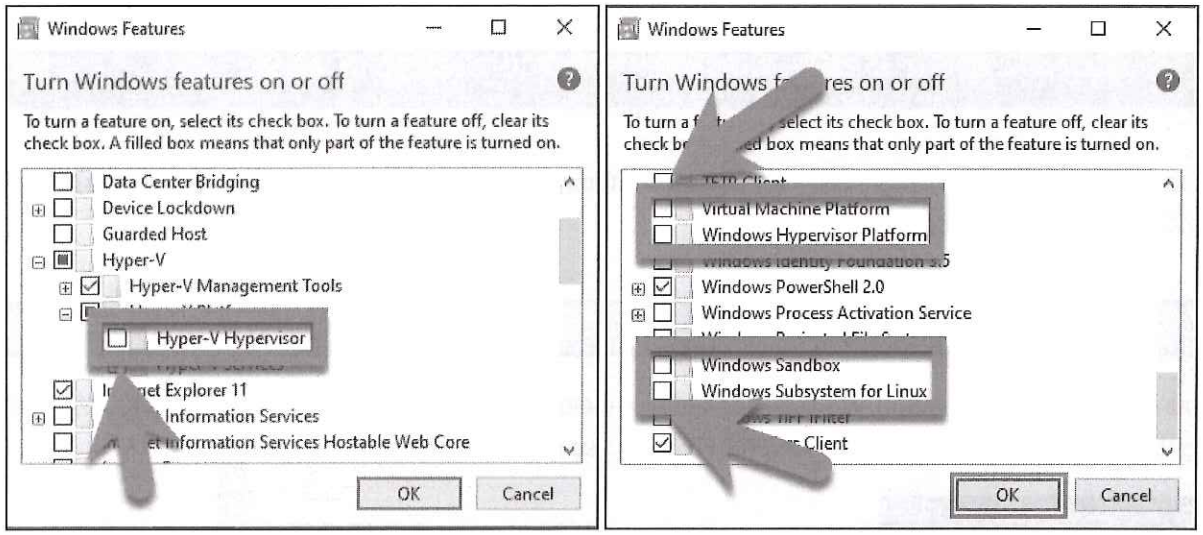
3. Ensure that the following options are unchecked:

> ⚠ **WARNING!**
>
> Keep track of which of the following options you need to change for the class. When class is over, you'll need to re-enable any options you have disabled.

- `Hyper-V Hypervisor`
- `Windows Hypervisor Platform`
- `Virtual Machine Platform`
- `Windows Sandbox`
- If you are using the Windows Subsystem for Linux 2 (WSL2), ensure that the `Windows Subsystem for Linux` option is also unchecked.

Click `OK`.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
https://t.me/learningnets
Technet24



4. Your system will ask to reboot so the changes will take effect.

Re-enabling Hyper-V Features After Class

When class is over and you no longer need to use the class virtual machine, re-enable the options that you disabled above. If you disabled Credential Guard, re-enable it with the instructions provided here.

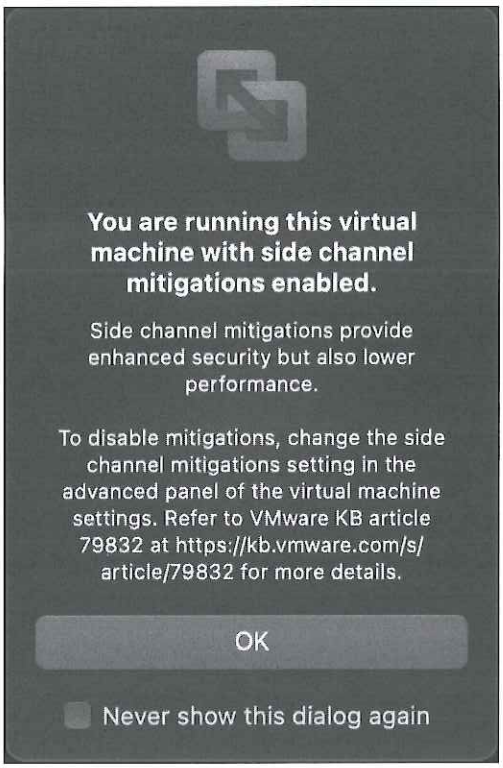
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

VMware Fusion Issues with macOS 11 (Big Sur)

With the update to macOS 11 (Big Sur), there are a few issues that may prevent you from using your class VM(s) in VMware Fusion 12. This document addresses these issues.

"Side Channel Mitigations" Error Message

Upon starting your class virtual machine(s), you may encounter a dialog such as below. You can safely click OK in order to continue running the affected virtual mahchine, however you may see degraded performance as a result.



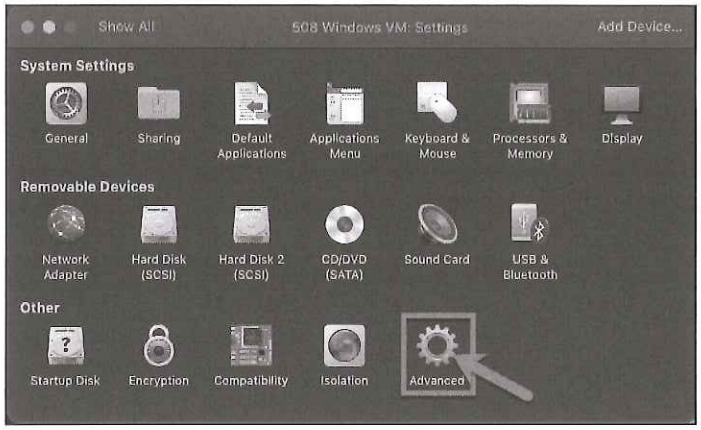
To overcome any performance issues take the following steps.

1. Shut down the virtual machine. (Not "Suspend".)
2. Click on the `Virtual Machine` menu item. Then click `Settings...`.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

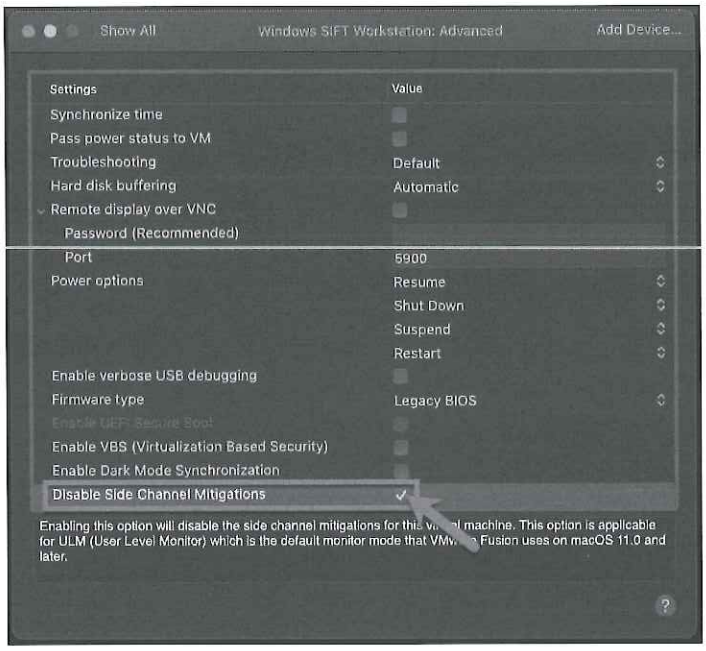


3. Click the **Advanced** icon.



4. Check the box next to **Disable Side Channel Mitigations**

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



5. Close the Settings dialog and start the virtual machine.

"Virtualized Performance Counters" Error Message

Upon starting your class virtual machine(s), you may encounter a dialog such as the one below. You will not be able to start the virtual machine.



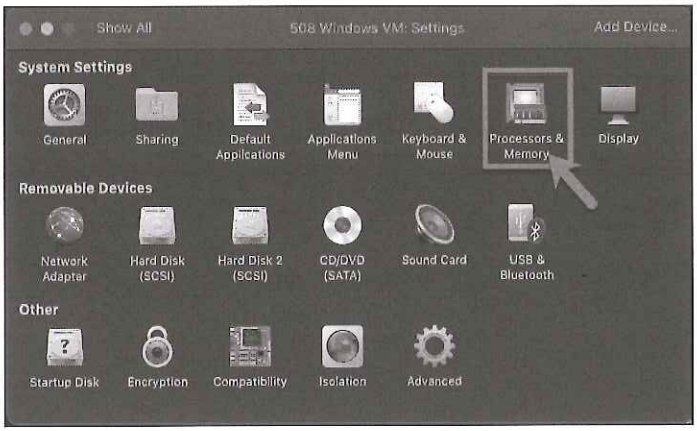
To correct this, take the following steps.

1. Click on the `Virtual Machine` menu item. Then click `Settings...`.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

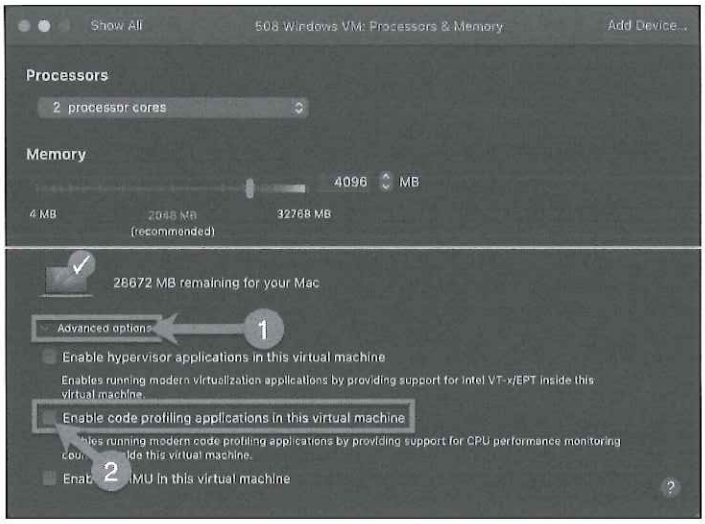


2. Click the `Processors & Memory` Icon.



3. Click the arrow to expand the `Advanced options` section. Then un-check the box next to `Enable code profiling applications in this virtual machine`.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



4. Close the Settings dialog and start the virtual machine.

"Nested Virtualization" Error Message

Upon starting your class virtual machine(s), you may encounter a dialog such as the one below. You will not be able to start the virtual machine.



To correct this, take the following steps.

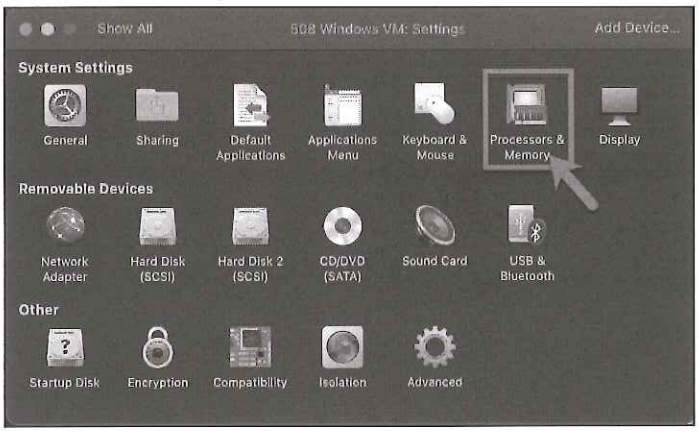
> ⚠ **WARNING!**
>
> While taking these steps will allow you to boot the virtual machine, you may not be able to complete any labs that rely on nested virtualization features. Contact your instructor or OnDemand support to determine if this affects your class.

1. Click on the `Virtual Machine` menu item. Then click `Settings...`.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

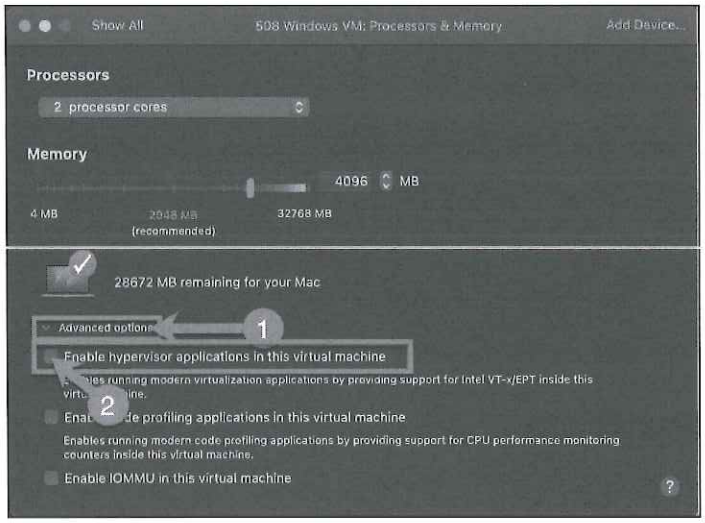


2. Click the `Processors & Memory` Icon.



3. Click the arrow to expand the `Advanced options` section. Then un-check the box next ot `Enable hypervisor applications in this virtual machine`.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon



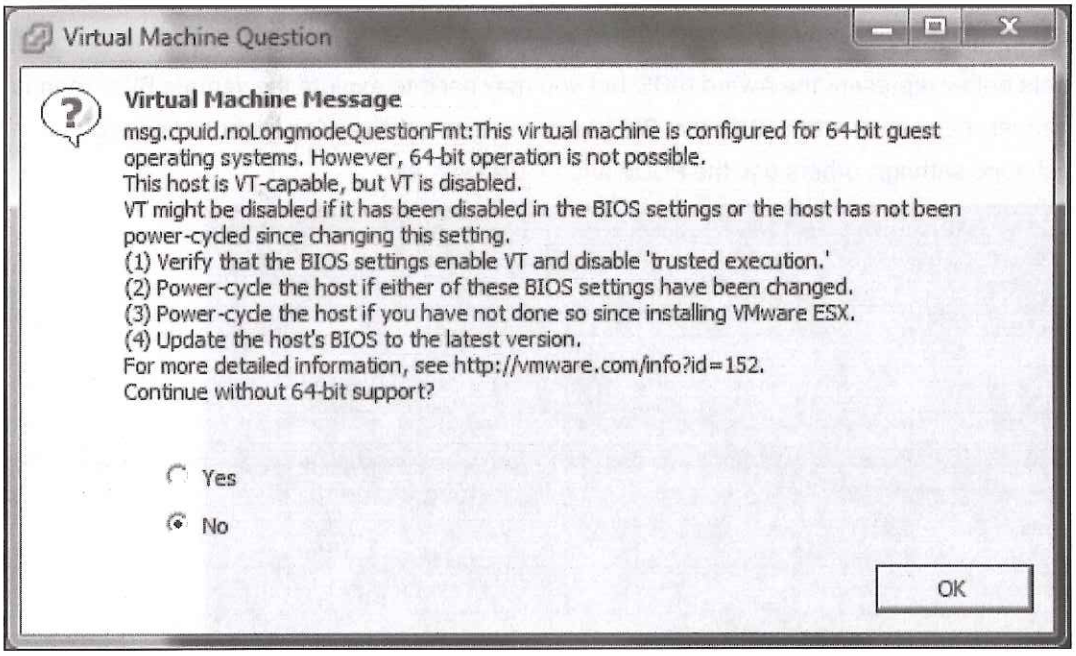
4. Close the Settings dialog and start the virtual machine.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

Enabling Virtualization Technology Extensions (VTx) in Intel and AMD BIOS

On Intel and AMD systems, there is a BIOS extension that must be enabled or you will not be able to boot your class VM(s) in VMware.

Upon starting your class virtual machine(s), you may encounter a dialog similar to the one below. Starting the virtual machine without 64-bit support will result in a non-functional VM.



To correct this, take the following steps.

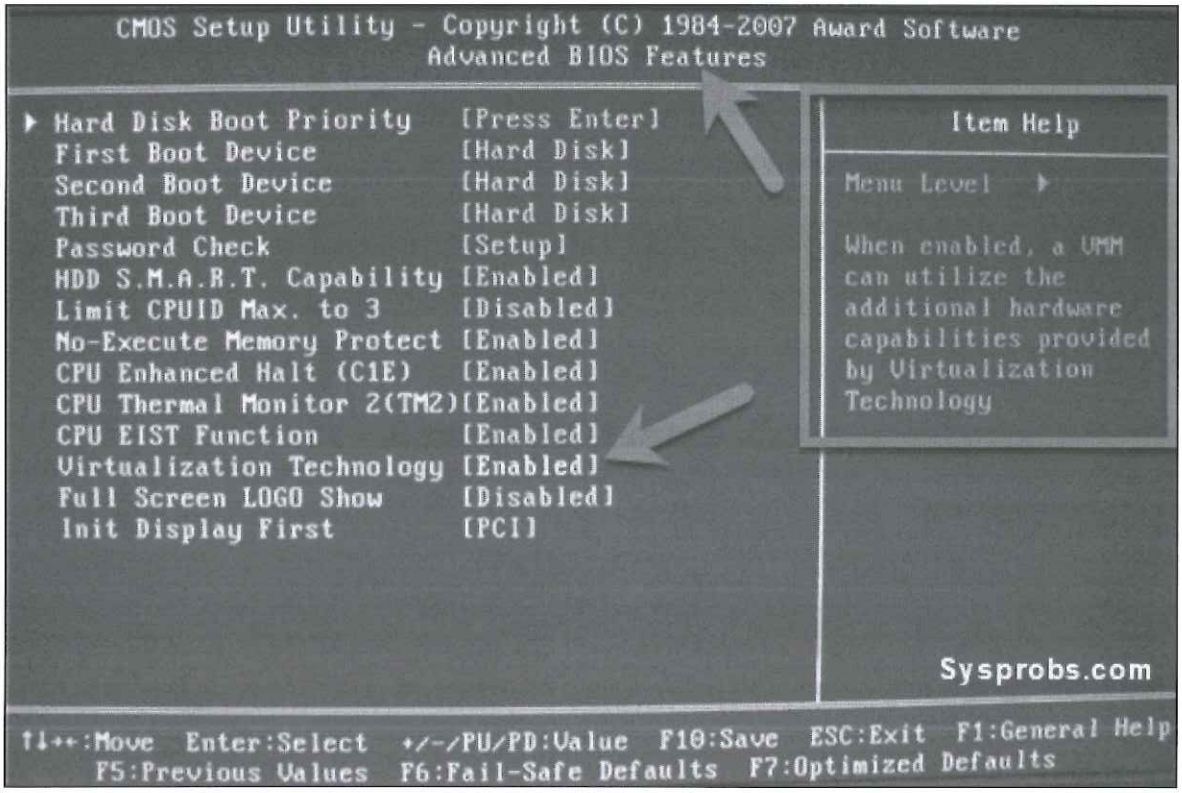
Enabling VTx for Class

1. Enter your system's BIOS configuration menus. This requires pressing a designated key immediately upon booting/rebooting your system, but the exact key depends on the system and BIOS manufacturers. Most systems use one of the following five keys:
    - F1
    - F2
    - DEL
    - ESC
    - F10

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

- Older computers may require multiple keys to be pressed simultaneously, or keys other than those listed above:
  - CTRL+ALT+ESC
  - CTRL+ALT+INS
  - CTRL+ALT+ENTER
  - CTRL+ALT+S
  - PGUP
  - PGDN

2. Identify the BIOS menu that controls the VTx settings. This is also dependent on the specific version of BIOS that your system uses. The screenshots below represent the Award BIOS, but you may need to explore the various BIOS menus on your system to find the proper menu and setting. Different BIOS versions also have varying keyboard controls - some use the space bar to change settings, others use the PGUP and PGDN keys, etc.



Saving the settings may require pressing F10 or other keys or menu sequences.

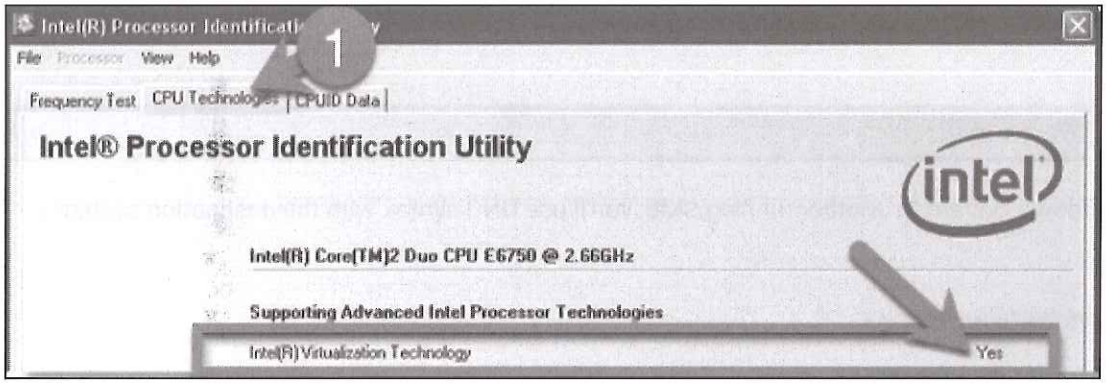
3. Exit the BIOS settings and reboot the system. Ideally, keep the power off for approximately one minute before powering it on to clear any residual configuration settings. The reboot is critical, as the BIOS settings are essentially a configuration file that is only read at boot time.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24

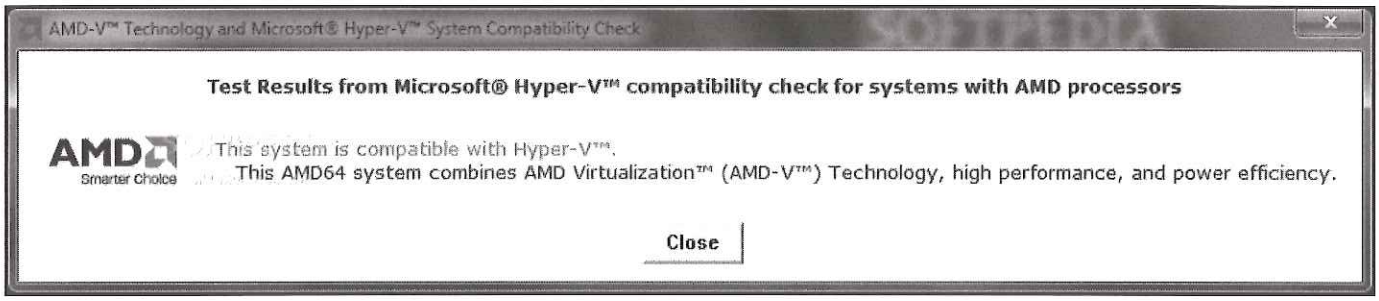
Verifying That VTx Settings are Correct

There are several ways to verify that the VTx settings above have been set correctly.

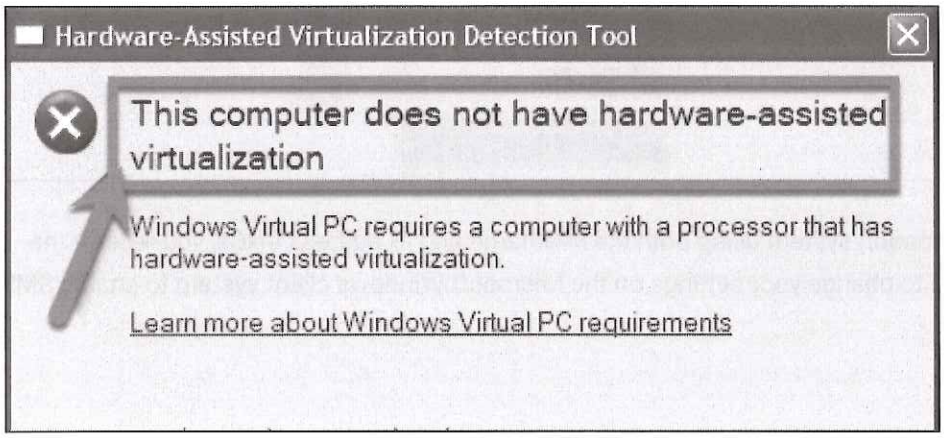
1. Boot your class VM(s) to ensure the VTx error at the beginning of this document is not displayed.
2. For Intel processors, you may download the Intel Processor Identification Utility. Run the utility and click the `CPU Technologies` tab to confirm if VTx is enabled or not.



3. For AMD processors, you may download the AMD Virtualization Technology and Microsoft Hyper-V System Compatibility Check Utility. Run the utility to confirm if VTx is enabled or not.



4. For both Intel and AMD processors, you may download Microsoft's Hardware-Assisted Virtualization Detection Tool. Run the utility to confirm if VTx is enabled or not.



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

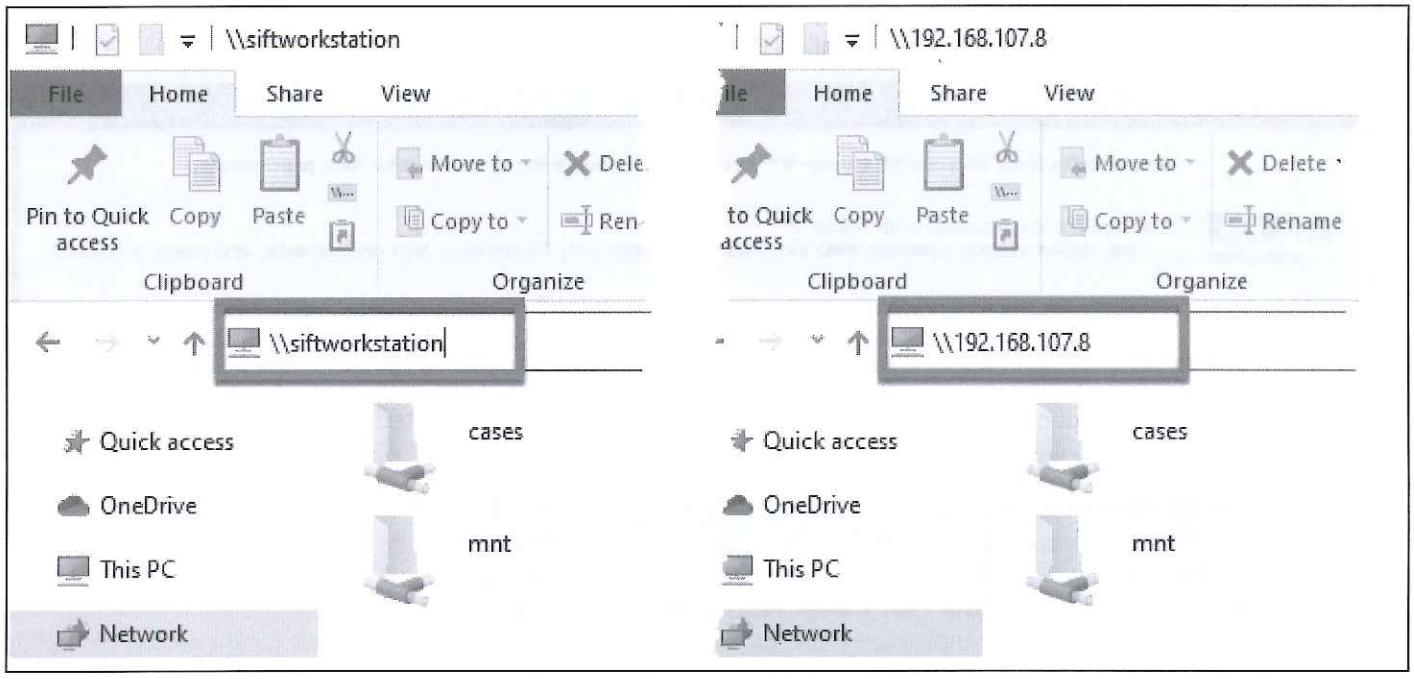
Windows File Sharing Issues

During your class, you may wish to share or copy files between your host system and a virtual machine or between virtual machines. One method of doing this is to use Microsoft Windows's native file sharing features, known as SMB. Tools that provide SMB functionality are available for Windows, macOS, and Linux operating systems. If you wish to use SMB to share files from a Windows client system, you'll need to follow the steps in this document to adjust the security settings. Using a macOS or Linux client system does not require these measures.

Using UNCs for SMB Sharing

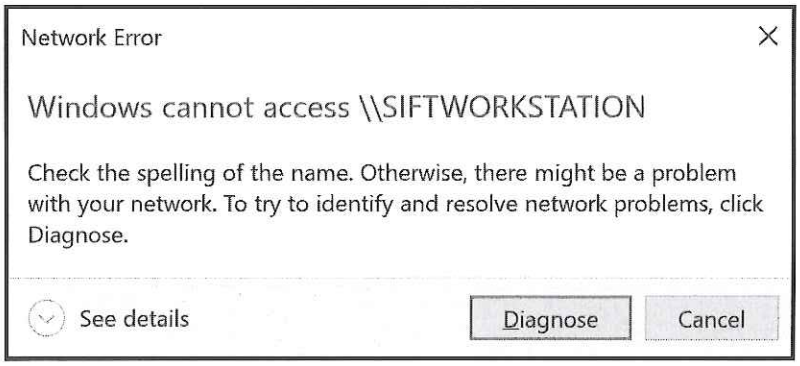
To connect from one Windows system to another running SMB, you'll use UNC syntax with the destination system's hostname or IP address:

- `\\<%DESTINATION_SYSTEM_HOSTNAME%>\`
- `\\<%DESTINATION_SYSTEM_IP_ADDRESS%>\`



If, after attempting to access the destination system using both the hostname and IP address UNCs, you receive the following error message, you will need to change your settings on the Microsoft Windows client system to enable SMB functionality.

© 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



First Troubleshooting Approach

The following PowerShell one-liner is often all that is needed to fix the above error. Run this command before doing moving forward with any other steps.

Run this command from an Administrator PowerShell Terminal.

Command lines

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"
AllowInsecureGuestAuth -Type DWORD -Value 1 -Force
```

If the command runs successfully, no results will be displayed in the PowerShell terminal.

Close and restart Windows Explorer and re-test your connection to file share. If you still receive the error message, see the additional troubleshooting steps below.

Additional Troubleshooting Approaches

If SMB sharing still is not working after running the above PowerShell one-liner, one or more of the following steps may be required.

1. Verify Lanman Workstation `AllowInsecureGuestAuth` Setting This PowerShell command will display the current Lanman Workstation `AllowInsecureGuestAuth` registry key. This MUST be set to `1` for Windows File Sharing to function.

   Run this command from an Administrator PowerShell Terminal.

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Command lines

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" | format-
list -property AllowInsecureGuestAuth
```

Expected Results

```
AllowInsecureGuestAuth : 1
```

If this returns a value of `0` instead, run the PowerShell one-liner in the First Troubleshooting Approach section above.

2. Verify the destination machine's IP address

   The network interface name can vary from system to system, and some systems will have more than one interface. You will need to know which interface is being used for SMB access. Your TA, SME, or instructor can assist you if you're unsure which interface is being used.

   Log in to the destination system.

   a. If the destination system is running Linux:

https://t me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Command lines

```
ip address
```

Notional results

```
    1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
    2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
1000
        link/ether 00:0c:29:3a:47:73 brd ff:ff:ff:ff:ff:ff
        inet 192.168.107.8/24 brd 192.168.107.255 scope global dynamic noprefixroute ens33
        valid_lft 85518sec preferred_lft 85518sec
        inet6 fd15:4ba5:5a2b:1008:35c7:81c:372d:e121/64 scope global temporary dynamic
        valid_lft 604786sec preferred_lft 86054sec
        inet6 fd15:4ba5:5a2b:1008:76b7:6100:3d57:95e9/64 scope global dynamic mngtmpaddr
noprefixroute
        valid_lft 2591985sec preferred_lft 604785sec
        inet6 fe80::ceae:7a20:f025:62b6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
    3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
        link/ether 02:42:24:25:69:75 brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

In this case, the interface `ens33` is the only one used for the VM's services and its IP address is `192.168.107.8`, indicated by the following line: inet 192.168.107.8/24 ...

b. If the destination system is running Windows:

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Command lines

```
ipconfig
```

Notional results

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : sansgear.com
IPv6 Address. . . . . . . . . . . : fd15:4ba5:5a2b:1008:9c14:e101:232:5a1c
Temporary IPv6 Address. . . . . . : fd15:4ba5:5a2b:1008:8b4:b370:203b:a766
Temporary IPv6 Address. . . . . . : fd15:4ba5:5a2b:1008:a426:af82:6efc:488
Link-local IPv6 Address . . . . . : fe80::9c14:e101:232:5a1c%12
IPv4 Address. . . . . . . . . . . : 192.168.107.2
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::472:1446:5c3d:7670%12
                                    192.168.107.1
```

In this case, the IP address is `192.168.107.2`, indicated by the following line:

```
IPv4 Address. . . . . . . . . . . : 192.168.107.2
```

3. Allow File and Print Sharing through the firewall

   The simplest approach is to turn off the Windows Firewall entirely while you are in the classroom environment. The following command will accomplish this.

   Run this command from an Administrator PowerShell Terminal or Administrator Command Prompt.

Command lines

```
netsh advfirewall set allprofiles state off
```

Expected results

```
Ok.
```

To re-enable the firewall after class, run the same command with `on` instead of `off`.

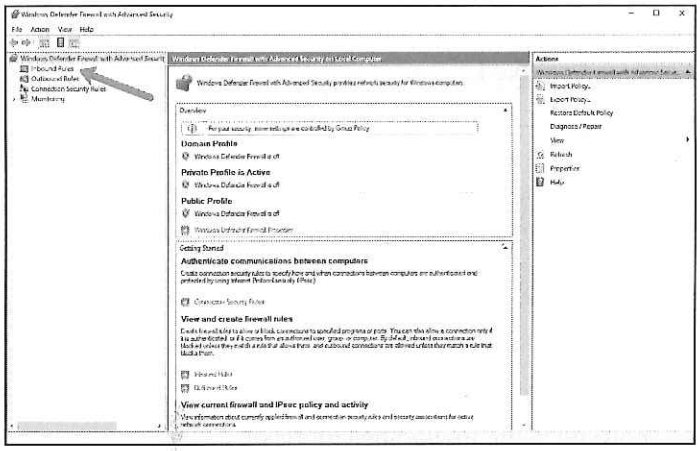
If you are not able to disable the firewall completely, you can open only the file and print sharing ports.

a. Open Control Panel, click System and Security, and then click Windows Firewall.

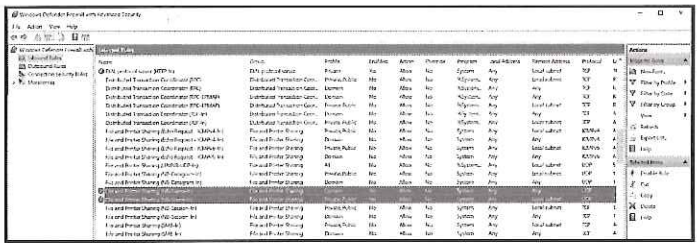
b. In the left pane, click Advanced settings, and in the console tree, click Inbound Rules.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

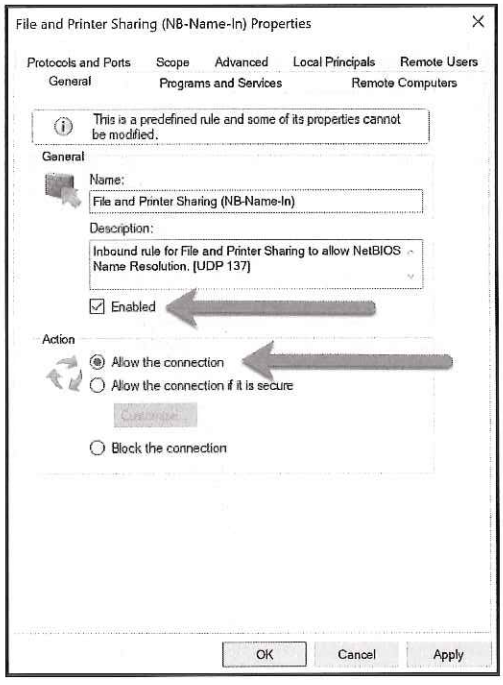
Technet24



c. Under Inbound Rules, locate the rules `File and Printer Sharing (NB-Session-In)` and `File and Printer Sharing (SMB-In)`.



d. For each rule, right-click the rule, and then click `Enabled` checkbox and `Allow the connection` option. Click the "OK" button.



4. Ensure SMB2 is enabled

 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

SMB version 2 (SMB2) is required for file sharing and is typically enabled by default. The following command will ensure SMB2 is enabled and will have no effect if it is alread enabled.

Run this command from an Administrator PowerShell Terminal.

Command lines

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Value 1 -
Force
```

If the command runs successfully, no results will be displayed in the PowerShell terminal.

5. Verify all SMB configuration options

   If you have completed all of the steps above and are still unable to use the SMB service, the following command will produce output that may be helpful in more exhaustive troubleshooting.

   Run this command from an Administrator PowerShell Terminal.

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon

Technet24

Command lines

```
Get-SMBServerConfiguration
```

Notional results

```
AnnounceComment                 :
AnnounceServer                  : False
AsynchronousCredits             : 64
AuditSmb1Access                 : False
AutoDisconnectTimeout           : 15
AutoShareServer                 : True
AutoShareWorkstation            : True
CachedOpenLimit                 : 10
DurableHandleV2TimeoutInSeconds : 180
EnableAuthenticateUserSharing   : True
EnableDownlevelTimewarp         : False
EnableForcedLogoff              : True
EnableLeasing                   : True
EnableMultiChannel              : True
EnableOplocks                   : True
EnableSecuritySignature         : False
EnableSMB1Protocol              : True
EnableSMB2Protocol              : True
EnableStrictNameChecking        : True
EncryptData                     : False
IrpStackSize                    : 15
KeepAliveTime                   : 2
MaxChannelPerSession            : 32
MaxMpxCount                     : 50
MaxSessionPerConnection         : 16384
MaxThreadsPerQueue              : 20
MaxWorkItems                    : 1
NullSessionPipes                :
NullSessionShares               :
OplockBreakWait                 : 35
PendingClientTimeoutInSeconds   : 120
RejectUnencryptedAccess         : True
RequireSecuritySignature        : False
ServerHidden                    : True
Smb2CreditsMax                  : 2048
Smb2CreditsMin                  : 128
SmbServerNameHardeningLevel     : 0
TreatHostAsStableStorage        : False
ValidateAliasNotCircular        : True
ValidateShareScope              : True
ValidateShareScopeNotAliased    : True
ValidateTargetName              : True
```

https://t.me/learningnets
© 2021 Pierre Lidome, David Cowen, and Josh Lemon

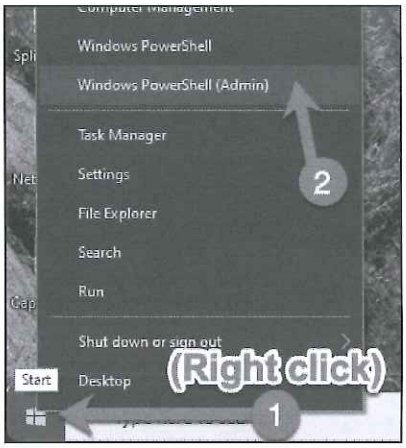
Running Administrator Terminal/Prompt

The steps in this document may require either an Administrator PowerShell Terminal or a Windows Command Prompt. To access these, use the following instructions.

1. Administrator PowerShell Terminal

   a. Right click the Windows Start Icon on the bottom left of your Task Bar.

   b. Select Windows PowerShell (Admin) from the Menu.



   c. You may see a dialog requesting permission to make changes on your device. Click `Yes` .



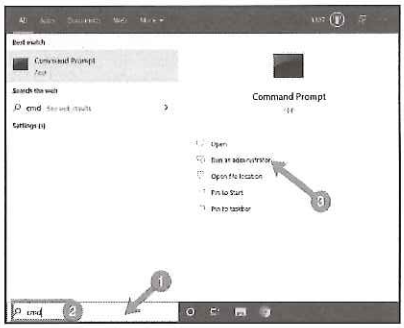
2. Administrator Command Prompt

   a. Click the Windows search box or the Windows search icon (magnifying glass) on the bottom left of your Task Bar.

   b. Type `cmd` in the search box.

   c. Select `Run as Administrator` .

https://t.me/learningnets © 2021 Pierre Lidome, David Cowen, and Josh Lemon
Technet24



d. You may see a dialog requesting permission to make changes on your device. Click `Yes` .



 © 2021 Pierre Lidome, David Cowen, and Josh Lemon

https://t.me/learningnets

Technet24

"As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned."
Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

SANS Programs
sans.org/programs

GIAC Certifications
Graduate Degree Programs
NetWars & CyberCity Ranges
Cyber Guardian
Security Awareness Training
CyberTalent Management
Group/Enterprise Purchase Arrangements
DoDD 8140
Community of Interest for NetSec
Cybersecurity Innovation Awards

Search SANSInstitute

SANS Free Resources
sans.org/security-resources

- E-Newsletters
  NewsBites: Bi-weekly digest of top news
  OUCH!: Monthly security awareness newsletter
  @RISK: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary

SANS Institute
8120 Woodmont Avenue | Suite 310
Bethesda, MD 20814
301.654.SANS(7267)
info@sans.org

https://t.me/learningnets