Unlocking The Power of Threat Intelligence Infused Detections in The SOC

Ray Huang
Senior Security Solution Architect
Cisco Splunk

© 2024 SPLUNK INC.

Agenda

- Detection Engineering Challenges and Level Set
- MITRE ATT&CK Framework for Strategizing Detections
- Valuable Sources for Detections
- Cyber Threat Intelligence Level Set
- Challenges with Natural Language Based Threat Advisories
- Usage of Large Language Models on NLP Based Threat Advisories towards Detection Engineering

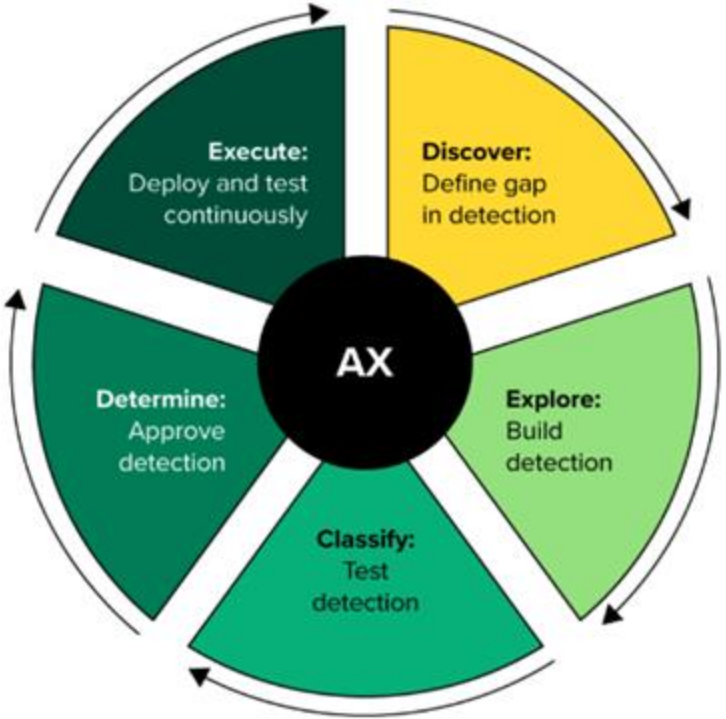
Detection Engineering Challenges

Lack of Dedicated Detection Engineering Team

- **Limited skillsets.**
- **Don’t know where to begin.**
- **No planning framework.**
- **Creation manual and adhoc**

- **Rabbit Hole of Noisy Detections**
- **Duplicate Detections**
- **Expired or Irrelevant Detections**

Level Set of Detection Engineering Lifecycle



Source: Forrester - Enhance Your Security Operations with Agile and Detection Engineering

How to Organize and Prioritize?

1. Focus on Tactics, Techniques and Procedures

2. Use a TTP Focussed Security Framework
   - Cyber Kill Chain
   - MITRE ATT&CK

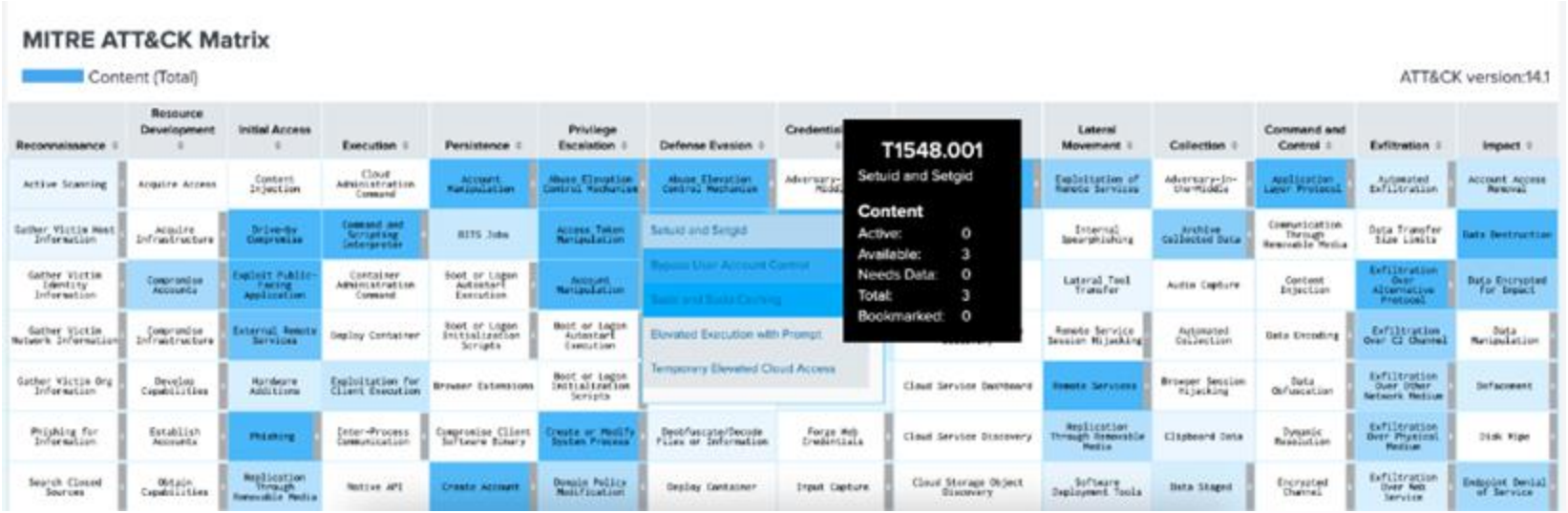
MITRE ATT&CK™

Planning Detection Coverage With MITRE ATT&CK

- TTP Based Detection Coverage

- Filters are your friend (APTs, Tactics, Techniques, Industry, Operating System, Software etc.)

- Color coding and comparison over time.



Why is Cyber Threat Intelligence A Critical Input?

External Visibility

We don’t know what we don’t know unless we look outside

Situation Awareness

Awareness of our own environment, risks, impacts, mitigations.

Pre-emptive Defense

Defend against the threat before it even occurs in our environment

Financial Loss Prevention

Successful pre-emption = Incident Avoidance = Financial Loss Prevention

Different Types of CTI

Technical

- Technical IOCs
- Machine Readable Format (e.g. STIX via TAXII)
- Easy to Ingest as Detection Engineering Inputs

Tactical

- Machine Readable Format
- TTP Enriched
- Easy for machine interpretation

Operational

- Intel of Specific Targeted Attacks
- Formatted in plain human language (plain English
- Easy for human, hard for machine

Strategic

- High Level Information for Execs
- Formatted in plain human language (plain English
- Easy for human, hard for machine

I will focus on value of these types today

Operation and Strategic CTI (Threat Advisories)

This is Good and Organized which we may see sometimes

Introduction to HAFNIUM and the Exchange Zero-Day Activity

On Tuesday, March 2, 2021, Microsoft released a set of security patches for its mail server, Microsoft Exchange. These patches respond to a group of vulnerabilities known to impact Exchange 2013, 2016, and 2019. It is important to note that an Exchange 2010 security update has also been issued, though the CVEs do not reference that version as being vulnerable.

While the CVEs do not shed much light on the specifics of the vulnerabilities or exploits, the first vulnerability (CVE-2021-26855) has a remote network attack vector that allows the attacker, a group Microsoft named HAFNIUM, to authenticate as the Exchange server. Three additional vulnerabilities (CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) were also identified as part of this activity. When chained t 2021-26855 for initial access, the attacker would have complete c Exchange server. This includes the ability to run code as SYSTEM a the server.

A temporary mitigation for these vulnerabilities from external threa to OWA, such as placing the OWA server behind a VPN to prevent e does not, however, prevent an internal attacker from exploiting the patch as soon as possible.

MITRE ATT&CK

Reviewing the blog posts from Microsoft and Volexity, we mapped the adversary's activity to MITRE ATT&CK. Each tactic is then linked to Splunk Content to help you hunt for that information. Be aware; these searches are provided as a way to accelerate your hunting. We recommend you configure them via the Splunk Security Essentials App. You may need to modify them to work in your environment! Many of these searches are optimized for use with the tstats command.

Finally, as more information becomes available, we will update these searches if more ATT&CK TTPs become known.

ATT&CK Tactic	Title	HAFNIUM activity	Splunk Searches
T1003.001	OS Credential Dumping: LSASS Memory	Used Procdump to export LSASS	Dump LSASS via Procdump Dump of LSASS using comsvcs.dll
T1059.001	Command and Scripting Interpreter: PowerShell	Nishang PowerShell	Malicious PowerShell Process - Connect To Internet With Hidden Window, Malicious PowerShell Process - Execution Policy Bypass Attempt To Set Default PowerShell Execution Policy To Unrestricted or Bypass

Mostly, This is What We May Get

Email scammers impersonating the ASD's ACSC

Alert status: Medium

Content complexity: Straight

First published: 28 Aug 2024
Last updated: 28 Aug 2024

Content written for: Individuals & families

Share on

This document has been written for individuals and families.

Background / What has happened?

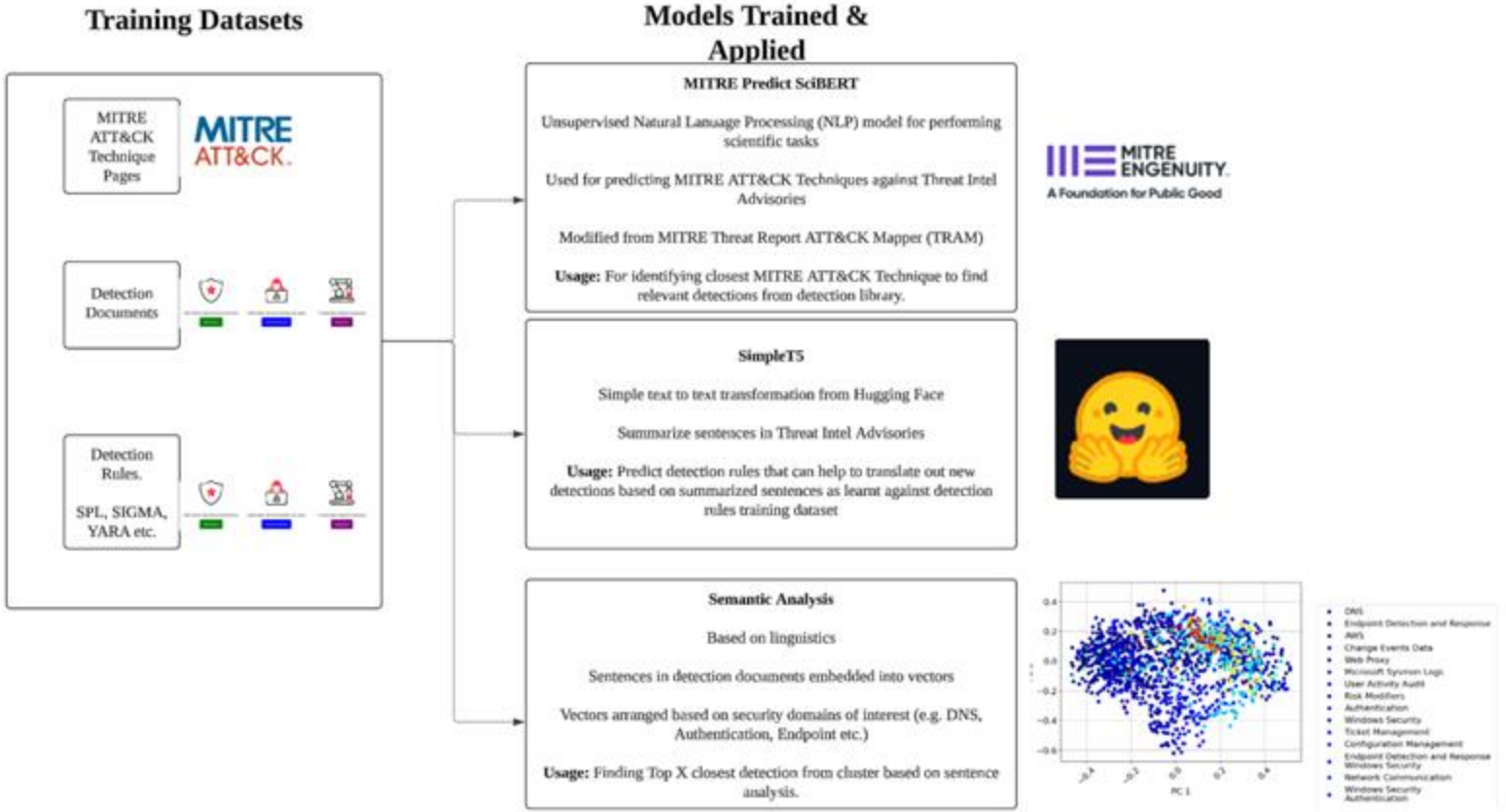
If you receive an email from the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and you wish to verify that it is legitimate, please contact us on 1300 CYBER (1300 292 371).

The ASD's ACSC is aware of emails from cybercriminals claiming to be ASD's ACSC. The cybercriminals are emailing from spoofed email accounts utilising ASD's ACSC's logo, with the subject and contents of the emails varying.

These emails suggest that an increase in cyber threats requires the recipient to download 'Antivirus' software through a malicious link to stay safe. If clicked on, there is potential that malicious software could be downloaded and installed to the individual's computer.

Other instances of the emails warn recipients that there have been complaints regarding their email address or IP address and again asks recipients to download the malicious 'Antivirus' software, to safeguard their account.

Large Language Model Applications for Natural Language Based Threat Intel Advisories Towards Detection Engineering



SciBERT Based LLM for MITRE Prediction For Advisories

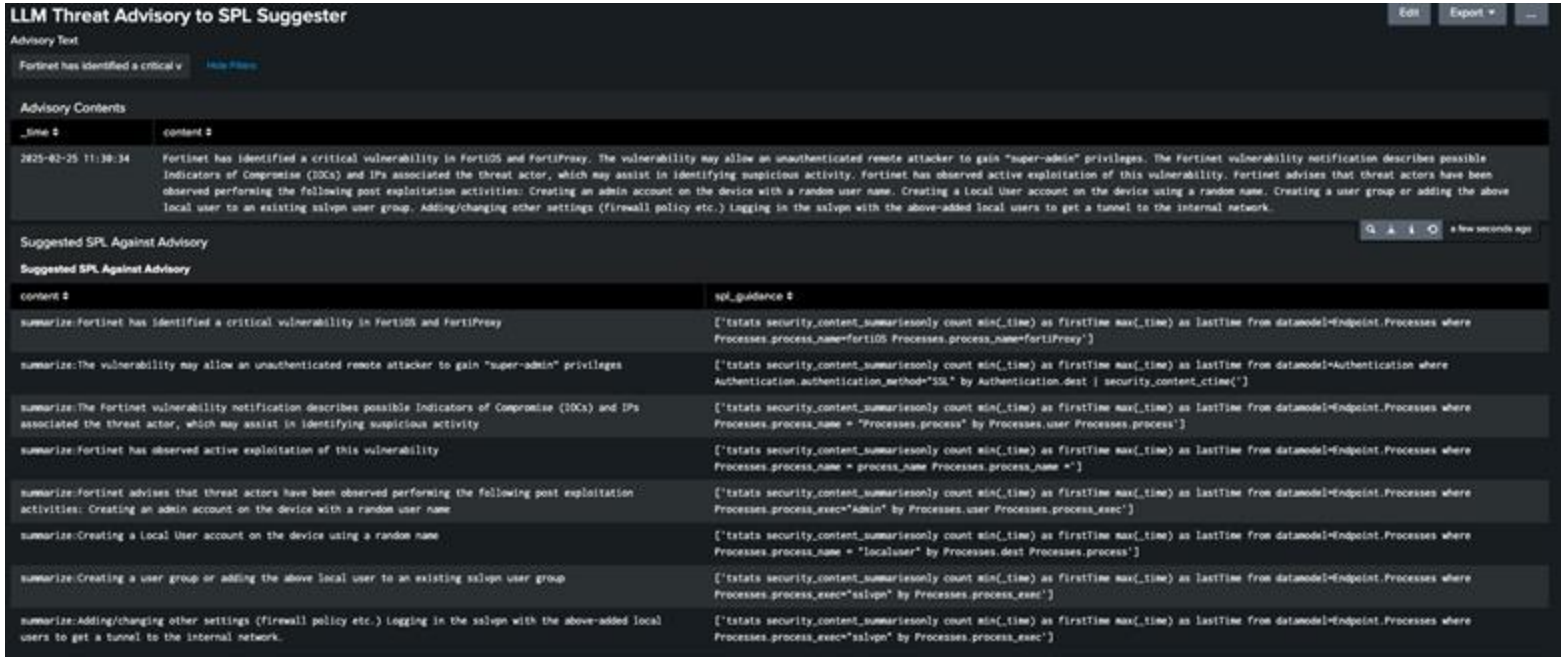
LLM prediction of MITRE Technique ID based on sentence

Selecting relevant model predicted techniques to identify relevant detections from library

predicted_segment	predicted_label(s)
["If you receive an email from the Australian Signals Directorate's Australian Cyber Security	{'Spearphishing Attachment - T1566.001'}
from the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and you	{'Disable or Modify Tools - T1562.001', 'Security Software Discovery - T1518.001', 'Remote Access Software - T1219'}
Australian Cyber Security Centre (ASD's ACSC) and you wish to verify that it	{'Security Software Discovery - T1518.001'}
ACSC) and you wish to verify that it is legitimate, please contact us	{'Brute Force - T1110', 'Security Software Discovery - T1518.001'}
verify that it is legitimate, please contact us on 1300 CYBER1 (1300 292	{'File and Directory Discovery - T1083', 'Security Software Discovery - T1518.001', 'Brute Force - T1110'}
please contact us on 1300 CYBER1 (1300 292 371). The ASD's ACSC is	{'Malicious File - T1204.002', 'Ingress Tool Transfer - T1105'}
CYBER1 (1300 292 371). The ASD's ACSC is aware of emails from cybercriminals	{'Spearphishing Attachment - T1566.001'}
ASD's ACSC is aware of emails from cybercriminals claiming to be ASD's ACSC.	{'Match Legitimate Name or Location - T1036.005', 'Spearphishing Attachment - T1566.001'}
emails from cybercriminals claiming to be ASD's ACSC. The cybercriminals are emailing from spoofed email accounts utilising ASD's ACSC's logo, with the subject	{'Spearphishing Attachment - T1566.001'}
accounts utilising ASD's ACSC's logo, with the subject and contents of the emails	{'Valid Accounts - T1078', 'Spearphishing Attachment - T1566.001'}

mitre_technique	detectionName
T1033	check_elevated_cmd_using_whoami
T1033	getcurrent_user_with_powershell
T1033	getcurrent_user_with_powershell_script_block
T1033	system_user_discovery_with_query
T1033	system_user_discovery_with_whoami

SimpleT5 LLM for Suggested Detection Rule Syntax



summarize:The vulnerability may allow an unauthenticated remote attacker to gain "super-admin" privileges	['tstats security_content_summariesonly count min(_time) as firstTime max(_time) as lastTime from datamodel=Authentication where Authentication.authentication_method="SSL" by Authentication.dest | security_content_ctime(']

Summarized Sentence **Suggested Detection Rule Syntax**

Semantic Analysis LLM for Suggested Rule Syntax

_time	content
2025-02-25 13:14:21	Fortinet has identified a critical vulnerability in FortiOS and FortiProxy. The vulnerability may allow an unauthenticated remote attacker to gain "super-admin" privileges. The Fortinet vulnerability notification describes possible Indicators of Compromise (IOCs) and IPs associated the threat actor, which may assist in identifying suspicious activity. Fortinet has observed active exploitation of this vulnerability. Fortinet advises that threat actors have been observed performing the following post exploitation activities: Creating an admin account on the device with a random user name. Creating a Local User account on the device using a random name. Creating a user group or adding the above local user to an existing sslvpn user group. Adding/changing other settings (firewall policy etc.) Logging in the sslvpn with the above-added local users to get a tunnel to the internal network.

Suggested Detections Against Advisory Sentence

Click on the suggestion value to view details of the suggested content

content	suggestion_1	suggestion_2	suggestion_3	suggestion_4
Fortinet has identified a critical vulnerability in FortiOS and FortiProxy		fortinet_appliance_auth_bypass	spectre_and_meltdown_vulnerable_systems	tt89
The vulnerability may allow an unauthenticated remote attacker to gain "super-admin" privileges	allow_operation_with_consent_admin	fortinet_appliance_auth_bypass	privileged_acts_unprivileged_users	splunk_list_all_nonstandard_admin_accounts

detectionName	description	datamodel	enabled
fortinet_appliance_auth_bypass	CVE-2022-40684 is a Fortinet appliance auth bypass that is actively being exploited and a POC is released publicy. The POC adds a SSH key to the appliance. Note that the exploit can be used with any HTTP method (GET, POST, PUT, DELETE, etc). The REST API request failing is not an indication that an attacker was unsuccessful. Horizon3 was able to modify the admin SSH keys though a REST API request that reportedly failed. The collection /api/v2/ endpoints can be used to configure the system and modify the administrator user. Any logs found that meet the above conditions and also have a URL containing /api/v2/ should be cause for concern. Further investigation of any matching log entries can reveal any damage an attack has done. Additionally, an attacker may perform the following actions to further compromise a system Modify the admin SSH key to enable the attacker to login to the compromised system. \ Add new local users. \ Update networking configurations to reroute traffic. \ Download the system configuration. \ Initiate packet captures to capture other sensitive system information. Reference Horizon3.ai	Web	No

Key Takeaways

- Understanding Challenges and Necessities of Detection Engineering
- Cyber Threat Intelligence Should Be a Key Input for Detections
- Never disregard Strategic and Operational Advisories just because its challenging for machine interpretation
- Large language models (LLMs), when used correctly, can be used to interpret these advisories and contribute these interpretations to overall detection engineering. We covered through 3 examples of such applications.

Thank you!

Contact

Ray Huang

https://www.linkedin.com/in/raymond-huang-8661b412/