



Desjardins

Purple Team: From Silos to Heroes

Hackfest 14 - Resurrection Edition

2022-10-29



VIEW THE AGENDA

Agenda

- Who we are
- Defining Purple Teaming
- Challenges with the current landscape
- Continuous Purple Teaming
 - Process
 - People
 - Techno
- Building a security posture
- The ultimate goal

TL;DR ❤️ + ❤️ = 💥 🚀





Bio: Martin Dubé

- Offensive Security Senior Manager 

 - Strive to improve Cyber-Security one meeting at a time 
 - Pentest, ROP, Red, AppSec, Threat Modeling

- Former HF board member and CTF Team Leader (2010-2015 + 2017)
- Former CTF Designer at NSEC (2018)
- Father of 2 , Woodworker , Runner 
- May be found where there is:
 - Espresso 
 - Whiskys 
 - BBQ 

Bio: Dany Lafrenière

- SOC Senior Manager 🚨
- Master at agenda Tetris 🧩📅🧩
- Tierless SOC strong believer ∞
- In love with a cat lover 😺😺😺
- I eat chicken wings with a fork 🍗
- My favourite superhero is ... Forrest Gump!



Inspiration for this talk

The screenshot shows a video player interface. At the top, the title 'Offense Defense Touchpoints' is displayed. Below it is a diagram illustrating various touchpoints between offense and defense. The diagram consists of several colored boxes connected by arrows:

- Vuln scan (red)
- Patch Management (blue)
- External pentest (red)
- Network controls / Admin rights (blue)
- Internal pentest (red)
- Configured Endpoints / EDRs (blue)
- Purple Team(s) (red)
- Centralized Logging (blue)
- Red team / ATT&CK (red)
- Finely tuned Alerting and Response (blue)
- Non-scoped long term / AdSims (red)
- Threat Hunting (blue)

At the bottom of the video player, there are playback controls (rewind, forward, volume), a progress bar (35:34 / 47:12), and a link 'Red Team >'. On the right side of the video player, there is a small video frame showing two men speaking on stage at an event. Below this frame is a slide with the following text:

DerbyConVIII
Victor or Victim? Strategies for Avoiding an InfoSec Cold War
Jason Lang, Stuart McIntosh
EVOLUTiON

At the bottom right of the slide, there are video player controls and a URL: <https://DerbyCon.com>.

Blue vs Purple vs Red (day-to-day)

Purple is a cooperative mindset between attackers and defenders working on the same side. As such, it should be thought of as a function rather than a dedicated team. ^1

Blue Team activities

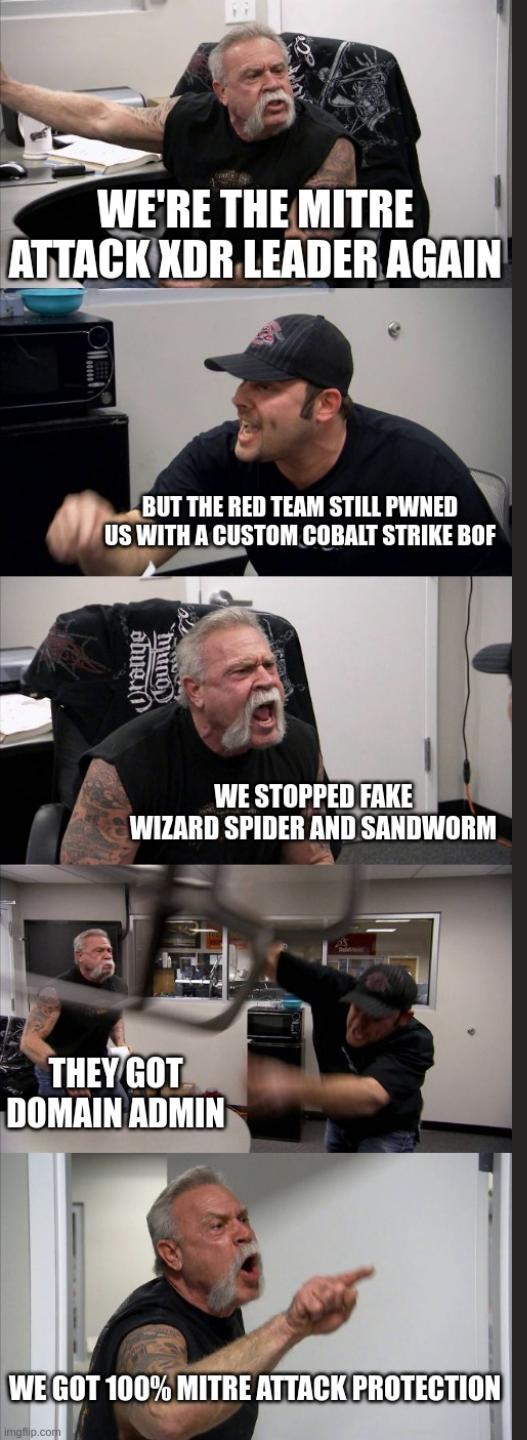
- Goal: Defend
- Require: Autonomy
- Velocity: High
- Analogy: Self-study

Purple Team activities

- Goal: Improve posture
- Require: Collaboration
- Velocity: High
- Analogy: Group study

Red Team activities

- Goal: Test resiliency
- Require: Incident (Surprise)
- Velocity: Low
- Analogy: The exam



Challenges with current landscape

The typical project-based testing workflow is limited.

- Priorization is often only based on public data
- CVSS is so imperfect
- Reports require unnecessary time to write and consume
 - And they "expire" once delivered (snapshots)
- Reports hardly feed a security posture

Some security vendors are very optimistic.

100% Mitre Attack Protection 🤪

Challenges with current landscape

- Results are hard to consume
 - Blue team manager's point of view ... TL;DR
- Recommendations are easy
- Multiples goals and priorities with finite resources
 - ...the never-ending operational backlog and incident response

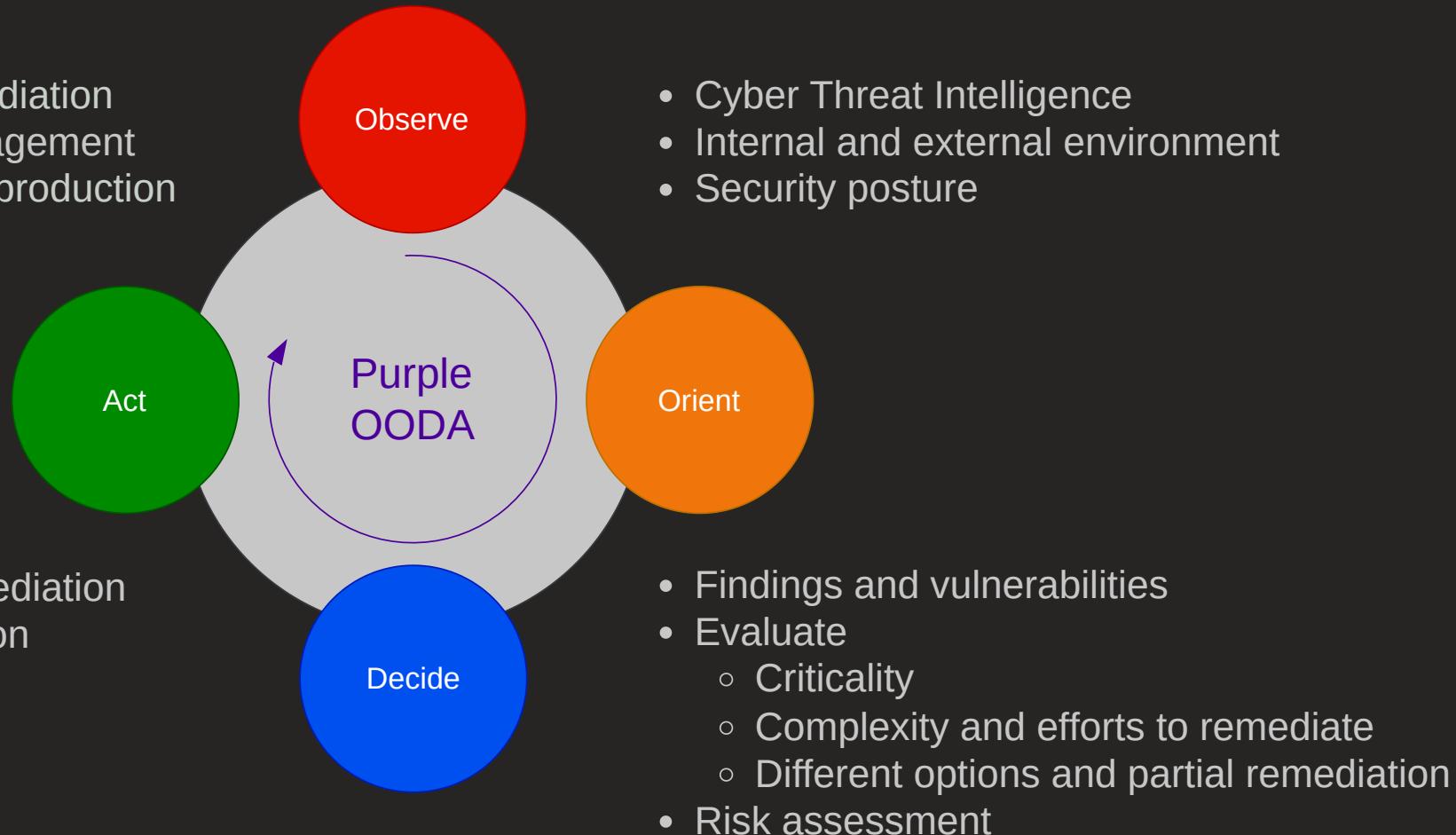


Continuous Purple Teaming

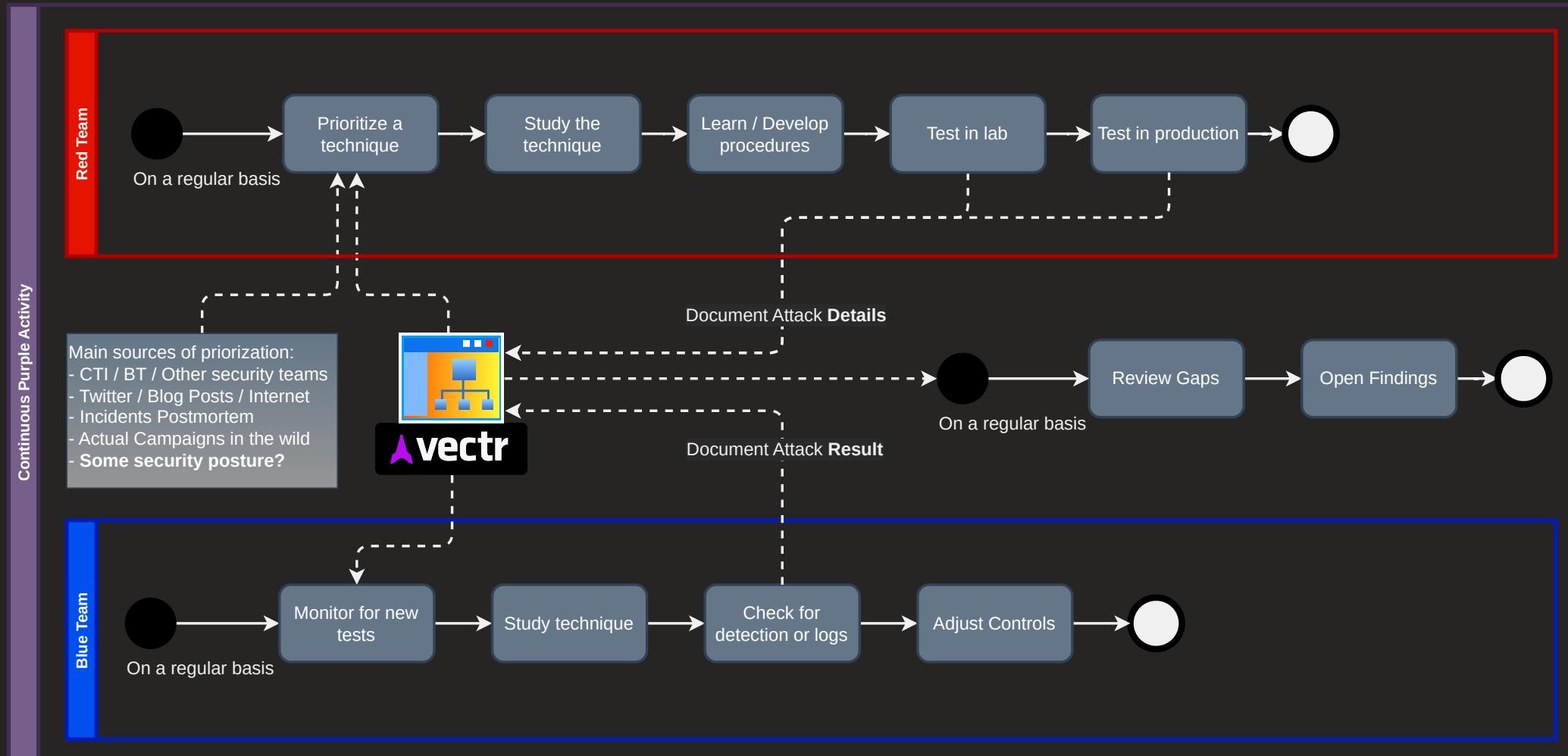
Process, People, Techno

Can Your Purple Team OODA Loop?

- Prepare remediation
- Change management
- Implement in production



How it looks on the field



Continuous Purple Teaming

Process, People, Techno

Manage your ego

- The foundational importance of trust in relationships
 - Consistency
 - Communication
 - Time
- Messages and actions from management is key
- The grass is always greener on the other side



Team or Teams?

What distinguishes a team from a group of people?

- The team has a **common goal**

A purple team is a *virtual* team, even though it is composed of multiple teams.

- One clear goal
- Autonomy
- Mastery

Continuous Purple Teaming

Process, People, **Techno**

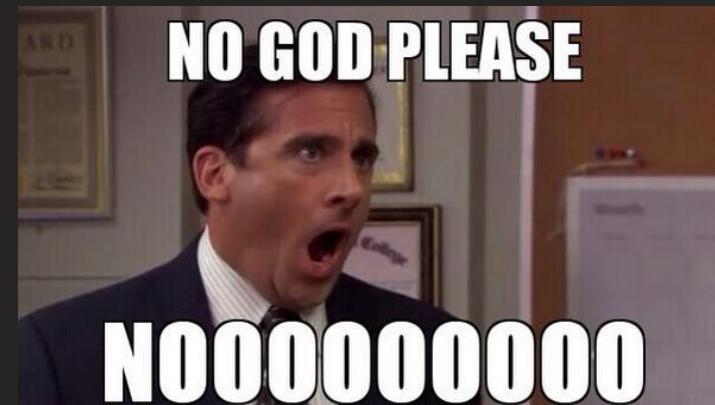
Principles

Do

- Testing Environment
 - Run in production
 - Share to both teams ❤️❤️
- Results Platform
 - Centralize results for all teams ❤️❤️❤️
 - APIs

Don't

- Write reports unless necessary
- Use Microsoft Office
 - Write results in Excel 😭
 - Macros are not meant for continuous operations



bugch3ck/
SharpEfsPotato

Local privilege escalation from SeImpersonatePrivilege using EfsRpc.

AK 1 Issues 0 Stars 90 Forks 13

c2bot 9:31 AM - Yesterday
✓ Created issue with label Privilege Escalation ... <https://github.com/bugch3ck/SharpEfsPotato/issues/1937> GitHub - bugch3ck/SharpEfsPotato: Local privilege escalation from SeImpersonatePrivilege using EfsRpc.

Execution 205 0 +

Defense Evasion 329 0 +

Persistence 71 0 +

- Fingerprinting (T1) #654
- Tailoring Cobalt Strike on Target | TrustedSec (T1) #328
- OPSEC Consideration R&D (T1) #390
- GitHub - NotProb/.NET-Obfuscator: Lists of .NET Obfuscator (Free, Trial, Paid and Open Source) (T1) #163
- GitHub - outflanknl/InlineWhispers: Tool for working with Direct System Calls in Cobalt Strike's Beacon Object Files (BOF) (T1) #297
- GitHub - slaeryan/AQUARMOURY: My musings in C and offensive tooling (T1) #155
- GitHub - br-sn/CheekyBlinder: Enumerating and removing kernel callbacks using signed vulnerable drivers (T1) #137
- COM Hijacking - Calibration Loader (WindowsColorSystem) (Purple) #250
- GitHub - 0xthirteen/StayKit: Cobalt Strike kit for Persistence (Goldorak T1) #133
- BOF - Registry (T1) #121
- Context Menu Hijacking (T1) #756
- Masquerading HKCU (T1) #755
- ShellLink (LNK) (T1) #137

Tradecraft Intelligence Platform

Intelligence Gathering is an everyday task.
Must be as lean as possible!

Prerequisite:

- Choose a ticketing system 💰
- Dev a bot 🤖

Then:

1. Discover attack procedures on twitter
2. Send them to the bot, specify the **Tactic**
3. The bot verify if it already exists
4. Append it to the pile 💩
5. Prioritize through Backlog Grooming

Testing Environment

■ Unit Testing Tools

- Great to quick start testing and automation
- Many open source options
- Can be hard to maintain ...

■ Breach and Attack Simulation (BAS)

- Feeds from up-to-date intel and TTPs
- Great to automatically test if the controls or detection are working... or still working
- Can be used to automate repeatable purple team tests

Results Platform - Vectr

DEMOPURPLE_CE / Enterprise Purple – 2017 Q1 / Malware Profile Simulation

Exploitation

Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 4

Files with Ransomware Extensions #1

Files with Ransomware Extensions #2

Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 1

Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 2

Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 3

01/22/2017 10:40:56
Files with Ransomware Extensions #2 : outcome changed to NotDetected

01/22/2017 09:19:34
Files with Ransomware Extensions #2 : status changed to Completed

01/22/2017 09:15:38
Files with Ransomware Extensions #2 : status changed to InProgress

01/22/2017 08:05:11
Files with Ransomware Extensions #1 : outcome changed to Detected

01/22/2017 07:47:04
Files with Ransomware Extensions #1 : status changed to Completed

01/22/2017 06:54:30
Files with Ransomware Extensions #1 : status changed to InProgress

Test Cases

CAMPAIGN ACTIONS

Action	Tags	Outcome	Status	Test Case	Technique	Phase					
					All	Not Detected	Completed	Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 4	Malware simulation	Exploitation	
					Completed	Detected	Completed	Files with Ransomware Extensions #1	Ransomware	Exploitation	
					Completed	Not Detected	Completed	Files with Ransomware Extensions #2	Ransomware	Exploitation	
					Completed	Not Detected	Completed	Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 1	Malware simulation	Exploitation	

Results Platform - Vectr

Edit Dump lsass.exe - procdump.exe Test Case ENTERPRISE ▾ ×

Status: Completed

▶ ⏸ ⏹ ⏏

Attack Start ? ⚙️
06/20/2019 11:58:29
status changed to InProgress

Attack Stop ? ⚙️
06/20/2019 12:04:51
status changed to Completed

Sources ⚙️

Targets ⚙️

Red Team Details ⚙️

Name
Dump lsass.exe - procdump.exe

Description
Dump lsass.exe from task manager

Technique ? Credential Dumping - T1003 Phase Credential Access

Operator Guidance
procdump.exe -accepteula -ma lsass.exe legit.dmp

Automation & logging
Supported Platform(s): Windows, Linux/MacOS (Bash shell)

Build/Run Logs **0** Import Logs

Configure Build & Download

Blue Team Details ⚙️

Outcome
 TBD Blocked Detected NotDetected

Detecting Blue Tool(s): ⚙️

What was the alert severity?
 TBD Info Low Med High Critical

Outcome Notes
dumped lsass.exe and downloaded legit.dmp

Tags ↗

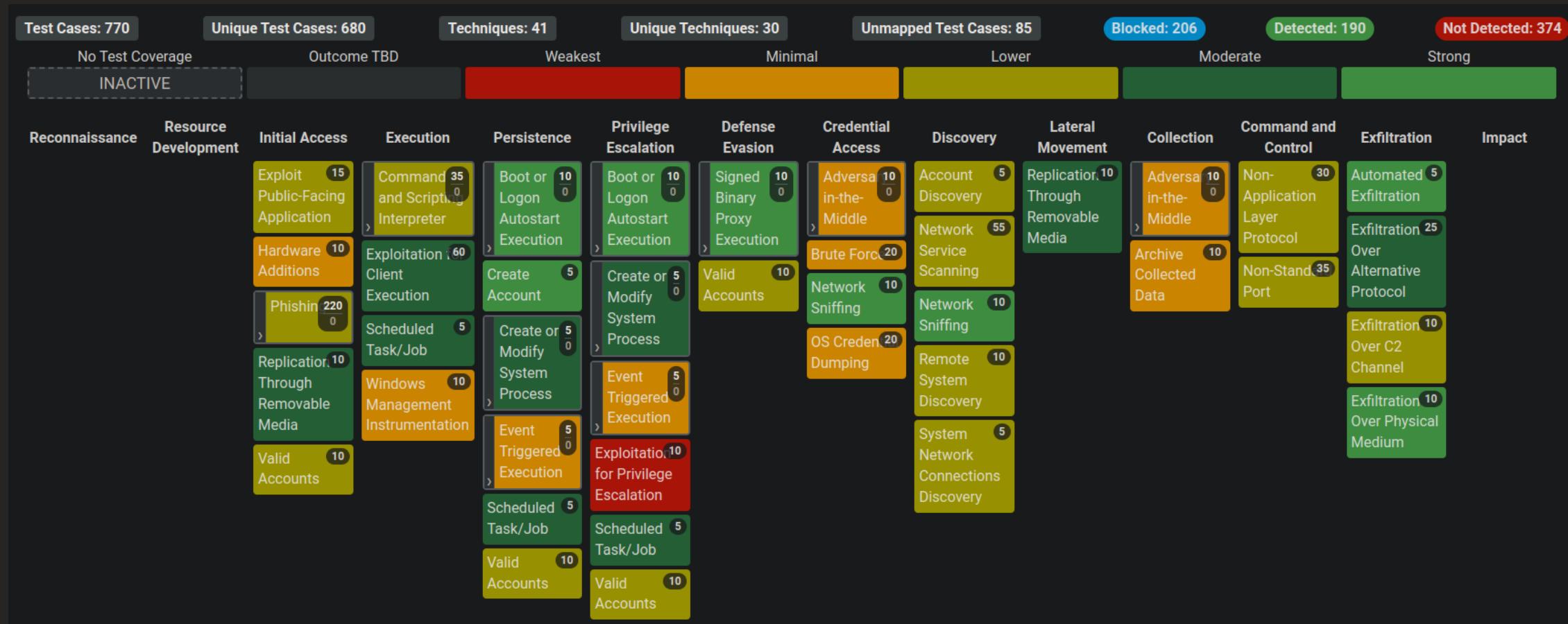
Rules
Sigma Sigma Sigma Sigma Sigma Sigma Sigma Sigma Sigma

Detection

Windows
Common credential dumpers such as [Mimikatz](https://attack.mitre.org/software/S0002) access the LSA Subsystem Service (LSASS) process by opening the process, locating the LSA secrets key, and decrypting the sections in memory where

Cancel Save < >

Results Platform - Vectr



Results Platform - Vectr

Campaigns Aggregated 105

Test Cases Completed: 765

Test Cases Passed: 361

 ■ Detected: 174

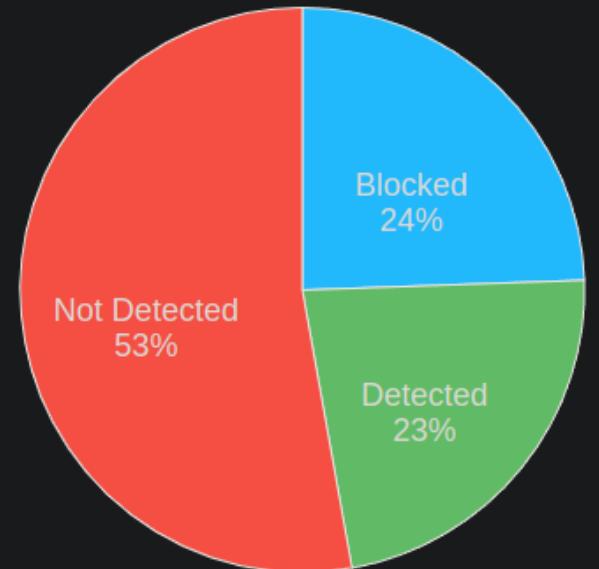
 ■ Blocked: 187

Test Cases Failed: 404

 ■ Not Detected: 404

Test Cases Not Completed: 0

 ■ To Be Determined: 0



Building a (*living*) security posture

What is our next best move?

The quest of building a living security posture

More challenges:

- How do we measure our progression?
- What is the baseline?
- How do we define "good enough"?
- How do we update it in real time?
- 🤯 What the hell is a security posture? 🤯



The quest of building a living security posture

A **security posture** is an organization's overall cybersecurity strength and how well it can predict, prevent, detect and respond to ever-changing cyber threats. ^{^1}

MVP

- Must be built from irrefutable data 
- Must fit a single page 
- Quantitative over Qualitative
- Indicators with colours 
- Support "ever-changing cyber threats" 
- Must quickly answer where we're **good** and where we're **bad**.

Solution: Use the Mitre ATT&CK Navigator *with a few hacks.*

ATT&CK Navigator

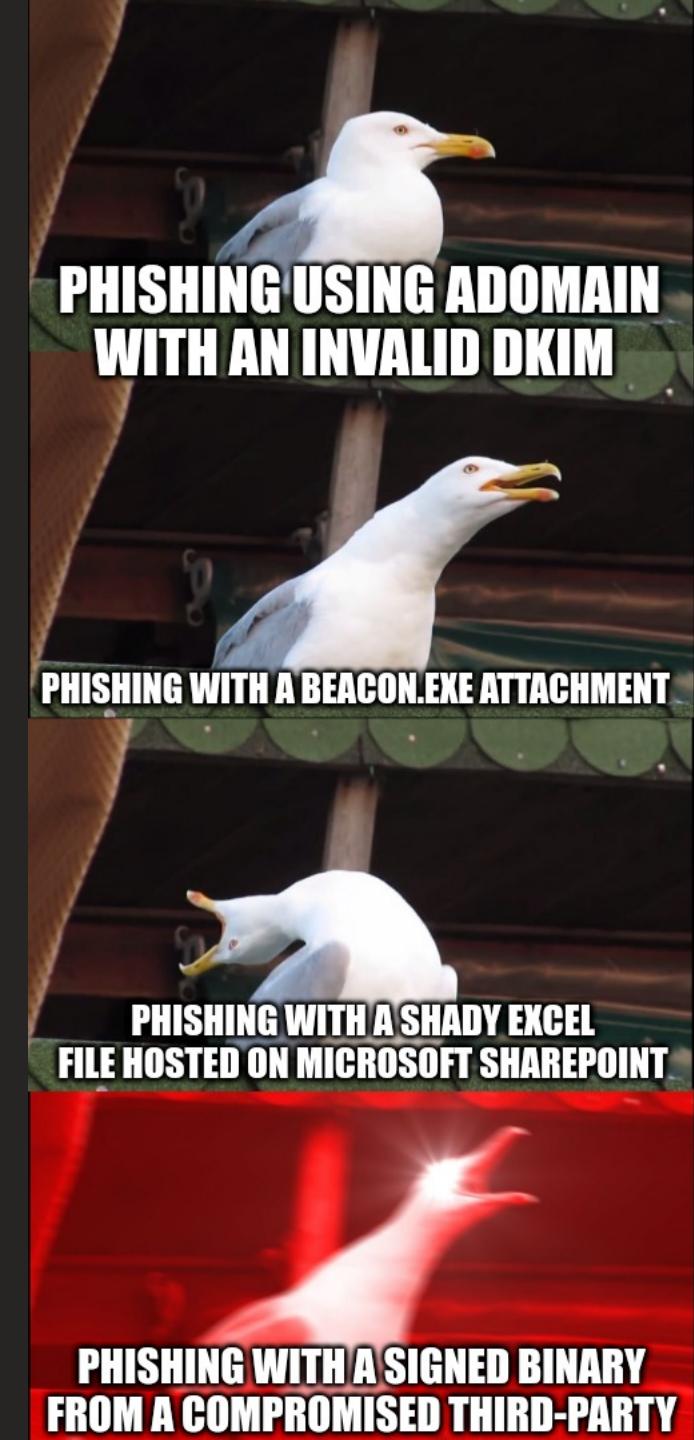
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction	
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact	
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Build Image on Host	Cloud Infrastructure Discovery	Cloud Service Dashboard	Remote Service Session Hijacking (0/2)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Debugger Evasion	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Discovery	Clipboard Data	Dynamic Resolution (0/3)	Data from Cloud Storage Object	Defacement (0/2)	Disk Wipe (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deploy Container	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Encrypted Services (0/6)	Replication Through Removable Media	Data from Configuration Channel (0/2)	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Direct Volume Access	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Input Capture (0/4)	Container and Resource Discovery	Fallback Channels	Data from Configuration Repository (0/2)	Firmware Corruption	Inhibit System Recovery	Network Denial of Service (0/2)
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Escape to Host	Execution Guardrails (0/1)	Execution Guardrails (0/1)	Modify Authentication Process (0/5)	Debugger Evasion	Ingress Tool Transfer	Data from Information Repositories (0/3)	Resource Hijacking	Service Stop	System Shutdown/Reboot
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Domain Trust Discovery	Software Deployment Tools	Scheduled Transfer	Multi-Stage Channels	Non-Application Layer Protocol	Non-Standard Port	
Search Victim-Owned Websites		System Services (0/2)	User Execution (0/3)	External Remote Services	Hijack Execution Flow (0/12)	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Interception	Taint Shared Content	Transfer Data to Cloud Account	Protocol Tunneling	Protocol Tunneling	Proxy (0/4)	
			Windows Management Instrumentation	Hijack Execution Flow (0/12)	Hide Artifacts (0/10)	Multi-Factor Authentication Request Generation	Use Alternate Authentication Material (0/4)	Data from Local System		Data from Removable Media	Data Staged (0/2)	Email Collection (0/3)	
				Implant Internal Image	Process Injection (0/12)	Network Sniffing		Data from Network Shared Drive		Input Capture (0/4)	Remote Access Software	Traffic Signaling (0/1)	
				Modify Authentication Process (0/5)	Scheduled Task/Job (0/5)	Impair Defenses (0/9)		Network Share Discovery		Screen Capture			
				Office Application Startup (0/6)	Valid Accounts (0/4)	OS Credential Dumping (0/8)		Network Sniffing					
					Indirect Command Execution	Indicator Removal on Host (0/6)		Password Policy Discovery					
					Masquerading (0/7)	Steal Application Access Token		Peripheral Device Discovery					
						Steal or Forge Kerberos		Permission Groups					

ATT&CK Navigator - Select your Threat Groups



ATT&CK Navigator - Technique vs Procedure

- The technique is **what**
- The procedure is **how**
- For example, the technique **Phishing** can be executed via:
 - A domain with an invalid DKIM
 - A domain with high reputation
 - A domain with low reputation
 - The organization's domain
 - All kinds of attachments
 - Links
 - *At least 100 more procedures...*



For each procedure, we will define 3 fields

Result	Expected result	Sophistication level
<p>The scored result of the attack during the purple team exercise.</p> <ul style="list-style-type: none">■ Blocked (3)■ Detected (2)■ Logged (1)■ Not Logged (0)	<p>The scored expected result of the attack during the purple team exercise.</p> <ul style="list-style-type: none">■ Blocked (3)■ Detected (2)■ Logged (1)■ Not Logged (0) <p>Need to be realistic, otherwise the posture will just be red...</p>	<p>The minimum sophistication level of the Threat Actor.</p> <ul style="list-style-type: none">■ Strategic (7)■ Innovator (6)■ Expert (5)■ Advanced (4)■ Intermediate (3)■ Minimal (2)■ None (1)

The sophistication level comes from STIX 2.1

Gaps

$$Gap = ExpectedResult - Result$$

An example with Phishing technique (T1566):

Procedure	Result	Expected result	Sophistication	Gap
Phishing using a domain with an invalid DKIM	Logged(1)	Blocked(3)	Minimal(2)	2
Phishing with an excel file hosted on Sharepoint	Logged(1)	Detected(2)	Intermediate(3)	1
Phishing with a signed binary from a compromised third-party	Logged(1)	Logged(1)	Expert(5)	0

Weighted Gaps

$$Gap' = Gap * Weight$$

We can push it even further by adding a **weight** dimension, which can be as simple as the **popularity of the attack technique** (not procedure). An example with several techniques

Procedure	Gap	Weight	Weighted Gap
Phishing using a domain with an invalid DKIM	2	7	14
Phishing with a signed binary from a compromised third-party	0	7	0
Hardware Additions via a Rubber Ducky	2	1	2

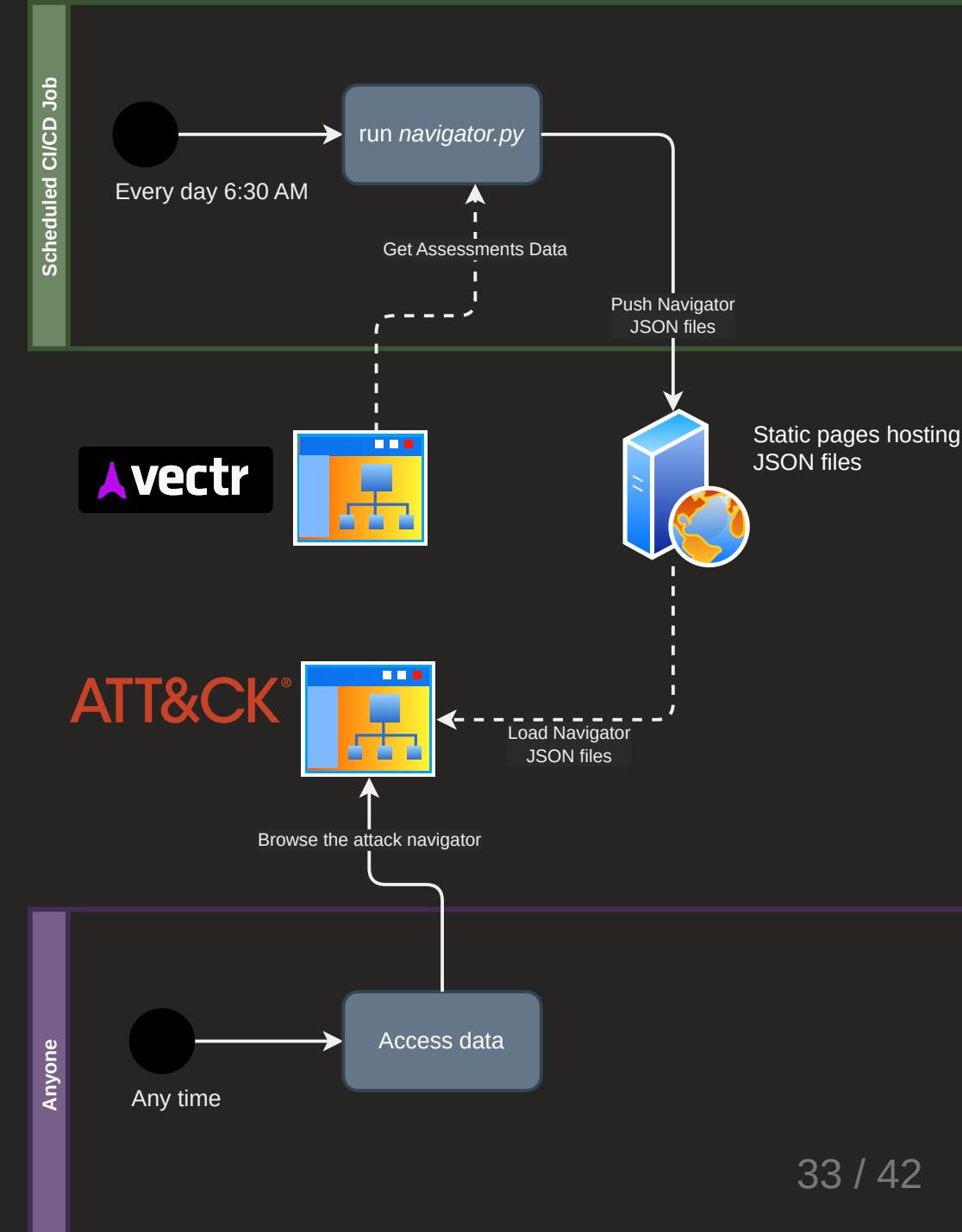
Add a pinch of CI/CD 🤝

Every morning:

1. A scheduled job start
2. Data is pulled from Vectr
3. Several JSON files are generated
4. The files are uploaded on a static website

Any time:

- Navigate the navigator 😊



Security Posture - Gaps

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impersonation 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (1/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Removal (0/1)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Desync for Impact (0/1)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Exfiltration Over Alternative Protocol (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/1)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Encoding (0/2)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/1)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Data Obfuscation (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wiping (0/1)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Container and Resource Discovery	Domain Trust Discovery	Dynamic Resolution (0/3)	Encrypted Channel (0/2)	Exfiltration Over Network Service (0/1)	Endpoint of Service Corruption (0/1)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Man-in-the-Middle (0/2)	Domain Trust Discovery	File and Directory Discovery	Data from Configuration Repository (0/2)	Firmware Corruption (0/1)	Inhibit Service Recovery (0/1)	Network Service Configuration (0/1)
Search Open Technical Databases (0/5)	Trusted Relationship	Shared Modules	Software Deployment Tools	Event Triggered Execution (0/11)	Escape to Host	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	Domain Trust Discovery	File and Directory Discovery	Data from Information Repositories (0/2)	File and Directory Discovery	Exfiltration Over Web (0/2)	Resource Hijacking (0/1)
Search Open Websites/Domains (0/2)	Valid Accounts (0/4)	System Services (0/2)	User Execution (0/3)	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Data from Local System	File and Directory Discovery	Scheduled Transfer (0/2)	Service Splicing (0/1)
Search Victim-Owned Websites			Windows Management Instrumentation	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	OS Credential Dumping (0/8)	File and Directory Discovery	Network Service Scanning	Data from Network Shared Drive	File and Directory Discovery	Transfer Data (0/2)	Custom Item (0/1)
				Implant Internal Image	Process Injection (0/11)	Hijack Execution Flow (0/11)	Steal Application Access Token	File and Directory Discovery	Network Share Discovery	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
				Modify Authentication Process (0/4)	Scheduled Task/Job (0/7)	Impair Defenses (0/7)	Steal or Forge Kerberos Tickets (0/4)	File and Directory Discovery	Network Sniffing	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
				Office Application Startup (0/6)	Valid Accounts (0/4)	Indicator Removal on Host (0/6)	Steal Web Session Cookie	File and Directory Discovery	>Password Policy Discovery	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
				Pre-OS Boot (0/5)		Indirect Command Execution	Two-Factor Authentication Interception	File and Directory Discovery	Peripheral Device Discovery	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
				Scheduled Task/Job (0/7)		Masquerading (0/6)	Unsecured Credentials (0/7)	File and Directory Discovery	Permission Groups Discovery (0/3)	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
				Server Software Configuration (0/1)		Modify Authentication Process (0/4)	Modify Cloud Compute Infrastructure (0/4)	File and Directory Discovery	Process Discovery	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
						Modify Cloud Compute Infrastructure (0/4)	Unsecured Credentials (0/7)	Query Registry	Query Registry	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
						Custom Item (0/1)	Custom Item (0/1)	Remote System Discovery	Remote System Discovery	Use Alternate Authentication Material (0/7)	File and Directory Discovery		
						Custom Item (0/1)	Custom Item (0/1)	Software Discovery (0/1)	Software Discovery (0/1)	Use Alternate Authentication Material (0/7)	File and Directory Discovery		

legend

#32e379 Tested and compliant (1)

#f5cb1b Tested and 1pts gap (2)

#f5881b Tested and 2pts gap (3)

#f16e6e Tested and 3pts gap (4)

Add Item

Clear

Security Posture - Weighted Gaps (*Most important*)

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (1/6)	Drive-by Compromise	Command and Scripting Interpreter (4/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (2/4)	Exploitation of Remote Services	Archive Collected Data (1/3)	Application Layer Protocol (2/4)	Automated Exfiltration (0/1)	Account Access Removal	
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (1/5)	Credentials from Password Stores (1/5)	Application Window Discovery	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction		
Gather Victim Identity Information (1/3)	Compromise Infrastructure (1/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (2/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol (1/3)	Data Encrypted for Impact		
Gather Victim Network Information (0/6)	Develop Capabilities (1/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Clipboard Data	Data Encoding (1/2)	Data Obfuscation (0/3)	Data Manipulation (0/3)		
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (2/3)	Inter-Process Communication (1/2)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Forge Web Credentials (0/2)	Cloud Service Dashboard	Cloud Service Discovery	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Defacement (0/2)		
Phishing for Information (0/3)	Obtain Capabilities (2/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (1/4)	Input Capture (0/4)	Container and Resource Discovery	Dynamic Resolution (2/3)	Disk Wipe (0/2)	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)		
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Scheduled Task/Job (1/7)	Shared Modules	Domain Policy Modification (1/2)	Domain Policy Modification (1/2)	Man-in-the-Middle (1/2)	Domain Trust Discovery	Encrypted Channel (1/2)	Encrypted Channel (1/2)	Exfiltration Over Physical Medium (0/1)	Firmware Corruption		
Search Open Technical Databases (0/5)	Supply Chain Compromise (1/3)	Trusted Relationship	Software Deployment Tools	Create Account (0/3)	Escape to Host	Execution Guardrails (0/1)	File and Directory Discovery	Fallback Channels	Ingress Tool Transfer	Inhibit System Recovery			
Search Open Websites/Domains (0/2)	Valid Accounts (1/4)	System Services (1/7)	User Execution (2/15)	Event Triggered Execution (2/15)	Event Triggered Execution (2/15)	Exploitation for Defense Evasion	Network Service Scanning	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (0/2)			
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (0/11)	File and Directory Permissions Modification (1/2)	Network Share Discovery	Data from Removable Media	Transfer Data	Resource Hijacking			
				Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	Network Sniffing						
				Implant Internal Image	Impair Defenses (2/7)	Steal Application Access Token	Network Sniffing						
				Modify Authentication Process (0/4)	Indicator Removal on Host (2/6)	Steal or Forge Kerberos Tickets (1/4)	>Password Policy Discovery						
				Office Application Startup (0/6)	Indirect Command Execution	Peripheral Device Discovery							
				Pre-OS Boot (0/1)	Masquerading (2/6)	Steal Web Session Cookie	Permission Groups (0/3)						
					Modify Authentication Process (0/1)	Two-Factor Authentication Interception	Process Discovery						
					Unsecured	Unsecured	Query Registry						
							Remote System Discovery						

Where are our gaps?

Need to be able to answer the question quickly.

From quantitative to qualitative.

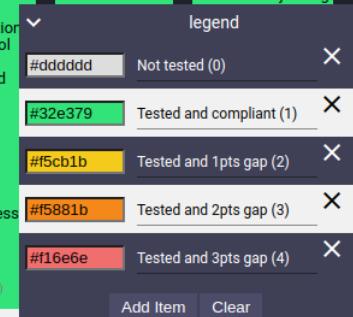
Solution: metadata field

How to: Mouse over

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense 39 tec
Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Mechanism
Exploit Public-Facing Application Phishing (T1566)	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation
Scored Remote *GAP* Using a domain with an invalid DKIM header	Execution (0/14)	Boot or Logon Autostart	Boot or Logon Autostart	BITS Jobs
GAP Using an aged domain in the finance category:	Boot or Logon Initialization Scripts (0/5)	Client Execution	Logged but should be Blocked	Logged but should be Detected
From employee A to employee B:itation for Additions	Browser Extensions	Initialization Scripts (0/5)	Deobfuscate Files or Info	Deploy Content
Phishing (0/3)	Inter-Process Communication (0/2)	Compromise Client Software Binary	Create or Modify System Process (0/4)	Direct Volume
Replication Through Removable Media	Native API	Scheduled Task/Job (0/7)	Domain Policy Modification (0/2)	Domain Policy Modification
Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Execution Guardrails (0/1)	Execution Guardrails
Trusted Relationship	Shared Modules	Software Deployment Tools	Escape to Host	Exploitation Evasion
Valid Accounts (0/4)	System Services (0/2)	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	File and Directory Permissions Modification
	User Execution (0/3)	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Hide Artifacts
	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (0/11)	Hijack Execution Flow
		Hijack Execution Flow (0/11)	Process Injection (0/11)	Impair Defense
		Implant Internal Image	Scheduled Task/Job (0/7)	Indicator Removal Host (0/6)
		Modify Authentication	Valid	Indirect Control

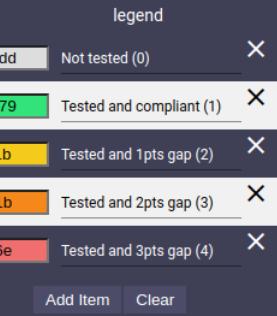
Security Posture - Gaps - filter (sophistication=1)

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (1/6)	Drive-by Compromise	Command and Scripting Interpreter (0/6)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command (0/6)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/4)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Clipboard Data	Cloud Service Dashboard	Data Obfuscation (0/3)	Exfiltration Over C2 Channel (0/1)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Remote Service Session Hijacking (0/2)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Direct Volume Access	Deploy Container	Input Capture (0/4)	Container and Resource Discovery	Remote Services (0/6)	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Man-in-the-Middle (0/2)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (0/2)	Fallback Channels	Infiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Trusted Relationship	Shared Modules	Software Deployment Tools	Create or Modify System Process (0/4)	Escape to Host	Execution Guardrails (0/1)	File and Directory Discovery	File and Directory Discovery	Data from Local System	Ingress Tool Transfer	Multi-Stage Channels	Inhibit System Recovery	File Corruption
Search Open Websites/Domains (0/2)	Valid Accounts (0/4)	System Services (0/2)	User Execution (0/2)	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Non-Application Layer Protocol	Exfiltration Over Network Medium (0/2)	Network Denial of Service (0/2)
Search Victim-Owned Websites		Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/6)	Network Share Discovery	Use Alternate Authentication Material (2/4)	Data from Removable Media	Non-Standard Port	Protocol Tunneling	Resource Hijacking
		Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Process Injection (0/11)	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Sniffing	Data Staged (0/2)	Email Collection (0/3)	Proxy (0/4)	Remote Access Software	
		Implant Internal Image	Scheduled Task/Job (0/7)	Indicator Removal on Host (0/6)	Impair Defenses (0/7)	Impair Defenses (0/7)	Steal or Forge Kerberos Tickets (0/4)	Password Policy Discovery	Input Capture (0/4)	Man in the Browser	Traffic Signaling (0/1)		
		Modify Authentication Process (0/4)	Office Application Startup (0/6)	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Steal Web Session Cookie	Peripheral Device Discovery	Man-in-the-Middle (0/2)	Screen Capture			
				Masquerading (0/6)	Masquerading (0/6)	Masquerading (0/6)	Two-Factor Authentication Interception	Permission Groups Discovery	Process Discovery				
				Modify Authentication	Modify Authentication	Modify Authentication	Remote System	Query Registry					



Security Posture - Gaps - filter (sophistication=2)

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2) Gather Victim Host Information (0/4) Gather Victim Identity Information (0/3) Gather Victim Network Information (0/6) Gather Victim Org Information (0/4) Phishing for Information (0/3) Search Closed Sources (0/2) Search Open Technical Databases (0/5) Search Open Websites/Domains (0/2) Search Victim-Owned Websites	Acquire Infrastructure (1/6) Compromise Accounts (0/2) Compromise Infrastructure (0/6) Develop Capabilities (0/4) Establish Accounts (0/2) Obtain Capabilities (0/6) Stage Capabilities (0/5) Supply Chain Compromise (0/3) Trusted Relationship Valid Accounts (0/4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (0/3) Replication Through Removable Media Scheduled Task/Job (0/7) Shared Modules Software Deployment Tools System Services (0/2) User Execution (0/3) Windows Management Instrumentation	Command and Scripting Interpreter (0/8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (0/2) Native API Compromise Client Software Binary Create Account (0/3) Create or Modify System Process (0/4) Event Triggered Execution (0/15) Event Triggered Execution External Remote Services Hijack Execution Flow (0/1) Hijack Execution Flow (0/1) Implant Internal Image Modify Authentication Process (0/4) Office Application Startup (0/8)	Account Manipulation (0/4) BITS Jobs Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Software Binary Create Account (0/3) Create or Modify System Process (0/4) Event Triggered Execution (0/15) Exploitation for Privilege Escalation External Remote Services Hijack Execution Flow (0/11) Process Injection (0/11) Scheduled Task/Job (0/7) Valid Accounts (0/4)	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create Account (0/3) Create or Modify System Process (0/4) Domain Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Hide Artifacts (0/7) Hijack Execution Flow (0/11) Impair Defenses (0/7) Indicator Removal on Host (0/6) Indirect Command Execution Masquerading (0/6) Modify Authentication	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create Account (0/3) Create or Modify System Process (0/4) Domain Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Hide Artifacts (0/7) Hijack Execution Flow (0/11) Impair Defenses (0/7) Indicator Removal on Host (0/6) Indirect Command Execution Masquerading (0/6) Modify Authentication	Brute Force (0/4) Credentials from Password Stores (0/5) Exploitation for Credential Access Forge Web Credentials (0/2) Input Capture (0/4) Man-in-the-Middle (0/2) Modify Authentication Process (0/4) Network Sniffing OS Credential Dumping (0/8) Steal Application Access Token Steal or Forge Kerberos Tickets (0/4) Steal Web Session Cookie Two-Factor Authentication Interception Remote System	Account Discovery (0/4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (0/2) Process Discovery Query Registry Remote System	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (0/2) Remote Services (0/6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (2/4) Data from Network Shared Drive Data from Removable Media Data Staged (0/2) Non-Standard Port Email Collection (0/3) Input Capture (0/4) Man in the Browser Man-in-the-Middle (0/2) Screen Capture	Archive Collected Data (0/3) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (0/2) Data from Information Repositories (0/2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (0/2) Non-Standard Port Email Collection (0/3) Input Capture (0/4) Man in the Browser Man-in-the-Middle (0/2) Screen Capture	Application Layer Protocol (0/4) Communication Through Removable Media Data Transfer Size Limits Exfiltration Over Alternative Protocol (0/2) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (0/1) Encrypted Channel (0/2) Exfiltration Over Physical Medium (0/1) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Protocol Tunneling Proxy (0/4) Remote Access Software Traffic Signaling (0/1)	Automated Exfiltration (0/1) Data Manipulation (0/3) Defacement (0/2) Disk Wipe (0/2) Endpoint Denial of Service (0/4) Firmware Corruption Inhibit System Recovery Network Denial of Service (0/2) Resource Hijacking	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (0/3) Defacement (0/2) Disk Wipe (0/2) Endpoint Denial of Service (0/4) Firmware Corruption Inhibit System Recovery Network Denial of Service (0/2) Resource Hijacking



Security Posture - Gaps - filter (sophistication=3)

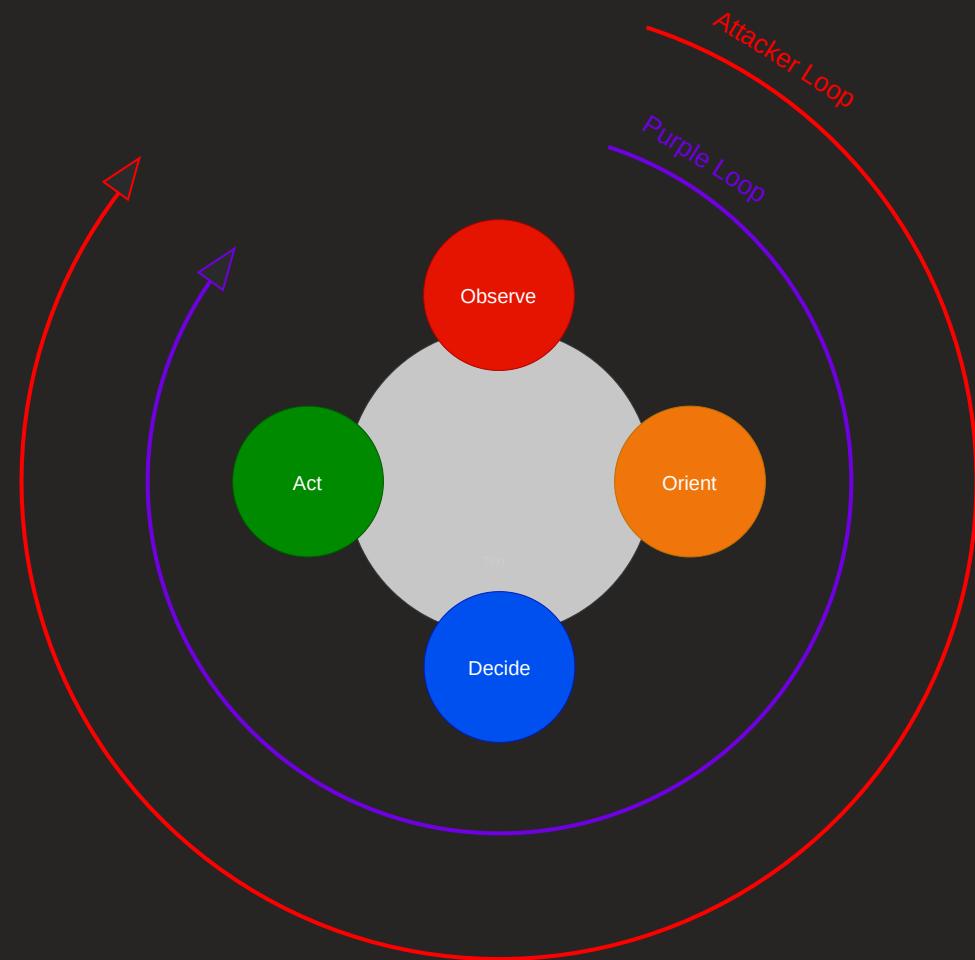
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2) Gather Victim Host Information (0/4) Gather Victim Identity Information (0/3) Gather Victim Network Information (0/6) Gather Victim Org Information (0/4) Phishing for Information (0/3)	Acquire Infrastructure (1/6) Compromise Accounts (0/2) Compromise Infrastructure (0/6) Develop Capabilities (0/4) Establish Accounts (0/2) Obtain Capabilities (0/6) Stage Capabilities (0/5)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (0/3) Replication Through Removable Media Supply Chain Compromise (0/3) Trusted Relationship Valid Accounts (0/4)	Command and Scripting Interpreter (0/8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (0/2) Native API Scheduled Task/Job (0/7) Shared Modules Software Deployment Tools System Services (0/2) User Execution (0/3) Windows Management Instrumentation	Account Manipulation (0/4) BITS Jobs Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create Account (0/3) Create or Modify System Process (0/4) Event Triggered Execution (0/15) External Remote Services Hijack Execution Flow (0/11) Implant Internal Image Modify Authentication Process (0/4) Office Application Startup (0/6)	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) Boot or Logon Autostart Execution (0/14) Build Image on Host Boot or Logon Initialization Scripts (0/5) Create or Modify System Process (0/4) Direct Volume Access Domain Policy Modification (0/2) Execution Guardrails (0/1) Escape to Host Exploitation for Defense Evasion Event Triggered Execution (0/15) Exploitation for Privilege Escalation External Remote Services Hijack Execution Flow (0/11) Implant Internal Image Modify Authentication Process (0/4) Office Application Startup (0/6)	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (0/2) Execution Guardrails (0/1) Escape to Host Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Hide Artifacts (0/7) Hijack Execution Flow (0/11) Impair Defenses (0/7) Indicator Removal on Host (0/6) Indirect Command Execution Masquerading (0/6) Modify Authentication	Brute Force (0/4) Credentials from Password Stores (0/5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (0/2) Input Capture (0/4) Man-in-the-Middle (0/2) Modify Authentication Process (0/4) Network Sniffing OS Credential Dumping (0/6) Steal Application Access Token Steal or Forge Kerberos Tickets (0/4) Steal Web Session Cookie Two-Factor Authentication Interception Remote System	Account Discovery (0/4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (0/3) Process Discovery Query Registry	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (0/2) Remote Services (0/6) Replication Through Removable Media Data from Configuration Repository (0/2) Data from Information Repositories (0/2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (0/2) Email Collection (0/3) Input Capture (0/4) Man in the Browser Man-in-the-Middle (0/2) Screen Capture	Archive Collected Data (0/3) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (0/2) Data from Fallback Channels Data from Information Repositories (0/2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (0/2) Email Collection (0/3) Input Capture (0/4) Man in the Browser Man-in-the-Middle (0/2) Screen Capture	Application Layer Protocol (0/4) Communication Through Removable Media Data Transfer Size Limits Data Obfuscation (0/3) Data Transfer Over Alternative Protocol (0/3) Data Transfer Over C2 Channel Data Transfer Over Other Network Medium (0/1) Data Transfer Over Physical Medium (0/1) Data Transfer Over Web Service (0/2) Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (0/4) Remote Access Software Traffic Signaling (0/1)	Automated Exfiltration (0/1) Data Destruction Data Encrypted for Impact Data Manipulation (0/3) Defacement (0/2) Disk Wipe (0/2) Endpoint Denial of Service (0/4) Firmware Corruption Inhibit System Recovery Network Denial of Service (0/2) Resource Hijacking	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (0/3) Defacement (0/2) Disk Wipe (0/2) Endpoint Denial of Service (0/4) Firmware Corruption Inhibit System Recovery Network Denial of Service (0/2) Resource Hijacking
Search Closed Sources (0/2) Search Open Technical Databases (0/5) Search Open Websites/Domains (0/2) Search Victim-Owned Websites													
legend													
#dddddd">Not tested (0) X													
#32e379 Tested and compliant (1) X													
#f5cb1b Tested and 1pts gap (2) X													
#f5881b Tested and 2pts gap (3) X													
#f16e6e Tested and 3pts gap (4) X													
Add Item Clear													

The ultimate goal

Improve the security posture!

The Shortest Loop Wins!

- Can you identify your gaps faster than the attacker?
- Can you adjust faster than your opponent?
- How can you disrupt their OODA Loop?



Thank you! 🤘 🙏 ❤

We wish you an awesome HF14!

And the most important of all: Avoid Excel 😊

