HideZeroOne
INE – Cyber Sec
www.hide01.ir

Incident Handling & Response Professional

Creating a Baseline & Detecting Deviations

Section 04 | Module 05

OUTLINE

Table of Contents

Module 05 | Creating a Baseline & Detecting Deviations

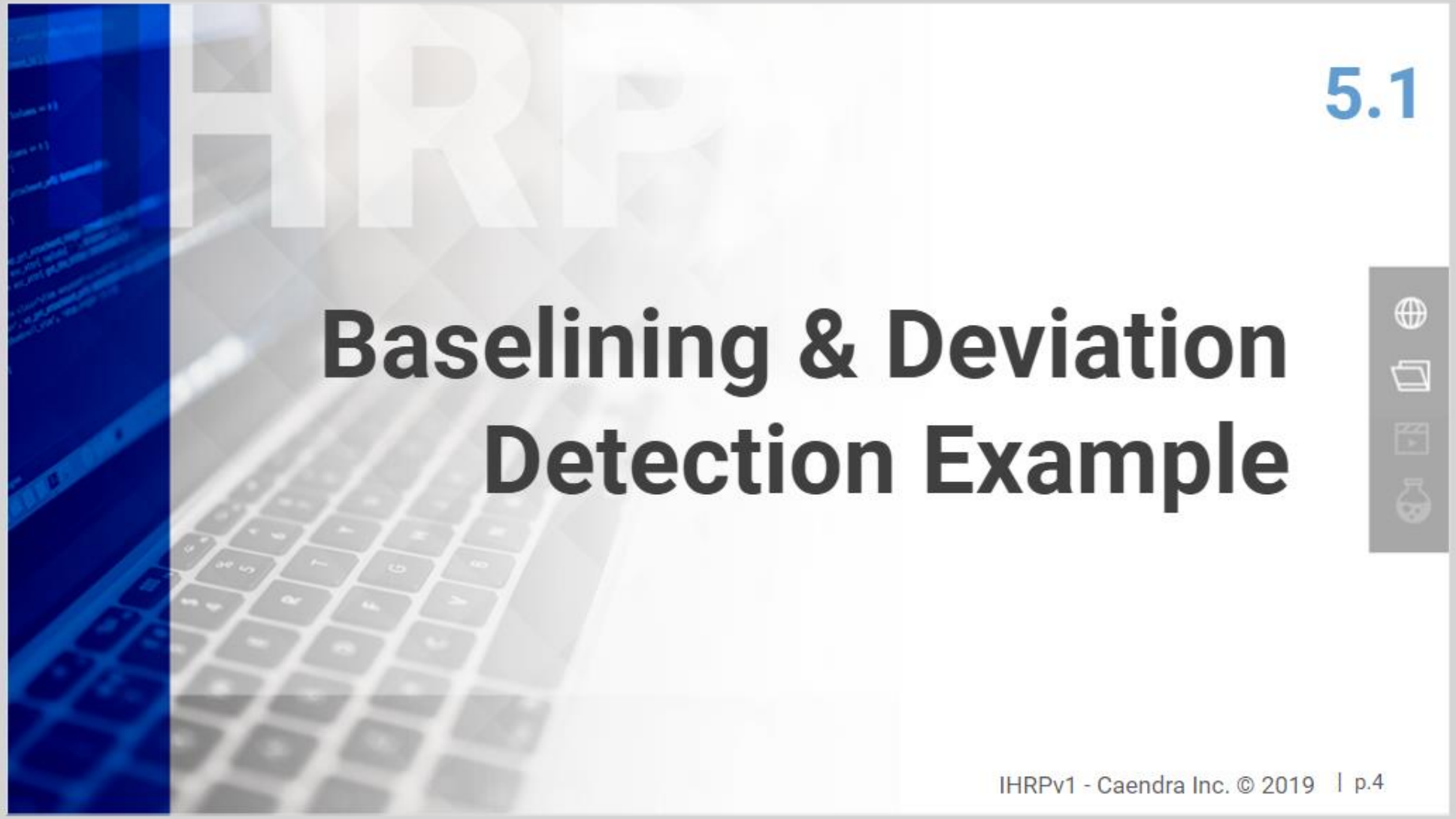
5.1 Baselining & Deviation Detection Example

OUTLINE

Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ How a basic baselining methodology can result in better intrusion detection



5.1

Baselining & Deviation Detection Example

OUTLINE

5.1 Baselining & Deviation Detection Example

Knowing the normal state of an environment can result in effortless abnormality detection.

Baselining can be performed everywhere, from network connections and filesystem interactions to user behavior.

OUTLINE

5.1 Baselining & Deviation Detection Example

Great examples of detecting deviations through baselinining are the ELK and Splunk visualizations we have come across so far in the course.

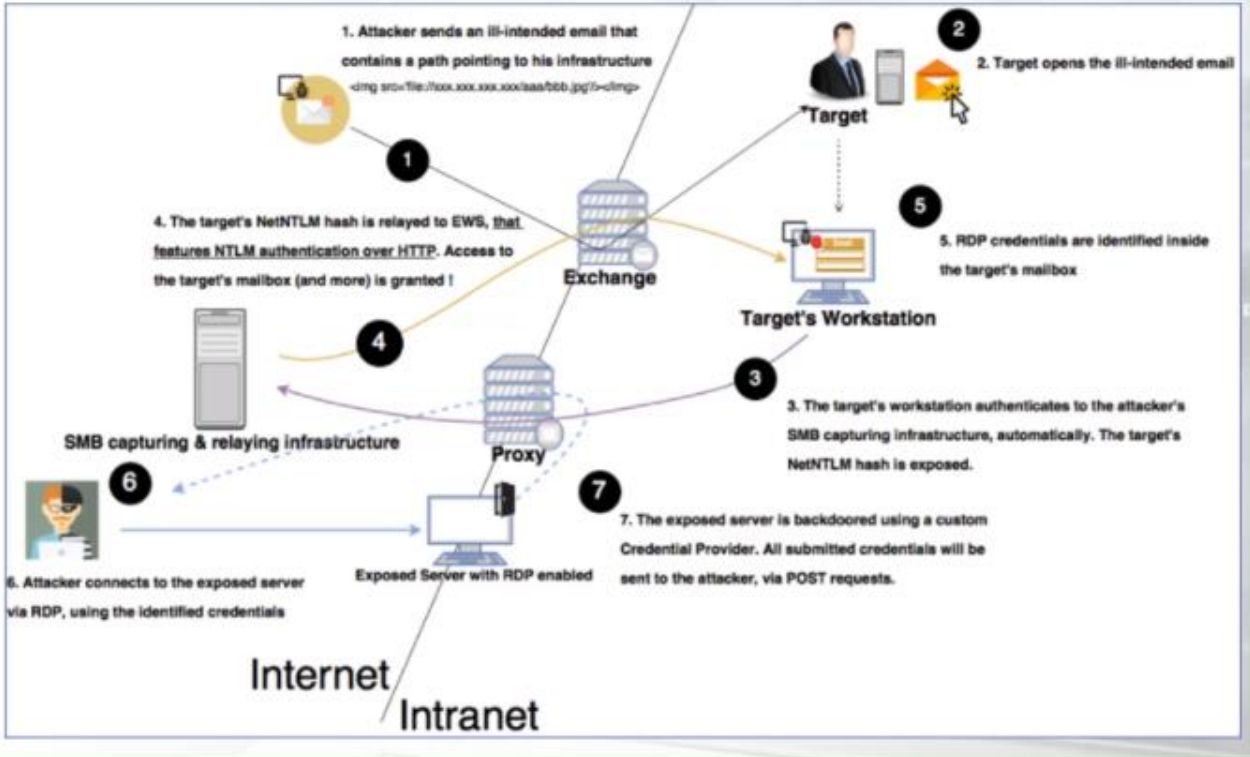
To better understand how baselining works go through the following example.

5.1.1 RDP Activity Baselining

Microsoft Terminal Services Remote Desktop Protocol (RDP) is being heavily used by IT Administrators and personnel worldwide for interactively using a remote Windows system.

Unfortunately, credential theft has oftentimes resulted in attackers moving laterally through RDP. Find an example of such an attack in the following slide.

5.1.1 RDP Activity Baselining



OUTLINE

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ How can we create a baseline?
- ❑ Are there any events that can help us in our tracking activities?
- ❑ Is log enrichment required?
- ❑ How can we automate this?

OUTLINE

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ **What do we want to monitor?**
- ❑ How can we create a baseline?
- ❑ Are there any events that can help us in our tracking activities?
- ❑ Is log enrichment required?
- ❑ How can we automate this?

OUTLINE

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ **What do we want to monitor?**
- ❑ How can we create a baseline?
- ❑ Are there any events that can help us in our tracking activities?
- ❑ Is log enrichment required?
- ❑ How can we automate this?

We want to monitor RDP activity.

OUTLINE

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ **How can we create a baseline?**
- ❑ Are there any events that can help us in our tracking activities?
- ❑ Is log enrichment required?
- ❑ How can we automate this?

OUTLINE

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ **How can we create a baseline?**
- ❑ Are there any events that can help us in our tracking activities?
- ❑ Is log enrichment required?
- ❑ How can we automate this?

To create a baseline, we first need to identify how normal RDP activity looks like in our network and then create detections based on abnormal actions.

Questions to help us with that are:

1. Does the ABC or XYZ department (network segment) typically use RDP?
2. Do any of our ABC colleagues RDP to a remote Windows system in XYZ?
3. Do any of our ABC or XYZ colleagues RDP to more than one systems?
4. Do ABC or XZY departments typically see any inbound RDP traffic?
5. Do IT administrators always RDP from systems belonging to the organization's intranet?
6. Do any of our critical servers have logon entries from systems outside the organization?
7. Do any of our critical servers have RDP logon entries that can be associated with ABC or XYZ user accounts ?
8. Is it normal to see a single user account RDPing from multiple systems?

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ How can we create a baseline?
- ❑ **Are there any events that can help us in our tracking activities?**
- ❑ Is log enrichment required?
- ❑ How can we automate this?

OUTLINE

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ How can we create a baseline?
- ❑ **Are there any events that can help us in our tracking activities?**
- ❑ Is log enrichment required?
- ❑ How can we automate this?

According to https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf we can focus on the following events at the destination system.

- EID 21 and EID 25 which reside in the "*TerminalServices-LocalSessionManager*" log, commonly located at *"%systemroot%\Windows\System32\winevt\Logs\Microsoft-TerminalServices-LocalSessionmanager%3Operational.evtx"*
- EID 4624 entries of Type 10 logons which reside in the "Security" log, commonly located at *"%systemroot%\Windows\System32\winevt\Logs\Security.evtx"*

All collected data should then be sent for frequency analysis. Metrics should be generated per user accounts, RDP-initiating systems and destination systems.

https://technet.microsoft.com/en-us/library/ee891131(ws.10).aspx
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee891126(v=ws.10)
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee891126(v%3dws.10)

OUTLINE

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ How can we create a baseline?
- ❑ Are there any events that can help us in our tracking activities?
- ❑ **Is log enrichment required?**
- ❑ How can we automate this?

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ How can we create a baseline?
- ❑ Are there any events that can help us in our tracking activities?
- ❑ **Is log enrichment required?**
- ❑ How can we automate this?

For optimum results the collected data (such as the source network addresses) should be enriched with DHCP logs, so that an actionable mapping can be performed. By mapping we mean associating IP addresses to hostnames.

In addition, identifying which systems are associated with user accounts or departments is also important.

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ How can we create a baseline?
- ❑ Are there any events that can help us in our tracking activities?
- ❑ Is log enrichment required?
- ❑ **How can we automate this?**

5.1.1 RDP Activity Baselining

Let's create a baselining methodology.

- ❑ What do we want to monitor?
- ❑ How can we create a baseline?
- ❑ Are there any events that can help us in our tracking activities?
- ❑ Is log enrichment required?
- ❑ **How can we automate this?**

Through SIEM searches and correlations that will perform RDP-related metrics per user, per RDP-initiating system and per destination system, we can automate tracking deviations from the norm.

Such metrics are:

- RDP-initiating systems per user
- RDP destination systems per user
- Total RDP logons per destination system
- Destination systems for each RDP-initiating system etc.

Please refer to the following resource to further study the associated events.

https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/

https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/

OUTLINE

5.1.2 RDP Lateral Movement Detection (Bonus)

Note that every interactive session creates numerous forensics artifacts. Digital forensics analysts can leverage shellbags to reconstruct every directory viewed interactively by attackers.

https://www.magnetforensics.com/blog/forensic-analysis-of-windows-shellbags/

OUTLINE

References

OUTLINE

References

Detecting Lateral Movement through Tracking Event Logs

https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf

EID 21

https://technet.microsoft.com/en-us/library/ee891131(ws.10).aspx

EID 25

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee891126(v=ws.10)

EID 4624

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

References

Windows RDP-Related Event Logs: Identification, Tracking, and Investigation

https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/

Forensic Analysis of Windows Shellbags

https://www.magnetforensics.com/blog/forensic-analysis-of-windows-shellbags/