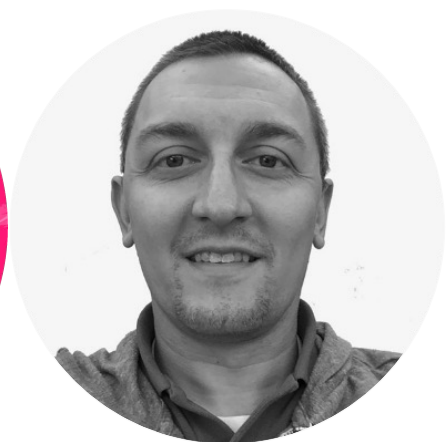


Active Defense with Powershell

Active Defense Principles



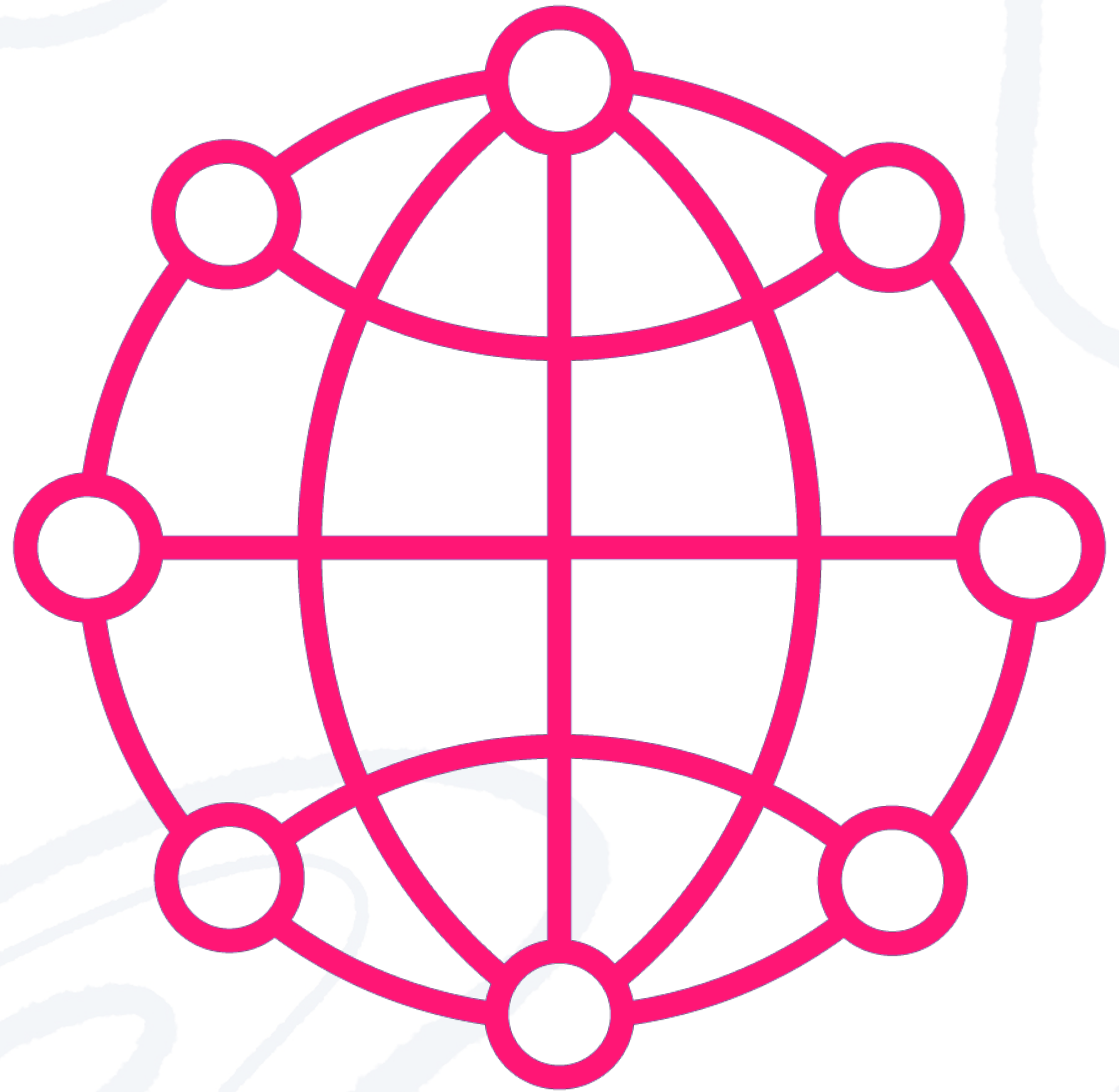
Michael Woolard

Risk and Compliance Manager

@wooly6bear | <https://wooly6bear.wordpress.com>



Overview



Course Agenda

Principles of Active Defense

Traps

Auditing



What Does Active Defense Mean?



Where Traditional Defense Falls Short

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

[About & Contact](#)

[Feedback](#)

[CVE Help](#)

[FAQ](#)

[Articles](#)

External Links :

[NVD Website](#)

[CWE Web Site](#)

View CVE :

(e.g.: CVE-2009-1234 or

2010-1234 or 20101234)

View BID :

(e.g.: 12345)

Search By Microsoft

Reference ID:

(e.g.: ms10-001 or

979352)

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vulnerability Feeds & Widgets

New

[www.itsecdb.com](#)

Security Vulnerabilities Published In February 2023

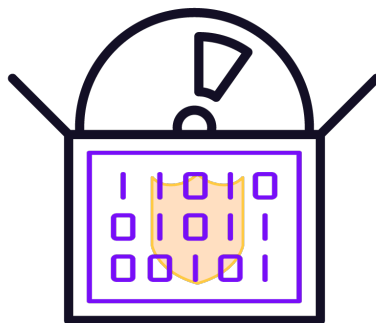
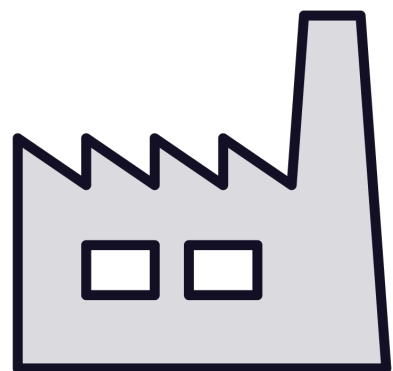
2023 : [January](#) [February](#) [CVSS Scores Greater Than: 0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

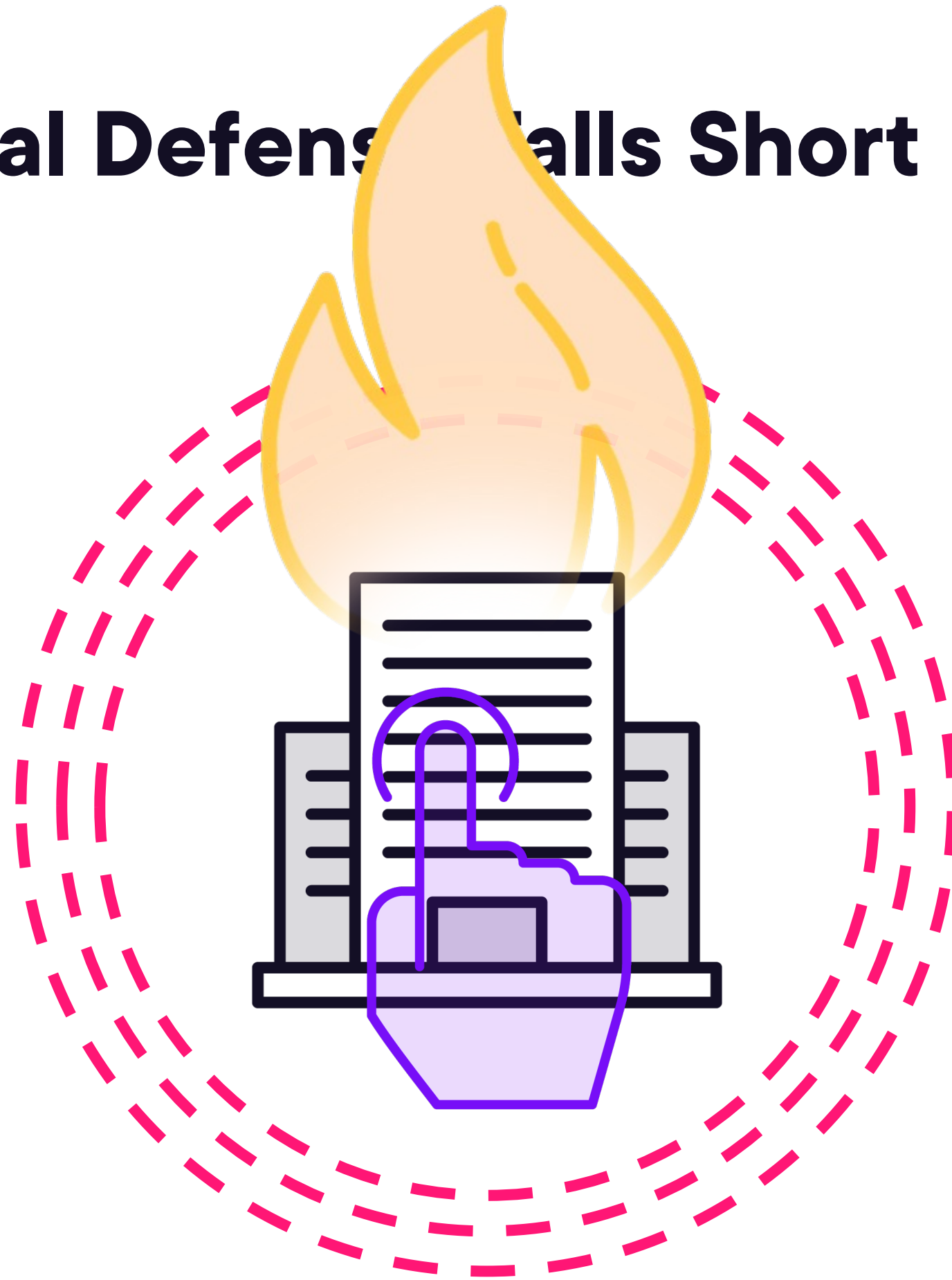
Total number of vulnerabilities : **317** Page : [1](#) (This Page) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2023-25193				2023-02-04	2023-02-04	0.0	None	???	???	???	???	???	???
hb-ot-layout-gsubpos.hh in HarfBuzz through 6.0.0 allows attackers to trigger O(n^2) growth via consecutive marks during the process of looking back for base glyphs when attaching marks.														
2	CVE-2023-25139			Overflow	2023-02-03	2023-02-03	0.0	None	???	???	???	???	???	???
sprintf in the GNU C Library (glibc) 2.37 has a buffer overflow (out-of-bounds write) in some situations with a correct buffer size. This is unrelated to CWE-676. It may write beyond the bounds of the destination buffer when attempting to write a padded, thousands-separated string representation of a number, if the buffer is allocated the exact size required to represent that number as a string. For example, 1,234,567 (with padding to 13) overflows by two bytes.														
3	CVE-2023-25136				2023-02-03	2023-02-03	0.0	None	???	???	???	???	???	???
OpenSSH server (sshd) 9.1 introduced a double-free vulnerability during options.kex_algorithms handling. This is fixed in OpenSSH 9.2. The double free can be triggered by an unauthenticated attacker in the default configuration; however, the vulnerability discoverer reports that "exploiting this vulnerability will not be easy."														
4	CVE-2023-25135			Exec Code	2023-02-03	2023-02-03	0.0	None	???	???	???	???	???	???
vBulletin before 5.6.9 PL1 allows an unauthenticated remote attacker to execute arbitrary code via a crafted HTTP request that triggers deserialization. This occurs because verify_serialized checks that a value is serialized by calling unserialize and then checking for errors. The fixed versions are 5.6.7 PL1, 5.6.8 PL1, and 5.6.9 PL1.														
5	CVE-2023-25015			CSRF	2023-02-02	2023-02-02	0.0	None	???	???	???	???	???	???
Clockwork Web before 0.1.2, when Rails before 5.2 is used, allows CSRF.														
6	CVE-2023-25014				2023-02-02	2023-02-02	0.0	None	???	???	???	???	???	???
An issue was discovered in the femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the InvitationController allow an unauthenticated user to delete all frontend users.														
7	CVE-2023-25013				2023-02-02	2023-02-02	0.0	None	???	???	???	???	???	???
An issue was discovered in the femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the InvitationController allow an unauthenticated user to set the password of all frontend users.														
8	CVE-2023-25012				2023-02-02	2023-02-02	0.0	None	???	???	???	???	???	???
The Linux kernel through 6.1.9 has a Use-After-Free in bigben_remove in drivers/hid/hid-bigbenff.c via a crafted USB device because the LED controllers remain registered for too long.														
9	CVE-2023-24997	502			2023-02-01	2023-02-01	0.0	None	???	???	???	???	???	???
Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick https://github.com/apache/inlong/pull/7223 https://github.com/apache/inlong/pull/7223 to solve it.														
10	CVE-2023-24977	125			2023-02-01	2023-02-01	0.0	None	???	???	???	???	???	???
Out-of-bounds Read vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick https://github.com/apache/inlong/pull/7214 https://github.com/apache/inlong/pull/7214 to solve it.														
11	CVE-2023-24956			Sql	2023-02-01	2023-02-01	0.0	None	???	???	???	???	???	???
Forget Heart Message Box v1.1 was discovered to contain a SQL injection vulnerability via the name parameter at /cha.php.														
12	CVE-2023-24613			DoS	2023-02-03	2023-02-03	0.0	None	???	???	???	???	???	???
The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481.														



Where Traditional Defense Falls Short

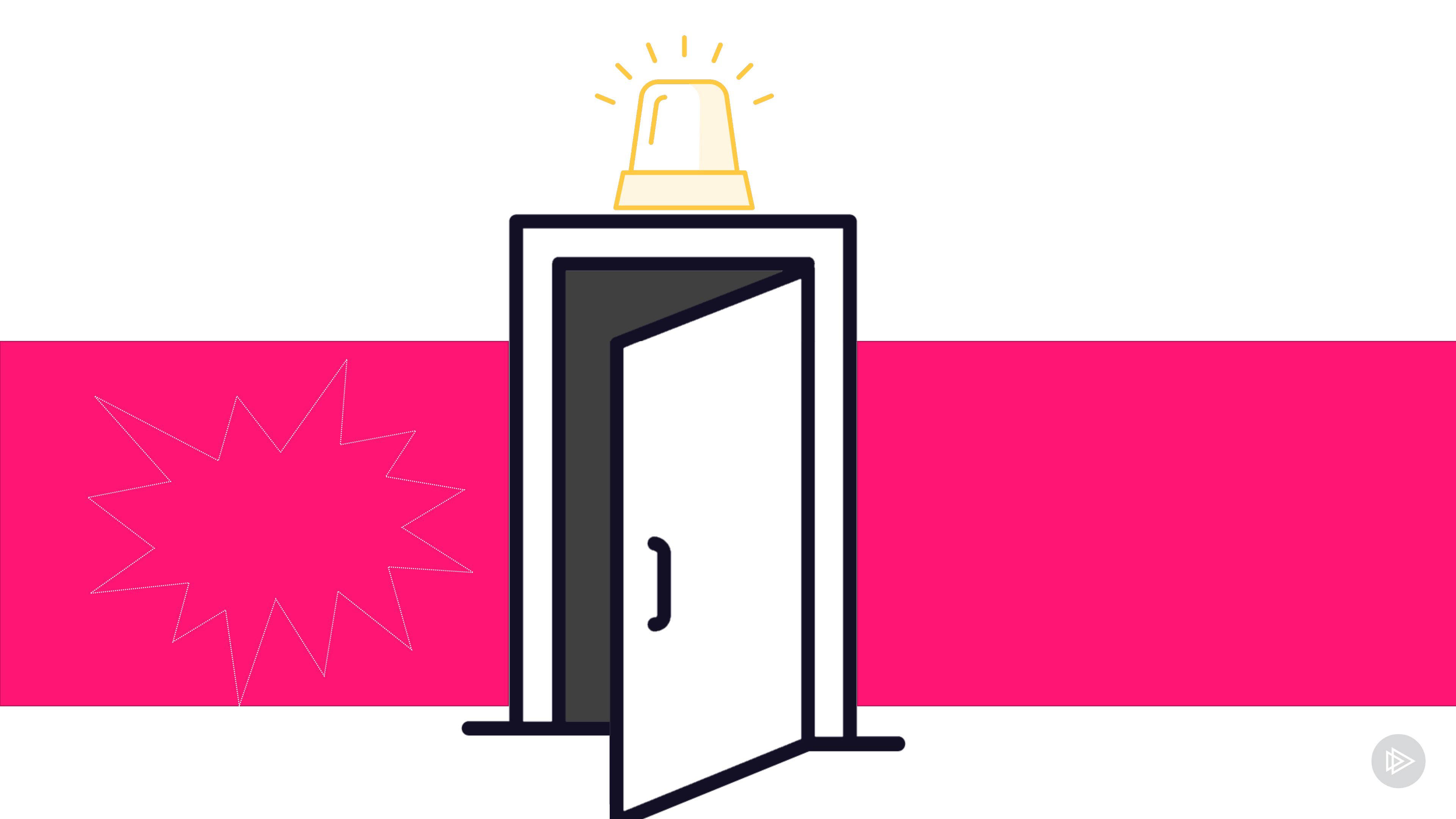


Active Defense

Proactive measures taken by an organization to detect, prevent, and respond to cyber threats.

Traditional Defense = Passive





Active Defense Techniques

Continuous monitoring and analysis of network

Deception technology

Honeypots and decoys

Honey tokens

Red teaming and penetration testing

Proactively patching systems





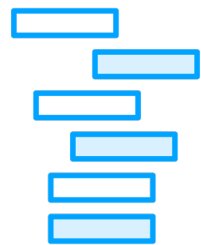
Why the Use of PowerShell for Active Defense



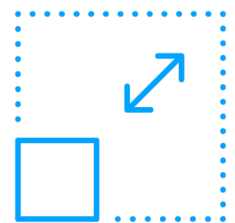
Why the Use of PowerShell for Active Defense



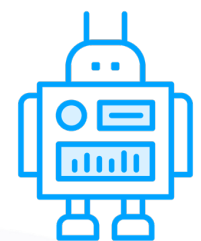
Cross Platform



Integration into the Operating System

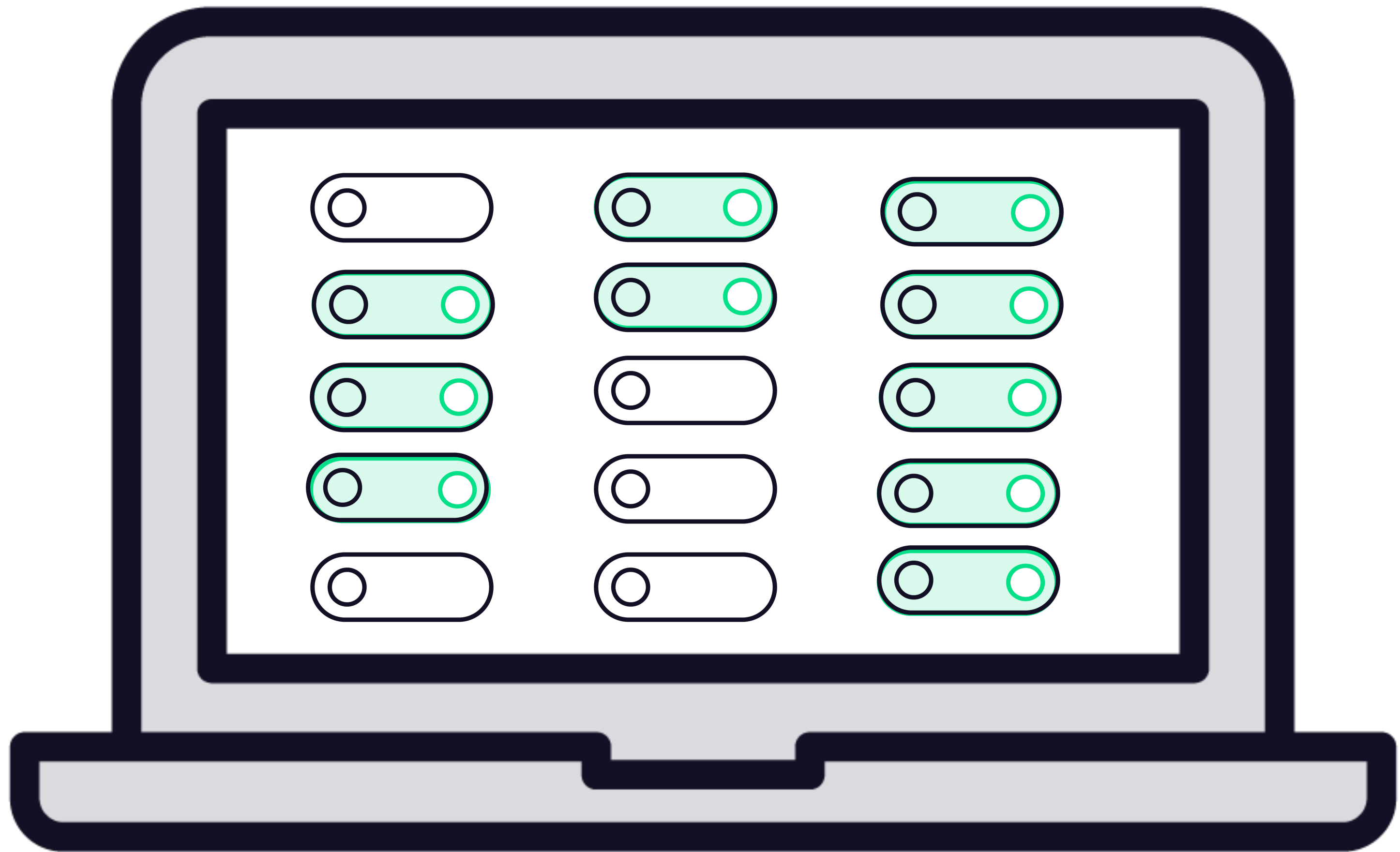


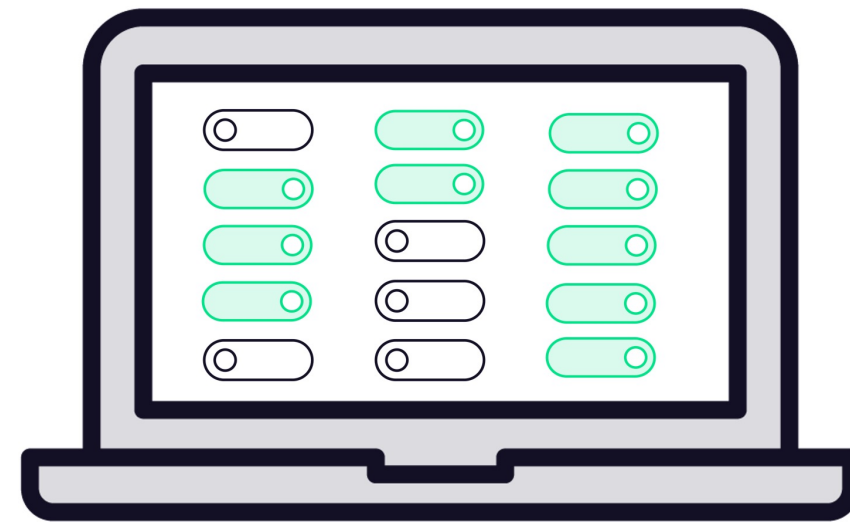
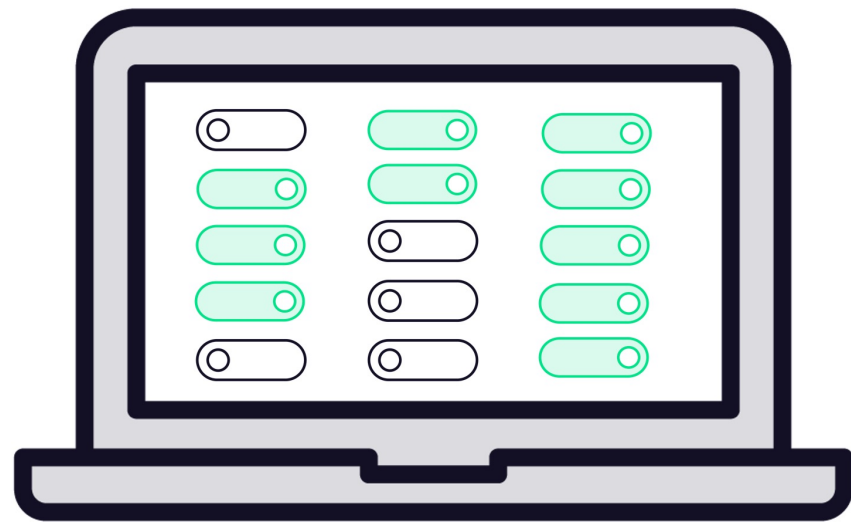
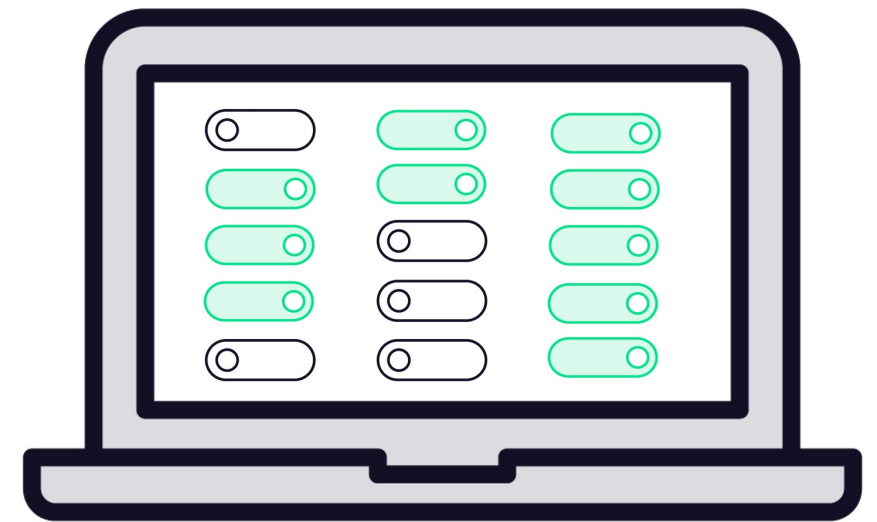
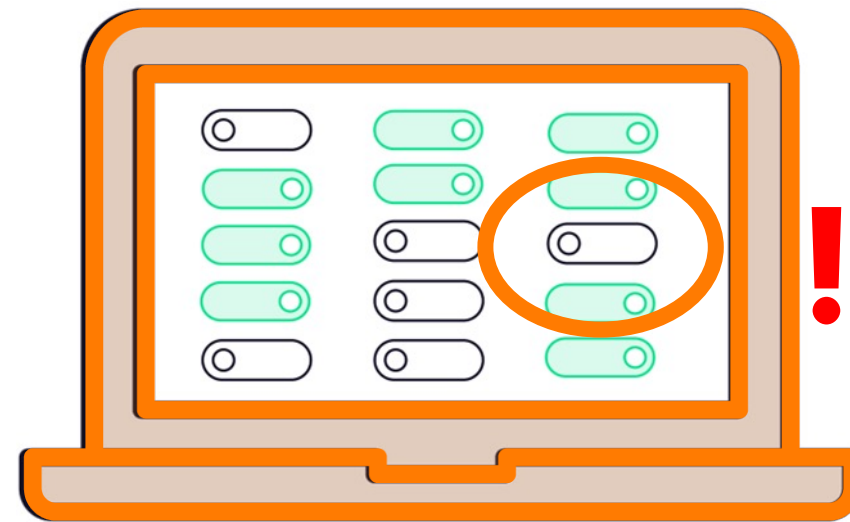
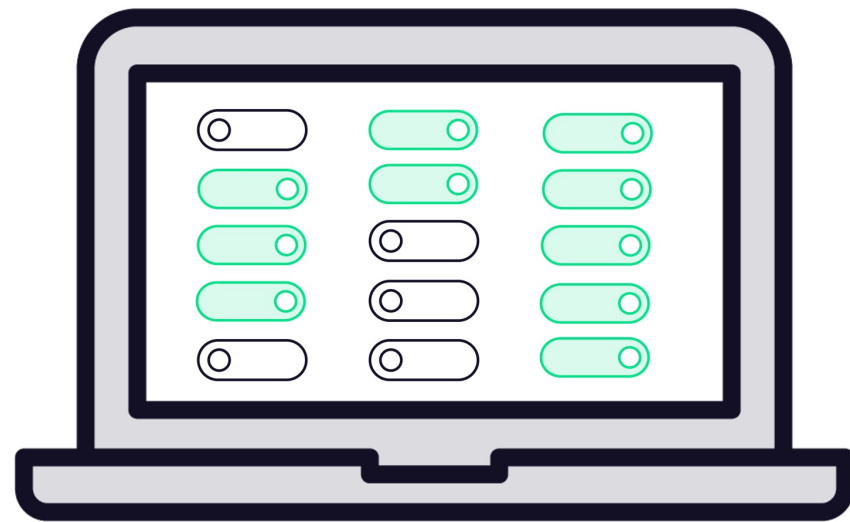
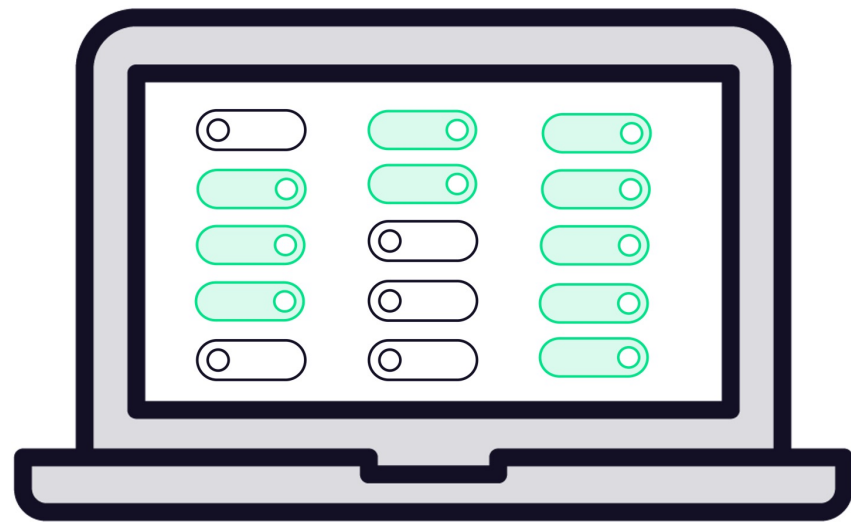
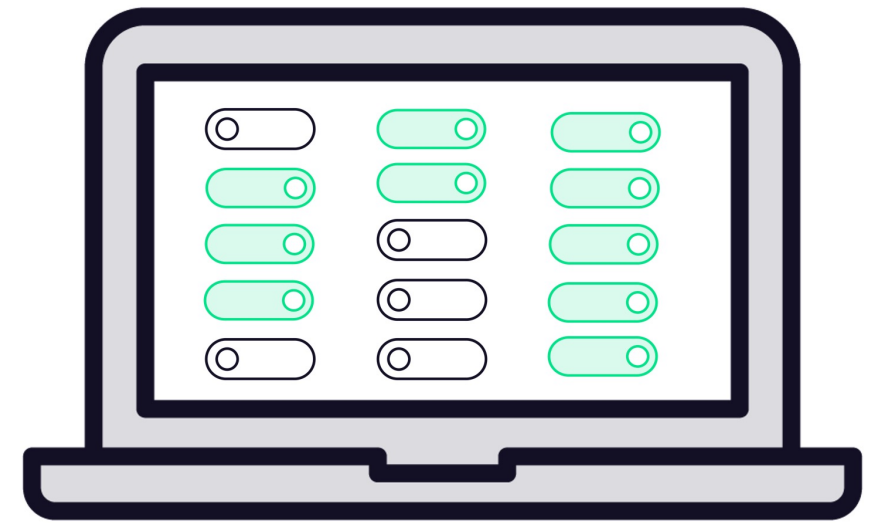
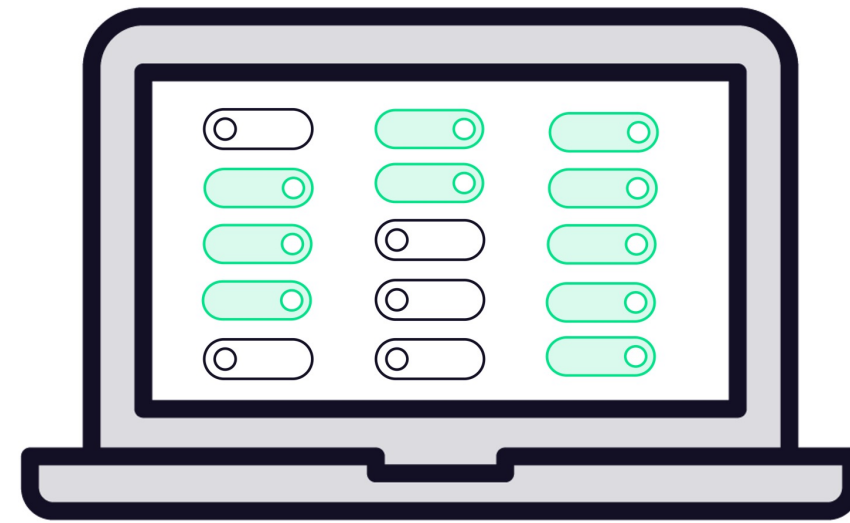
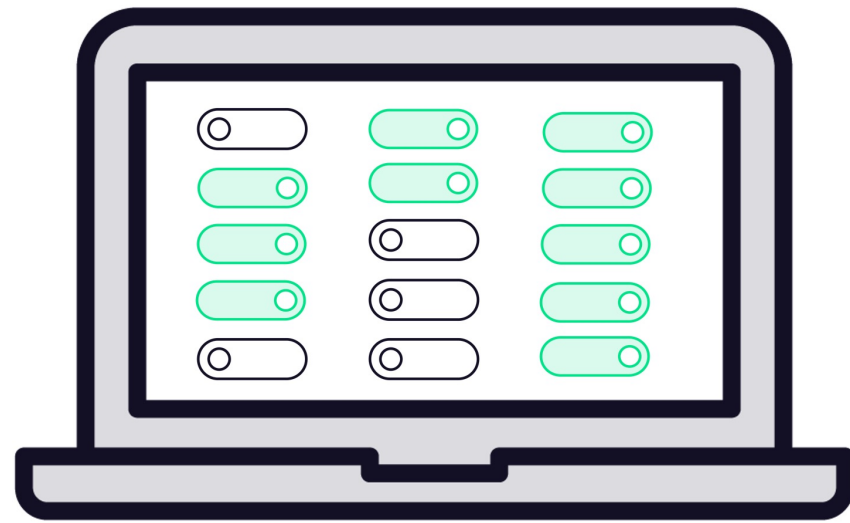
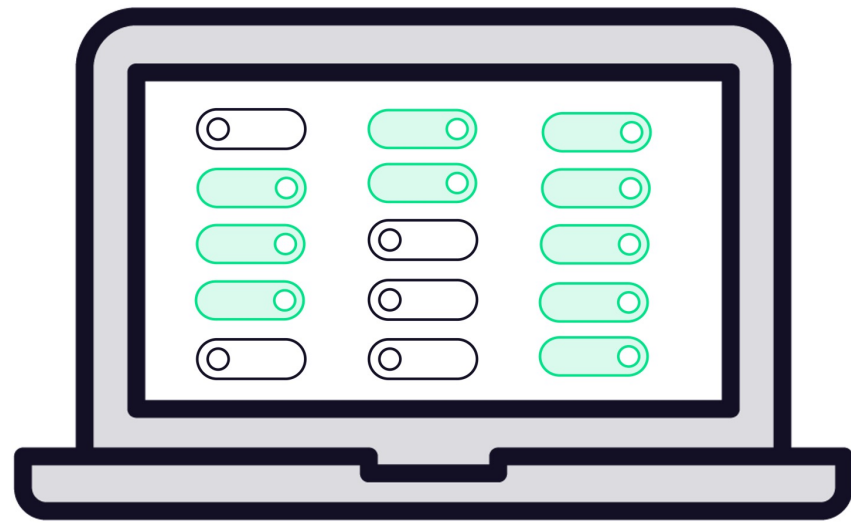
Scalable Functionality



Deep Automation Capabilities



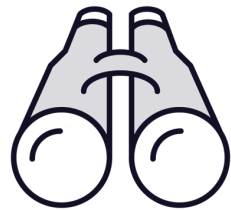




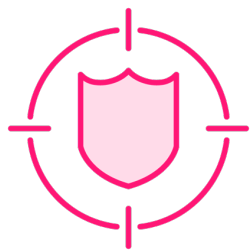
PowerShell for Active Defense



Scripting



Network Reconnaissance



Simulating Attacks



Remediation

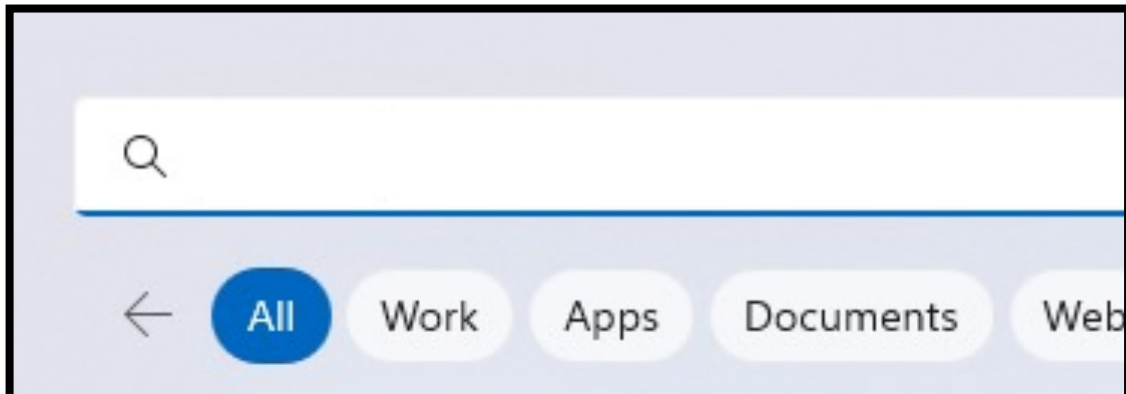




Tools for the Course



Windows PowerShell



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

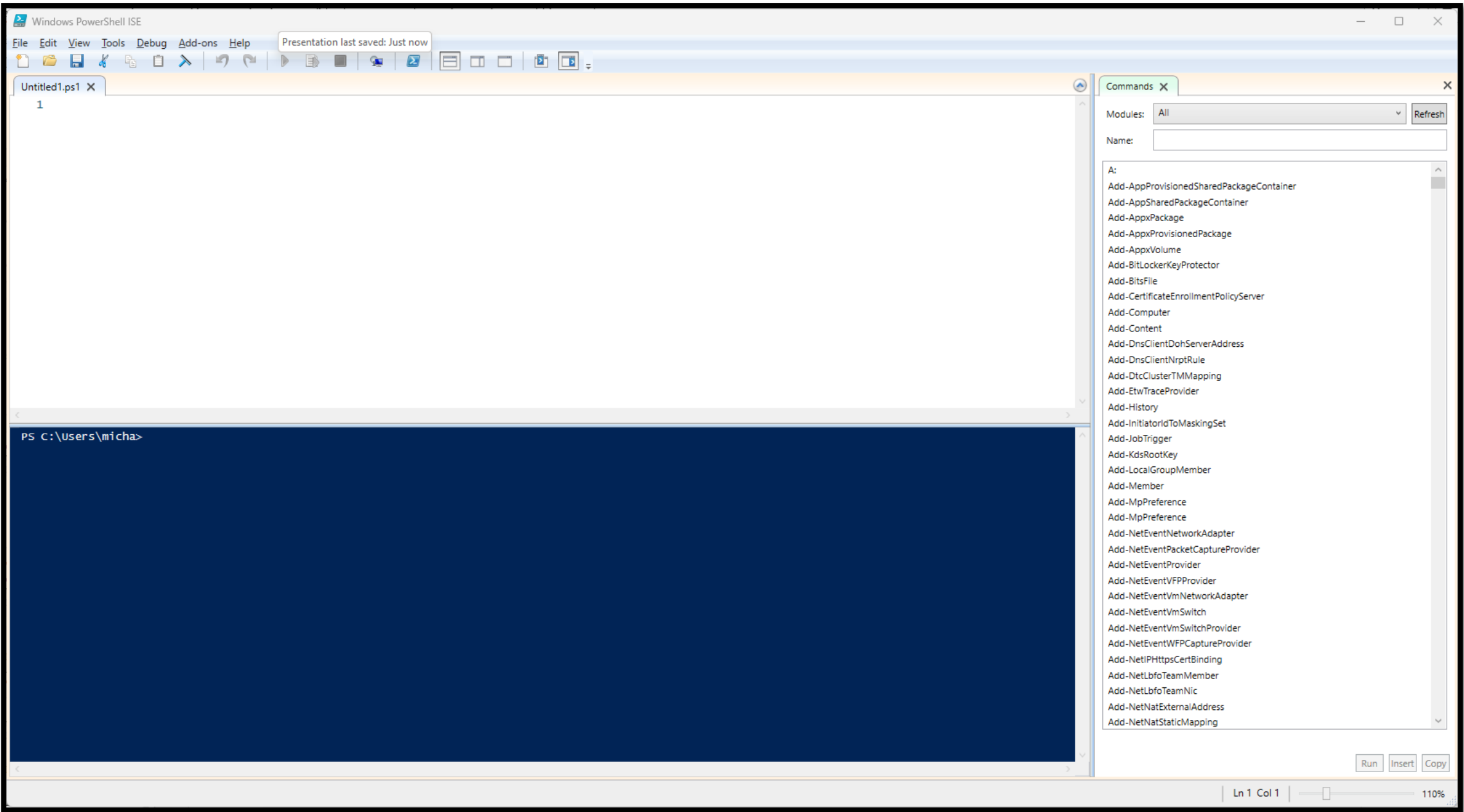
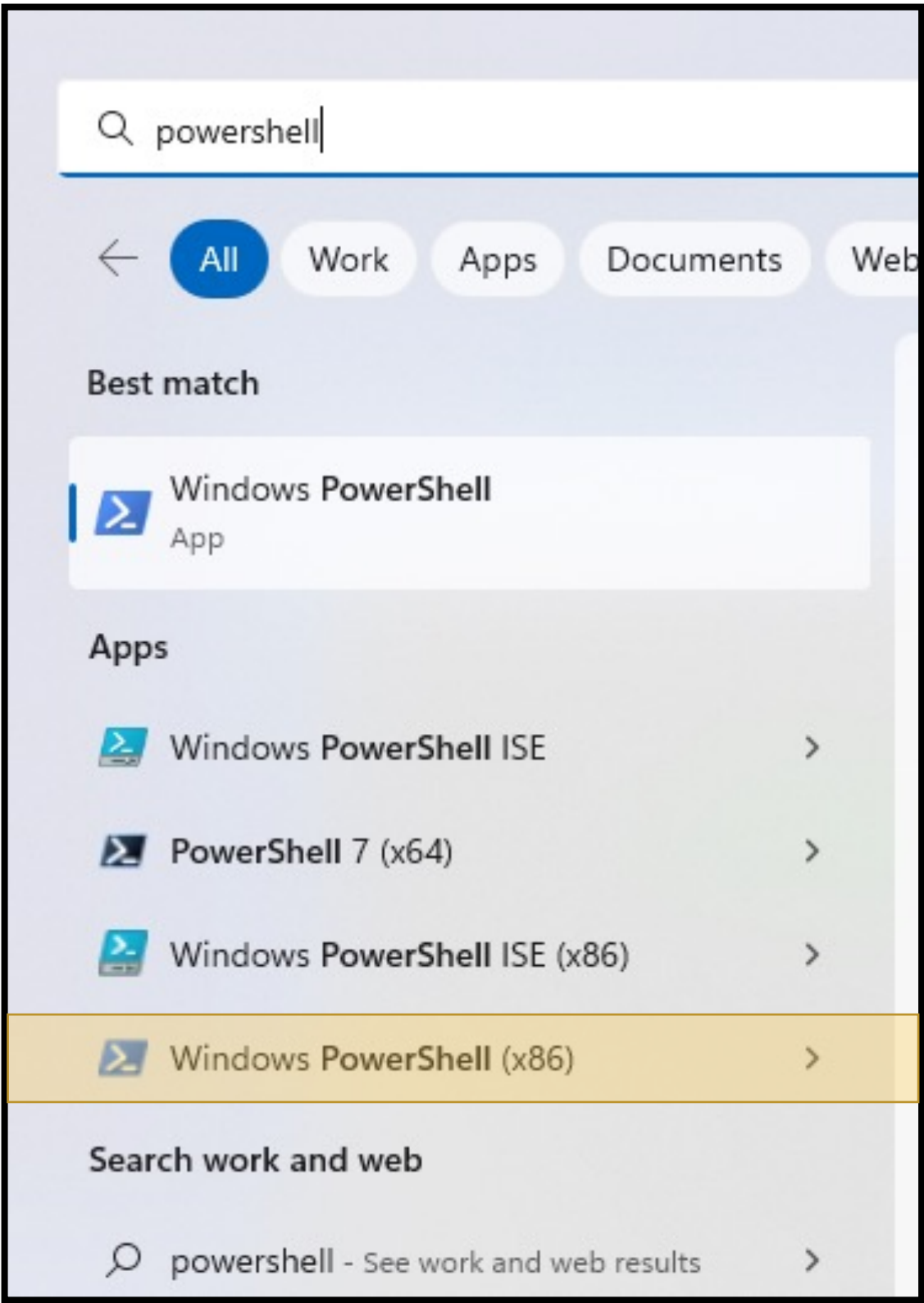
PS C:\Users\micha> $PSVersionTable

Name                           Value
----                           -
PSVersion                      5.1.22621.963
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.22621.963
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1

PS C:\Users\micha>
```

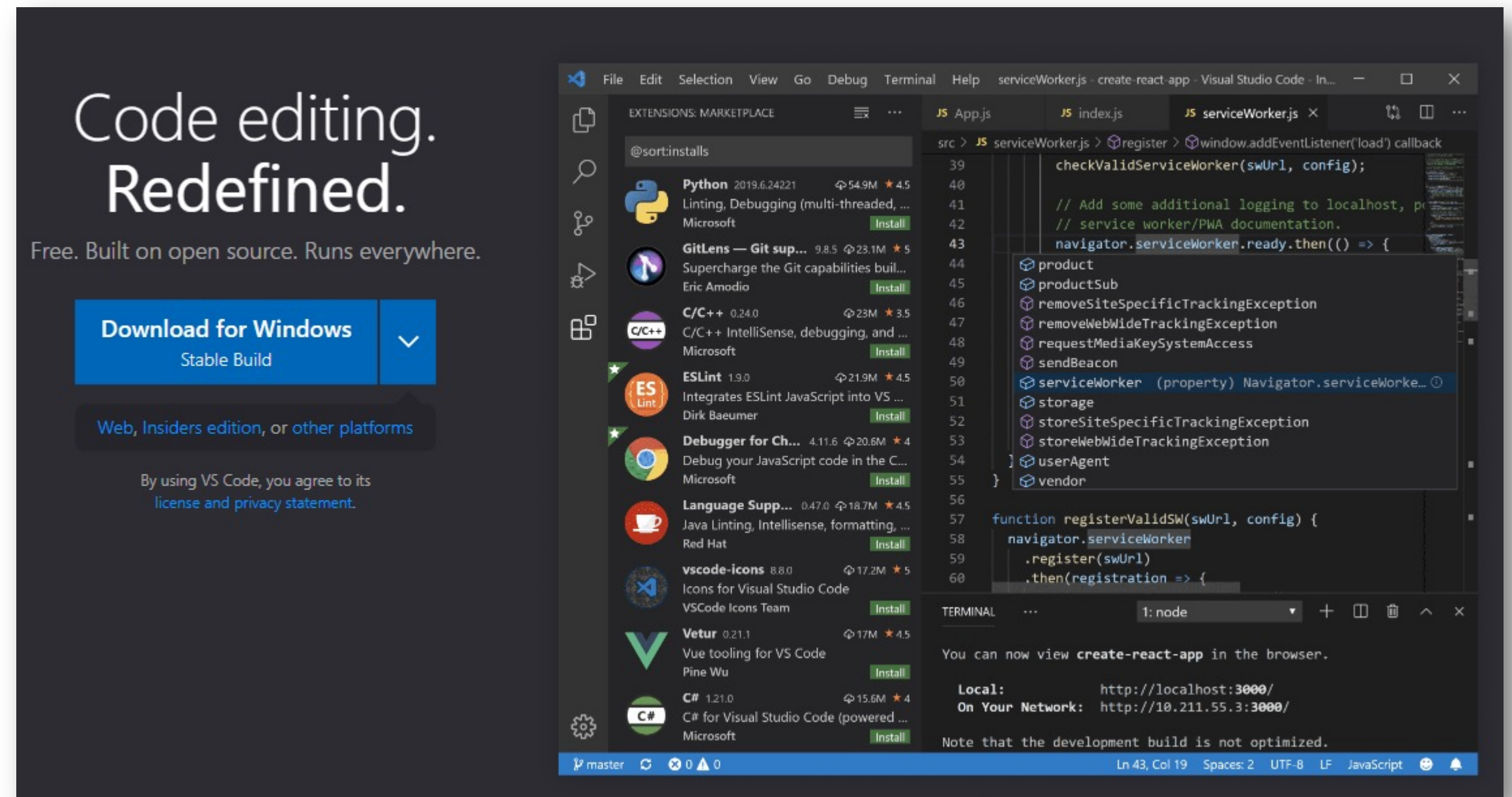
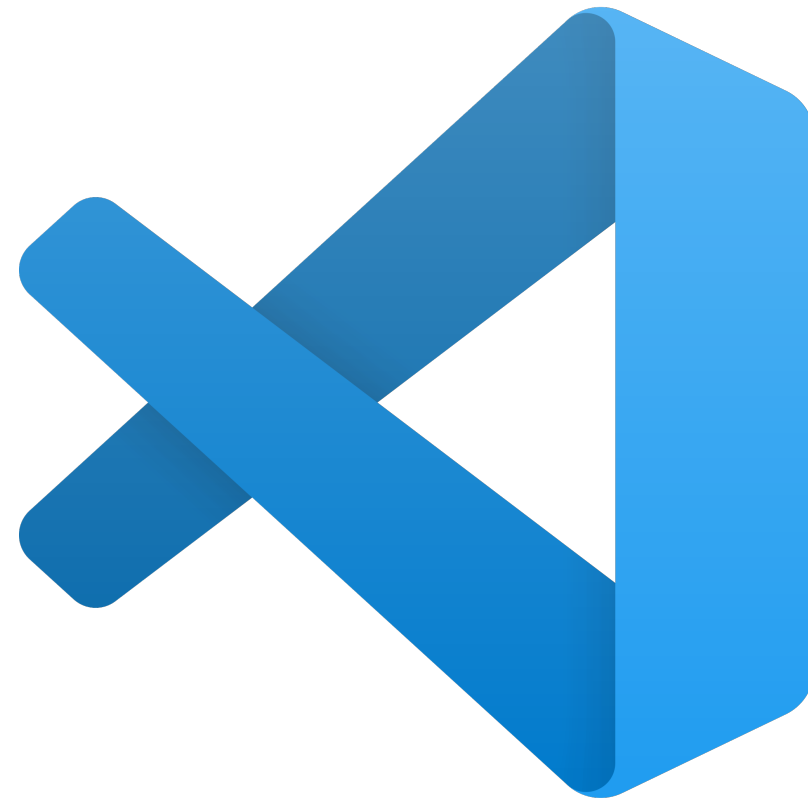


Windows PowerShell ISE



Visual Studio Code

<https://code.visualstudio.com/>



PowerShell 7 (Core)

<https://github.com/PowerShell/PowerShell/releases>

The image is a composite of three screenshots illustrating the installation and verification of PowerShell 7.3.2 Core.

Top Left: A placeholder image showing a blue square with a white right-pointing chevron.

Top Right: A browser window titled "PowerShell 7 (x64)" displaying the GitHub releases page for PowerShell. The URL <https://github.com/PowerShell/PowerShell/releases> is visible in the address bar.

Bottom Left: A Windows Start menu search results window. The search bar contains "PowerShell 7 (x64)". The results are categorized into "All", "Apps", "Documents", "Web", and "More". Under the "Apps" section, "PowerShell 7 (x64)" is listed as the "Best match". Other results include "Windows PowerShell", "Windows PowerShell ISE", "PowerShell-7.3.2-win-x64.msi", "Windows PowerShell ISE (x86)", and "Windows PowerShell (x86)".

Bottom Right: A terminal window titled "PowerShell 7 (x64)" showing the output of the command `$PSVersionTable`. The output is a table with two columns: "Name" and "Value". The "Name" column lists various system components, and the "Value" column shows their respective versions. The version of PowerShell is highlighted with a yellow box.

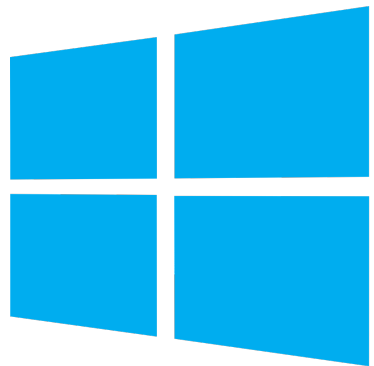
Name	Value
BuildVersion	7.3.2
CLRVersion	4.0.30319.42
OSVersion	Microsoft Windows 10.0.22621
Win32NT	6.0.2600.5512
IsOS	{1.0, 2.0, 3.0, 4.0...}
Version	2.3
BuildNumber	1.1.0.1
Build	3.0

Other Tools Used



VirtualBox

<https://www.virtualbox.org/>



Windows 10

<https://www.microsoft.com/en-us/evalcenter/download-windows-10-enterprise>



Windows Server 2019

<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019>



Up Next:

Setting the Trap



Setting the Trap



Michael Woolard

Risk and Compliance Manager

@wooly6bear | <https://wooly6bear.wordpress.com>

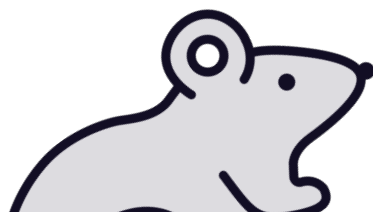
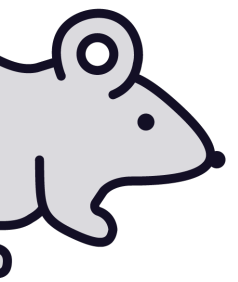
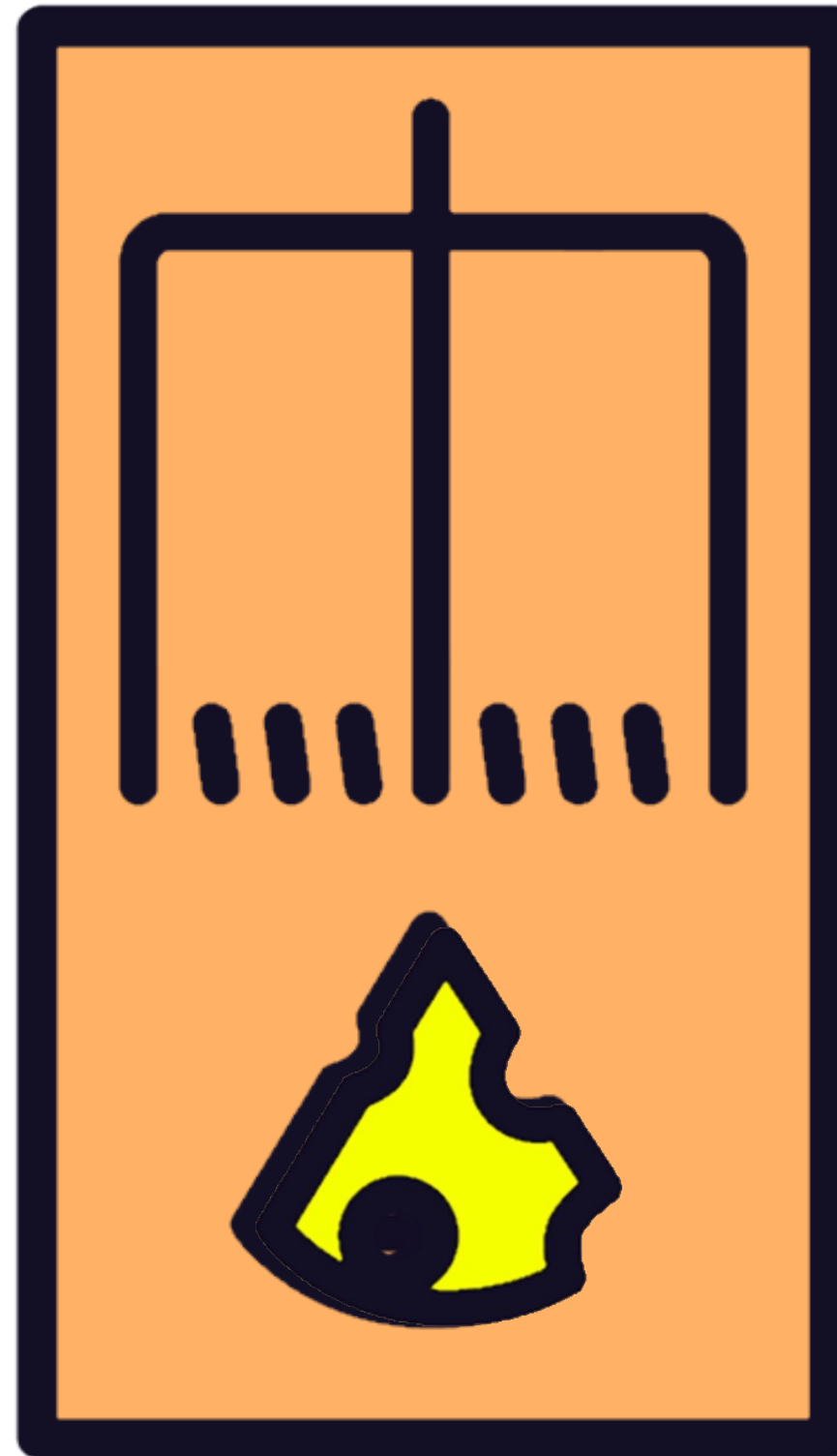




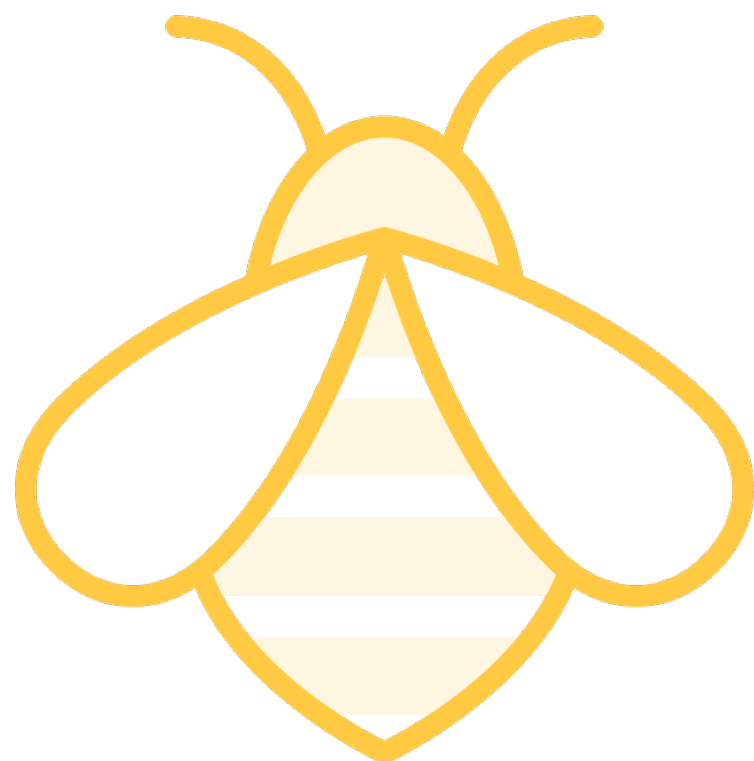
What Kind of Traps Can Be Set



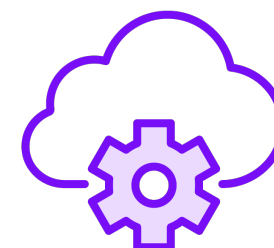
Honeypot



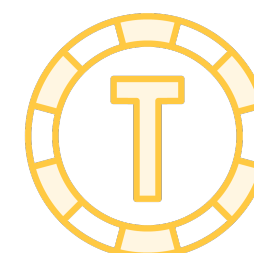
Create a Honeypot



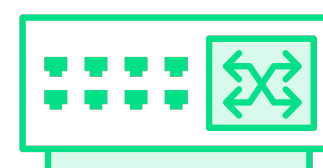
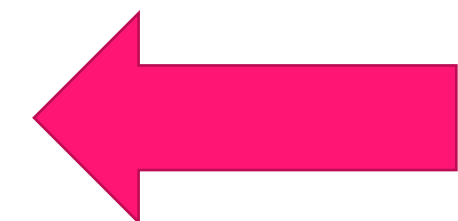
Files



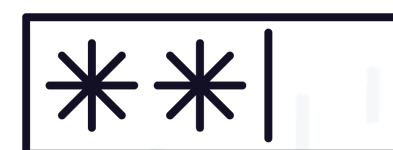
Services



Tokens



Ports



Credentials





Create a Honeypot



Honeyport



<https://github.com/gfoss/PowerShell-Honeyport/blob/master/honeyport.ps1>



honeyportCIM.ps1 in course exercise files



PowerShell 7



HoneyPortCIM.ps1



HoneyPortCIM. ps1

Notes

Log Aggregator / SIEM / EDR

- 1003
- 1002

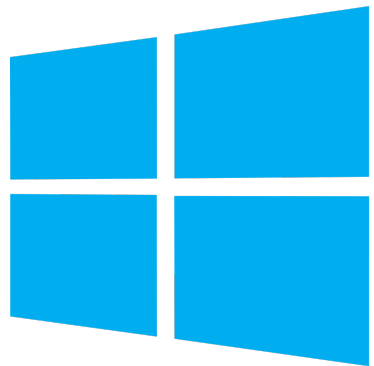
Nosy



Honeytoken



<https://github.com/Blumira/Kerberoast-Detection>



Domain Controller



Powershell 7



Local Group Policy Editor

File Action View Help



Local Computer Policy

Computer Configuration

Software Settings

Windows Settings

Name Resolution Policy

Scripts (Startup/Shutdown)

Deployed Printers

Security Settings

Account Policies

Local Policies

Windows Defender Firewall

Network List Manager Policies

Public Key Policies

Software Restriction Policies

Application Control Policies

IP Security Policies on Local Computer

Advanced Audit Policy Configuration

System Audit Policies

Account Logon

Account Management

Detailed Tracking

DS Access

Logon/Logoff

Object Access

Policy Change

Privilege Use

System

Subcategory

Audit Credential Validation

Audit Kerberos Authentication Service

Audit Kerberos Service Ticket Operations

Audit Other Account Logon Events

Audit Events

Not Configured

Not Configured

Not Configured

Not Configured

Create Service Account Honeyypot

Step 1 – Create a non-admin user account (example: backupexec)

Step 2 – Add a SPN to the account (see below)

Step 3 – Confirm the SPN was created > **setspn -Q */* | findstr backupsvc**

```
C:\Users\Administrator>setspn -a backupsvc/Win2019Server backupexec
Checking domain DC=PLURALSIGHT,DC=local

Registering ServicePrincipalNames for CN=backup svc,CN=Users,DC=PLURALSIGHT,DC=local
        backupsvc/Win2019Server
Updated object
```



Dogemira.ps1

- *Event ID: 4769*
- *Encryption type: 0x17*
- *Ticket options: 0x40810000*
- *SPN Name: <Name of your honeycred / SPN name>*





Monitor for Bad Credentials



Invoke-Fail2Ban



<https://github.com/wiredpulse/Invoke-Fail2Ban>



Invoke-Fail2Ban.ps1 in course exercise files



<https://cyberfibers.com/2019/08/invoke-fail2ban/>



Invoke-Fail2Ban

Honey Cred Admin Properties

Member Of Dial-in Environment Sessions
Remote control Remote Desktop Services Profile COM+
General Address Account Profile Telephones Organization

User logon name:
 @PLURALSIGHT.local

User logon name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never
☐ End of:



Invoke-Fail2Ban.ps1





Maintain the Look of an Active User



Hack the Hacker



When Was the Account Created?

When Did the Account Last Logon?

When Was the Password Last Changed?

Correlation to Another Non-Admin Account?



Hack the Hacker

```
$RegPath = "HKLM:\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon"
```

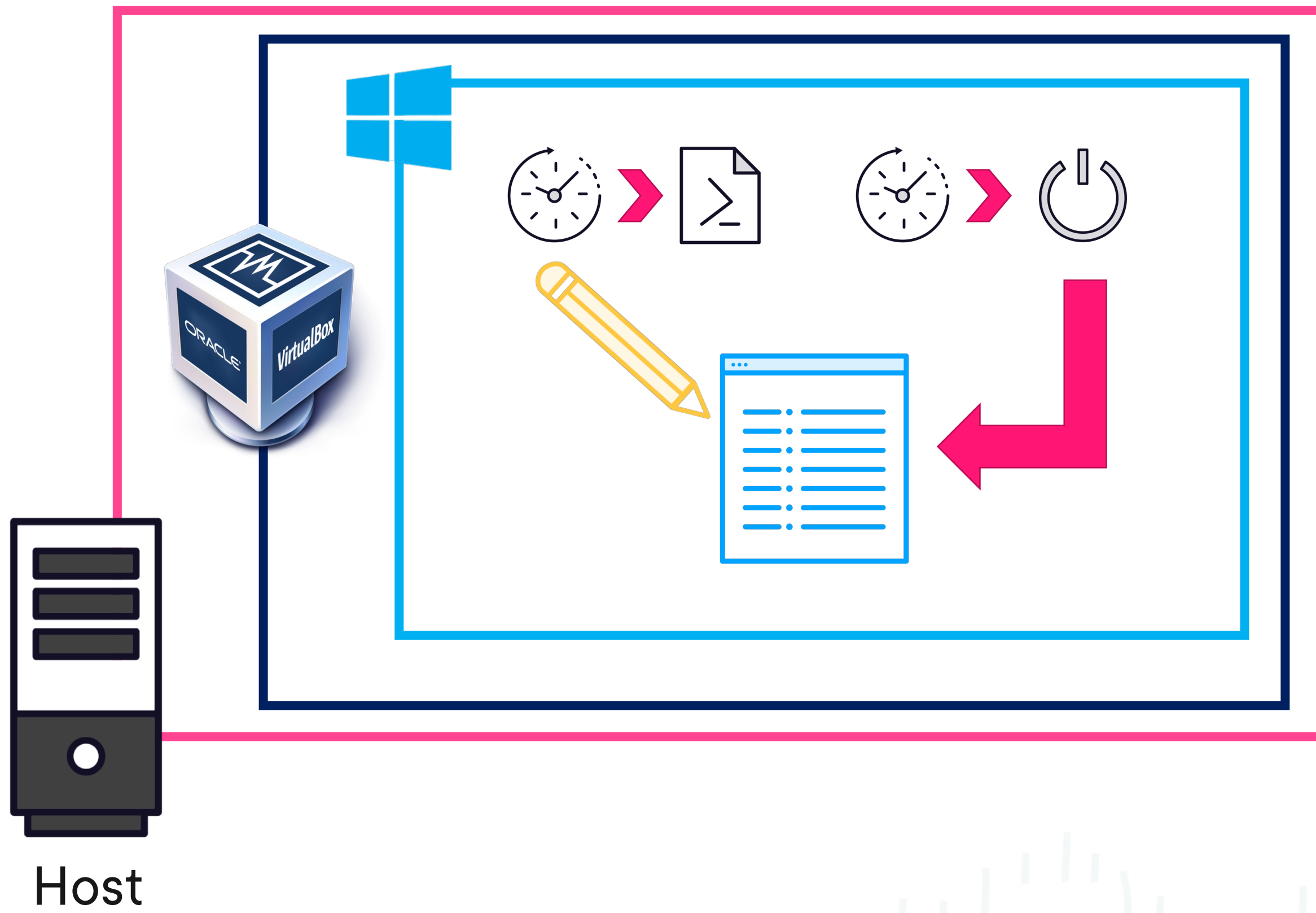
```
$DefaultUsername = "honeycredusername"
```

```
$DefaultPassword = "honeycredpassword"
```

```
Set-ItemProperty $RegPath "AutoAdminLogon" -value "1" -type String
```

```
Set-ItemProperty $RegPath "DefaultUsername" -value  
"$DefaultUsername" -type String
```





Start up and Shut down Virtualbox VM

C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" list vms

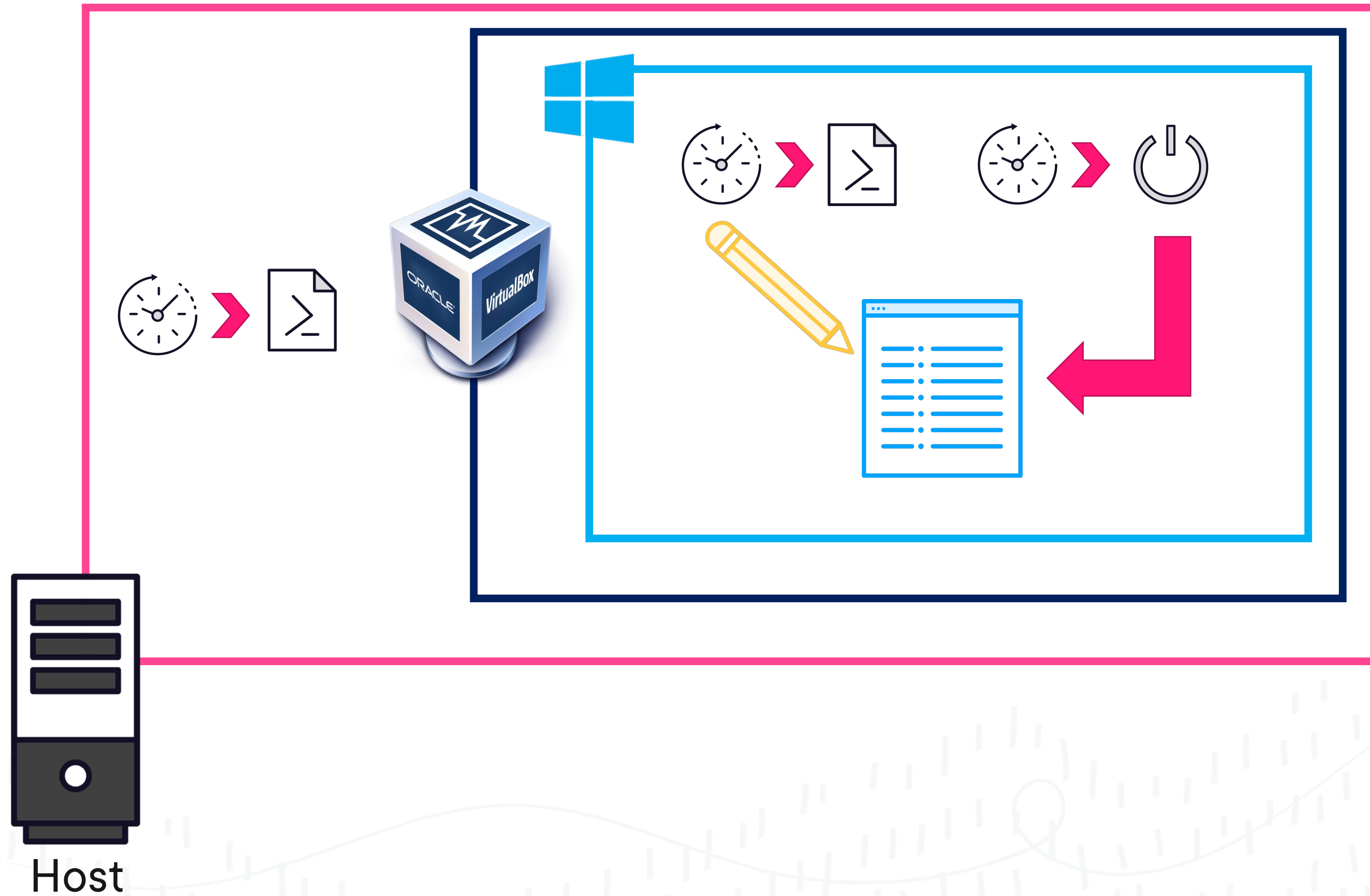
<https://www.virtualbox.org/manual/ch08.html#vboxmanage-startvm>

"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" startvm (name of vm)

<https://www.virtualbox.org/manual/ch08.html#vboxmanage-controlvm>

"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm (name of vm)
shutdown





Hack the Hacker

```
# Specify here the username whose password to reset.
```

```
$username = '(user account)'
```

```
# Import the System.Web .NET assembly
```

```
Add-Type -AssemblyName 'System.Web'
```

```
# Generate a random password that is 12-characters long with five non-AlphaNumeric characters.
```

```
$randomPassword = [System.Web.Security.Membership]::GeneratePassword(12, 5)
```

```
# Convert the plain text password to a secure string.
```

```
$newPassword = $randomPassword | ConvertTo-SecureString -AsPlainText -Force
```

```
# Reset the user password
```

```
Set-ADAccountPassword -Identity $username -NewPassword $newPassword -Reset
```

```
# Display the new password
```

```
$randomPassword
```





Review Attack Patterns



TT&CK Matrix for Enterprise

show sub-techniques

show sub-techniques

show sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limit
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture		Exfiltration Over Alternate Protocol
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C Channel
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Network Medium
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Plaintext Medium
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Domain Policy Modification (2)	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Scheduled Transfer
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Multi-Stage Channels	Transfer to Cloud Account
			System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Hide Artifacts (10)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	
			User Execution (3)	Implant Internal Image	Scheduled Task/Job (5)	Hijack Execution Flow (12)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Non-Standard Port	
			Windows Management Instrumentation	Modify Authentication Process (7)	Valid Accounts (4)	Impair Defenses (9)	Steal Application Access Token	Network Service Discovery		Data from Removable Media	Protocol Tunneling	
				Office Application Startup (6)		Indicator Removal (9)	Steal or Forge Authentication Certificates	Network Share Discovery		Data Staged (2)	Proxy (4)	
				Pre-OS Boot (5)		Indirect Command Execution	Steal or Forge Kerberos	Password Policy Discovery		Email Collection (3)	Remote Access Software	
				Scheduled		Masquerading (7)		Peripheral Device Discovery		Input Capture (4)	Traffic Signaling (2)	
						Modify Authentication Process (7)		Permission Groups Discovery (3)		Screen Capture	Web Service (3)	
						Modify Cloud Compute Infrastructure (4)		Process Discovery		Video Capture		

- Phishing reports
- AV alerts
- EDR alerts
- WAF logs
- IAM & MFA
- Server resources
- Production Incidents
- Security Incidents

Port Scanning



Brute Force



Kerberoasting



Auditing



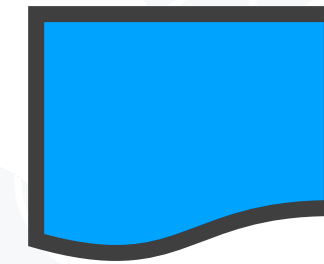
Auditing

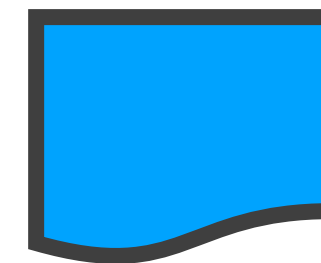


Michael Woolard

Risk and Compliance Manager

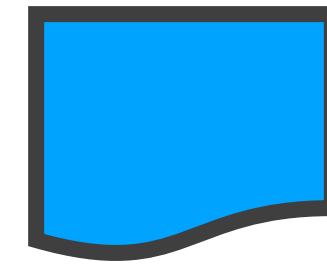
@wooly6bear | <https://wooly6bear.wordpress.com>





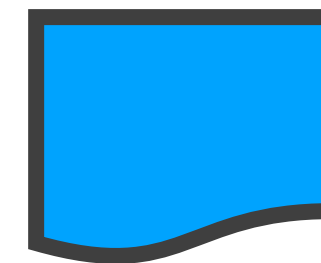
Intrusion Point Discovery





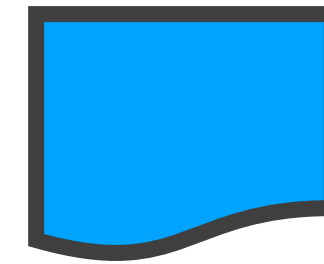
Using PowerShell to Access WMI Objects





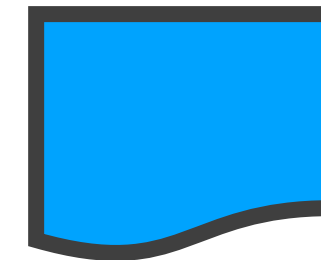
Get-CimInstance





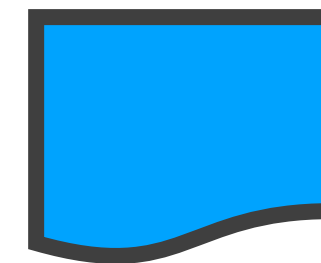
Invoke-CimMethod





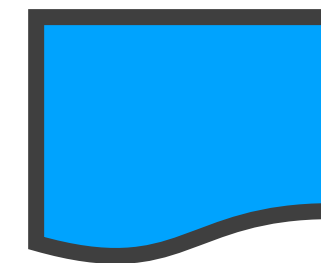
Get-ItemProperty





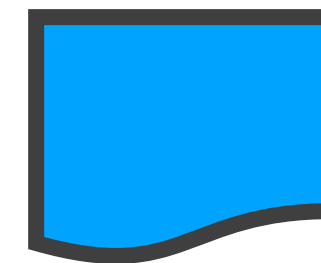
Get-WindowsFeature





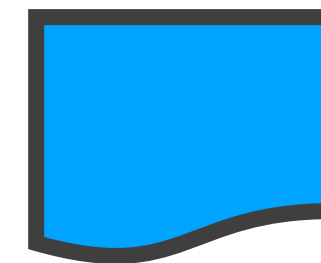
Get-ExecutionPolicy





Set-ExecutionPolicy

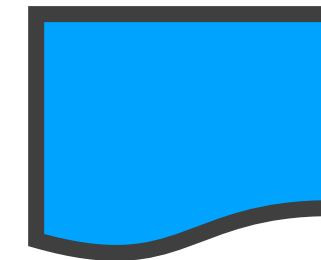


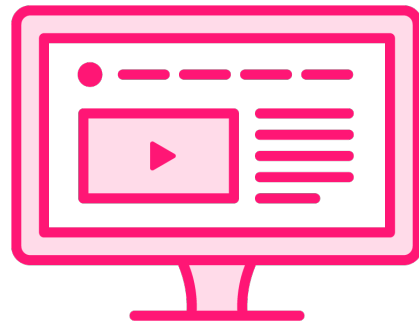


Summary



Summary





Web Application Penetration Testing Fundamentals

Getting Started with OWASP Zed Attack Proxy (ZAP)

Automate Web Application Scans with OWASP ZAP and Python

