Threat Hunting Using SIEM and MITRE Mapping

Group 7 Members and Roles

- Damien Rodziewicz-**INT250041**
  Role(s): Team Lead, Analyst Lead, Research Team, Presentation Lead
  Activities: Group Leader, SIEM Setup, Attack Simulation, Dashboard Creation, Presentation
- Melisa Nyamukondiwa-**INT250022**
  Role(s): Report Writer, Analyst, Research Team, GitHub Lead
  Activities: Report Writing, Dashboard Creation, GitHub Posting
- Sunday Dorcas Idorenyin **- INT250363**
  Role(s): Analyst, Research Team
  Activities: Dashboard Creation, MITRE Mapping and Mitigations
- Onah Nelson-OCHELLE **- INT250427**
  Role(s): Analyst, Research Team
  Activities: (MITRE Mapping, Mitigations and Lessons Learned
- Onyekachi Jude Nwizu**- INT250501**
  Role(s): Analyst, Research Team
  Activities: (Research

Contents

Threat Hunting Using SIEM and MITRE Mapping 1

Group 7 Members and Roles 1

Objectives 3

Tools Used 3

Configurations 3

Windows 10 Virtual Machine 3

Sysmon 3

APTSimulator 5

Splunk 5

Simulation 6

ATTACK Simulation 6

SOC Dashboard Creation and Data Analysis 7

Data Aggregation In Splunk 7

Dashboard Creation 8

MITRE ATT&CK Mapping 9

Key Findings 10

Mitigations 10

Lessons Learned 10

Conclusion 10

Objectives

Simulate attack using APT simulator, collect and aggregate data sources in Splunk in order to build a SOC dashboard. Analyze anomality in logs and map TTPs to MITRE ATT&CK. Propose remediations for observed attacks.

Tools Used

- **Windows 10 Virtual Machine**
  Controlled environment to simulate an attack against and collect logs from.
- **Apt Simulator**
  Safe Tool used to simulate attacks against systems without damaging the system.
- **Sysmon**
  Monitors windows system activity
- **Event Viewer**
  Windows program which tracks events from multiple sources and classifies them according to an event ID
- **Splunk**
  Platform to analyze logs collected during attack and build a dashboard

  In addition**: MITRE ATT&CK Framework** was utilized to map out threats and techniques used in the attack according to the event codes.

Configurations

Windows 10 Virtual Machine

- Although APTSimulator does not actually damage a system, the attack was conducted in a safe environment for increased security.
- A Windows 10 iso was downloaded from the official Windows website.
- A virtual machine was created in VirtualBox and configured to look like a real Windows System
- A snapshot was taken of the system before the attack commenced, so it would be possible to roll back to a clean install.

Sysmon

- Zip package containing program downloaded from https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
- Configuration file downloaded from https://github.com/SwiftOnSecurity/sysmon-config and renamed configuration file to sysmonconfig.xml
- Installed Sysmon by using command: `sysmon64.exe -accepteula -i sysmonconfig.xml`

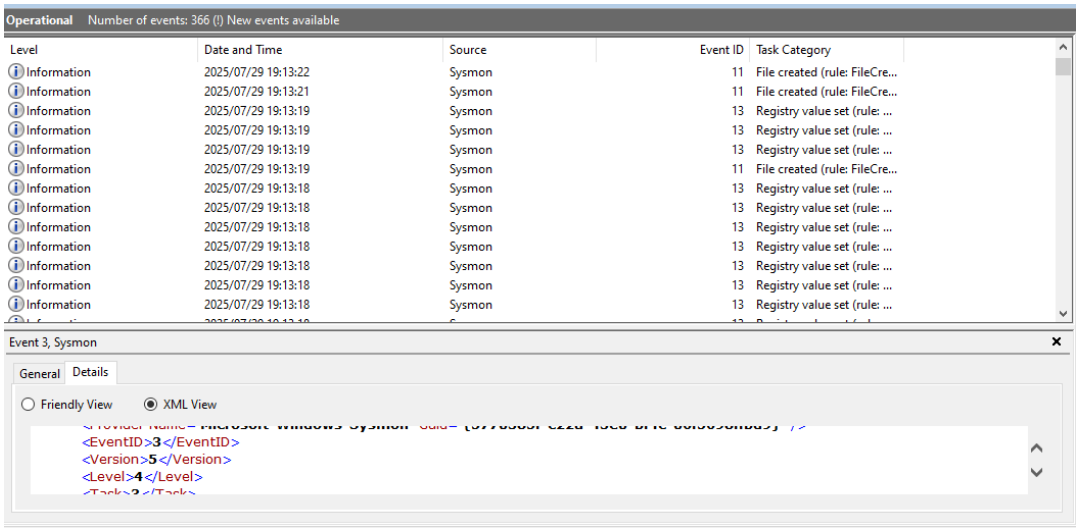
```
C:\Users\melis\Downloads>cd Sysmon

C:\Users\melis\Downloads\Sysmon>sysmon.exe -accepteula -i sysmonconfig.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon...
Sysmon started.
```

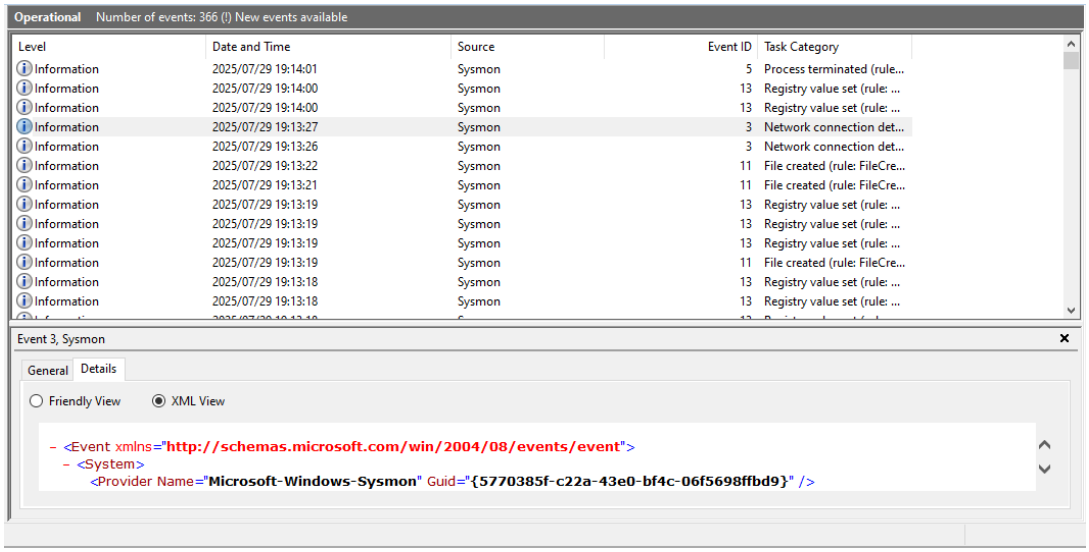
- Verification: In order to verify that Sysmon was working on the system, Windows Event Viewer was opened and navigated to the Sysmon logs through the path: **Event Viewer → Applications and Services Logs → Microsoft → Windows → Sysmon → Operational**



Then in command prompt, the command `ping www.google.com` was used to check if the Sysmon logs were being captured and it was confirmed that they were.

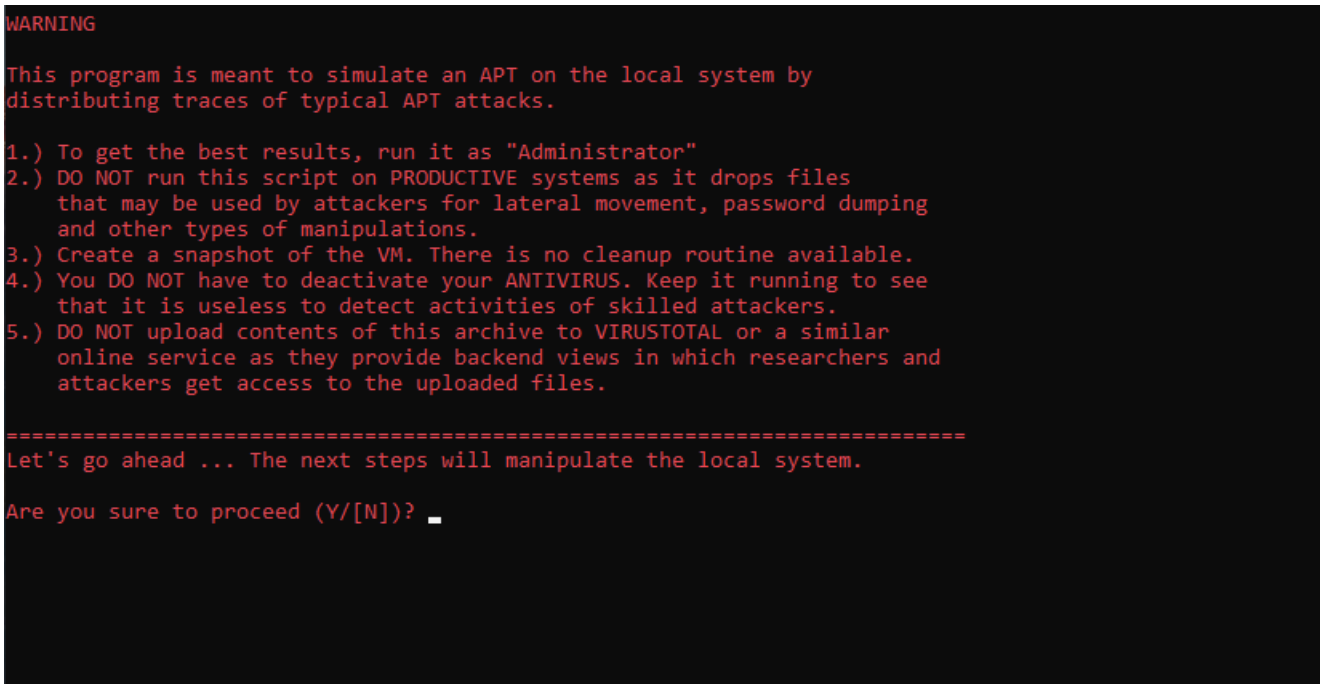
```
C:\Users\melis\Downloads\Sysmon>ping www.google.com

Pinging www.google.com [142.251.47.196] with 32 bytes of data:
Reply from 142.251.47.196: bytes=32 time=314ms TTL=255
Reply from 142.251.47.196: bytes=32 time=86ms TTL=255
Reply from 142.251.47.196: bytes=32 time=89ms TTL=255
Reply from 142.251.47.196: bytes=32 time=70ms TTL=255
```



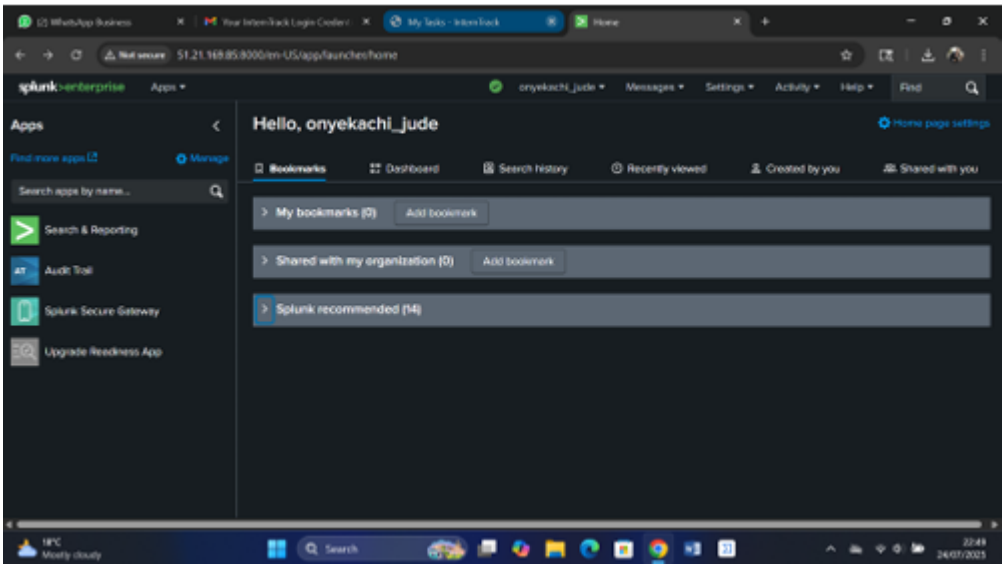
APTSimulator

- Apt simulator was downloaded from: https://github.com/NextronSystems/APTSimulator
- There was an executable named APTSimulator.bat in the zip containing the application. Opening it as administrator in the command prompt launched the application.



Splunk

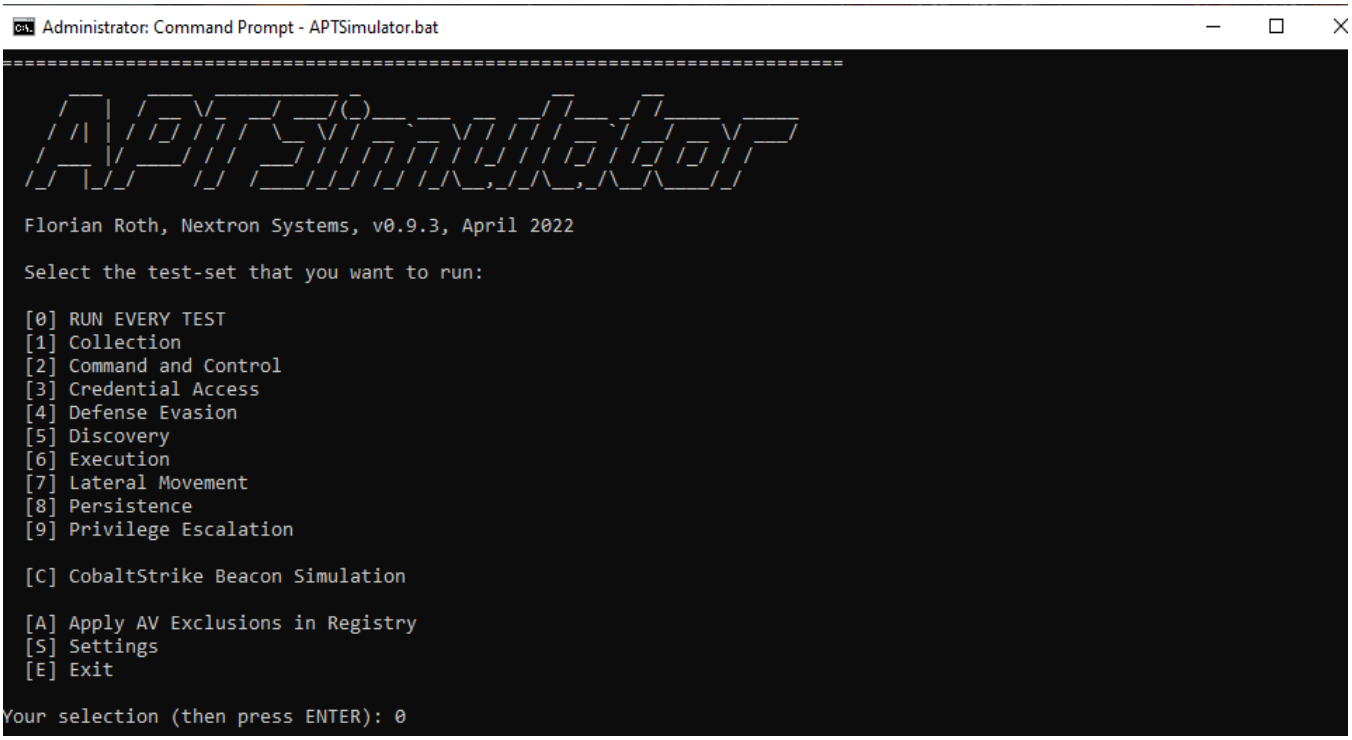
Splunk was chosen as the SIEM to analyze the logs. Splunk can be used as a tool to map observed Tactics, Techniques, and Procedures (TTPs) to the MITRE ATT&CK framework through several methods including: Splunk Enterprise Security (ES) and Security Essentials; Custom Correlation Searches and Annotations; Threat Intelligence Integration; MITRE ATT&CK App for the Splunk; Data Source Mapping. For the purpose of this project, it was used for data aggregation and dashboard creation. MITRE ATT&CK mapping was done manually using the logs and dashboards created in Splunk.



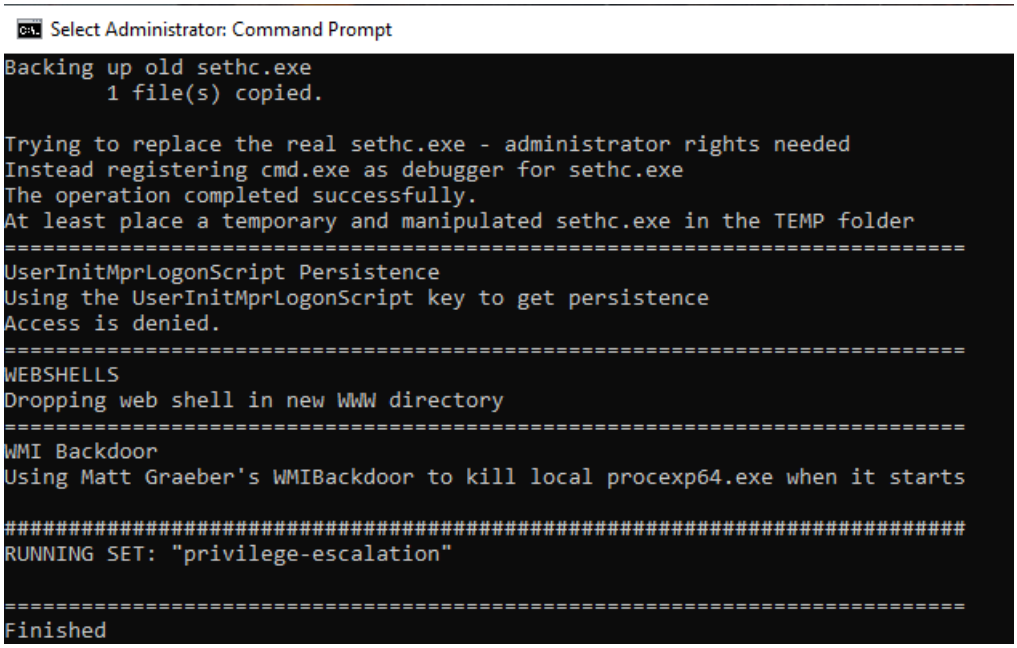
Simulation

ATTACK Simulation

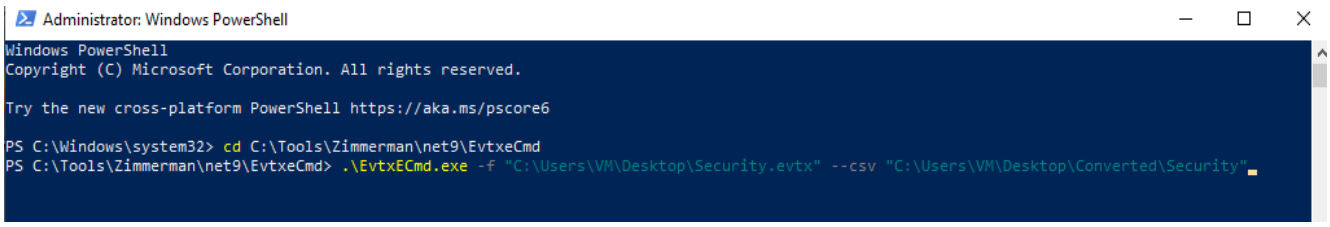
- Once all the tools and configurations were set up, the attack was conducted.
  All the tests were run by selecting Option 0 (RUN EVERY TEST)



This began the simulation and every attack was attempted.



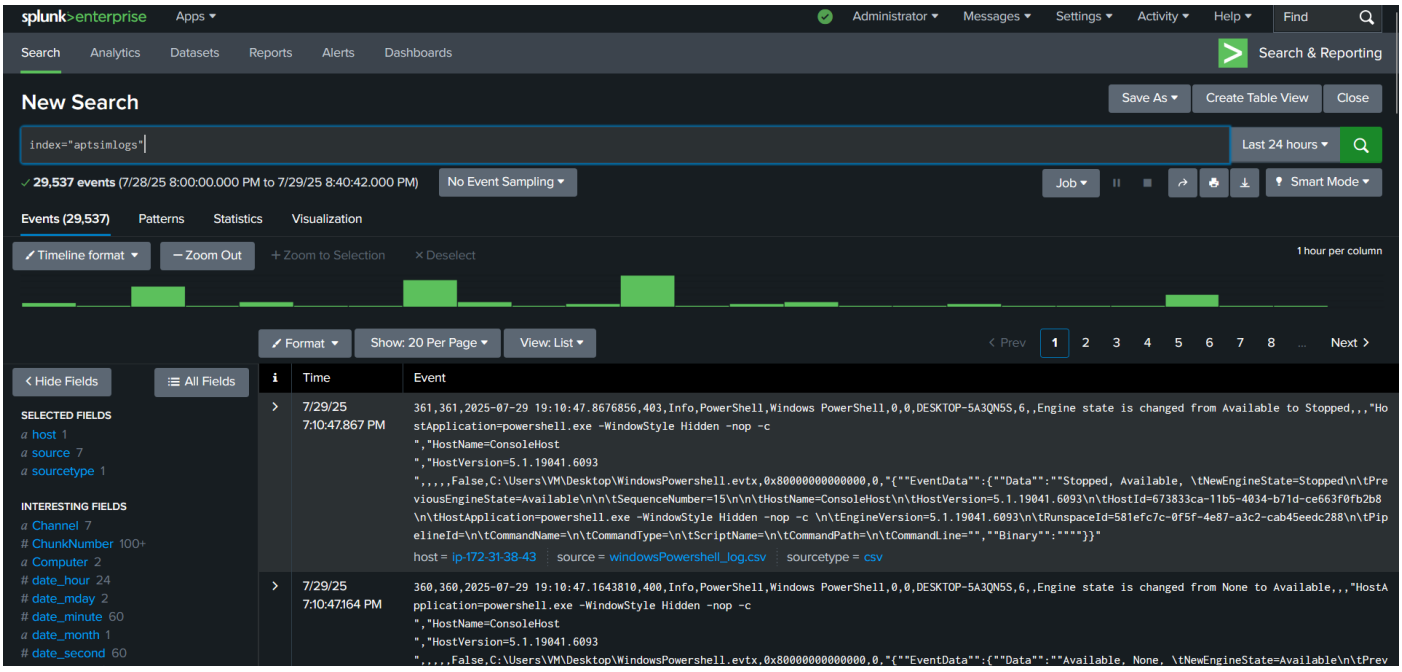
Once all the attacks were conducted, the event viewer logs were converted to csv in order to be compatible with Splunk. This was the command used for every log. The logs converted were from the following sources: Application, Firewall, Security, Sysmon, System, Windows Defender and Windows PowerShell.



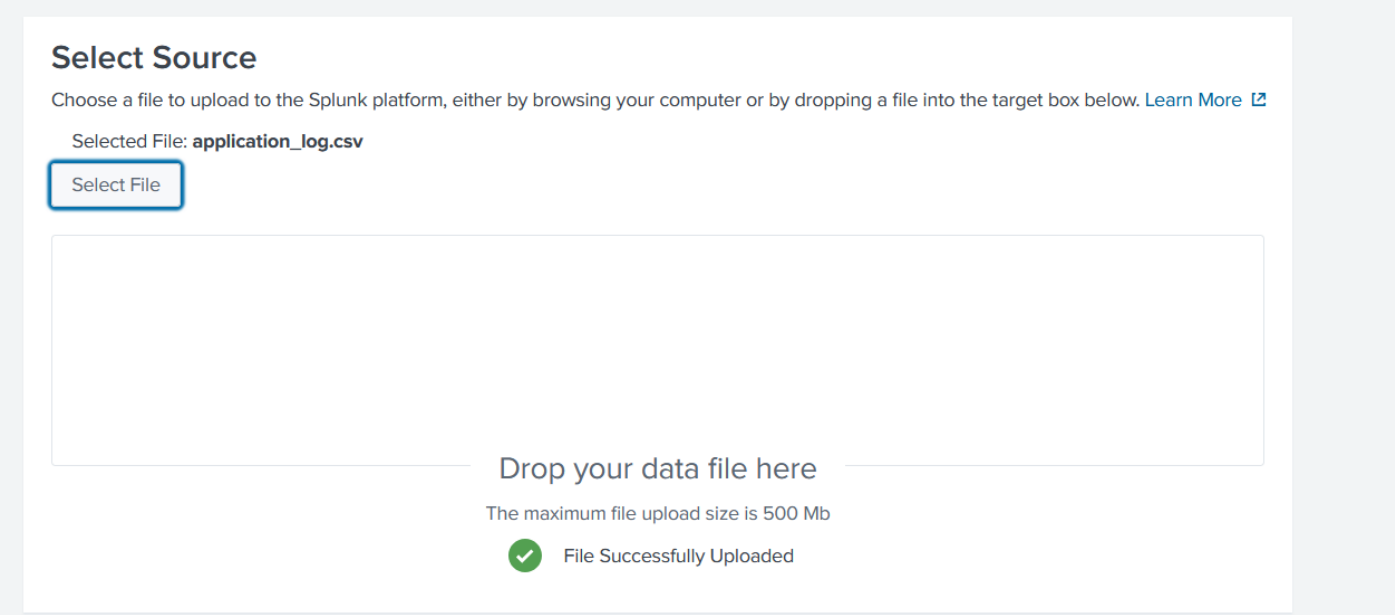
SOC Dashboard Creation and Data Analysis

Data Aggregation In Splunk

Once all the logs were converted to csv, they were uploaded to spunk under the index aptsimlogs:

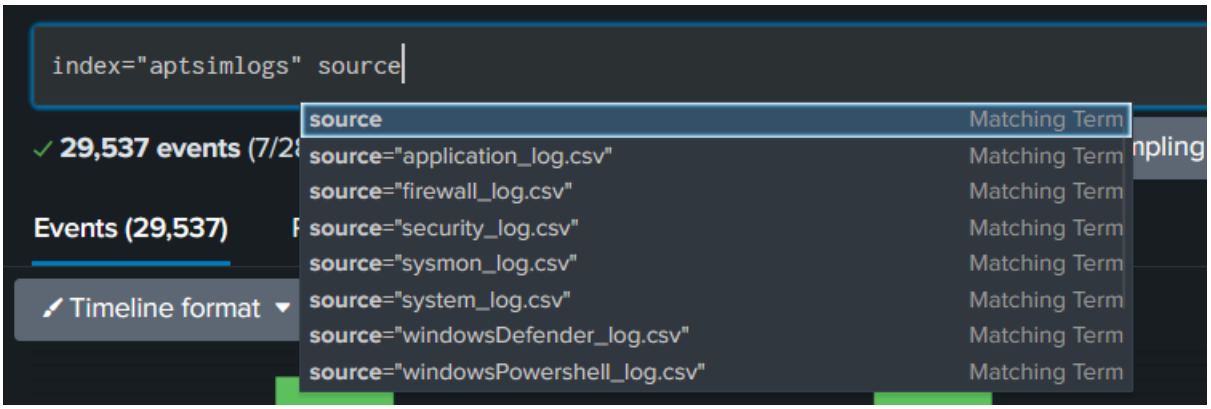


Each individual csv log was uploaded under the mentioned index.



The same was done for the rest and once done all data sources could be viewed using the query:

`Index=”aptsimlogs” source=`



Dashboard Creation

A dashboard for the privilege escalation attack was created. The multiple stages of the attack were separated into panels determined by the EventIDs.

Panel 1: Privileged Logons (Event ID 4672)

Purpose: See when users receive special privileges (e.g., SeDebugPrivilege, SeTakeOwnershipPrivilege).

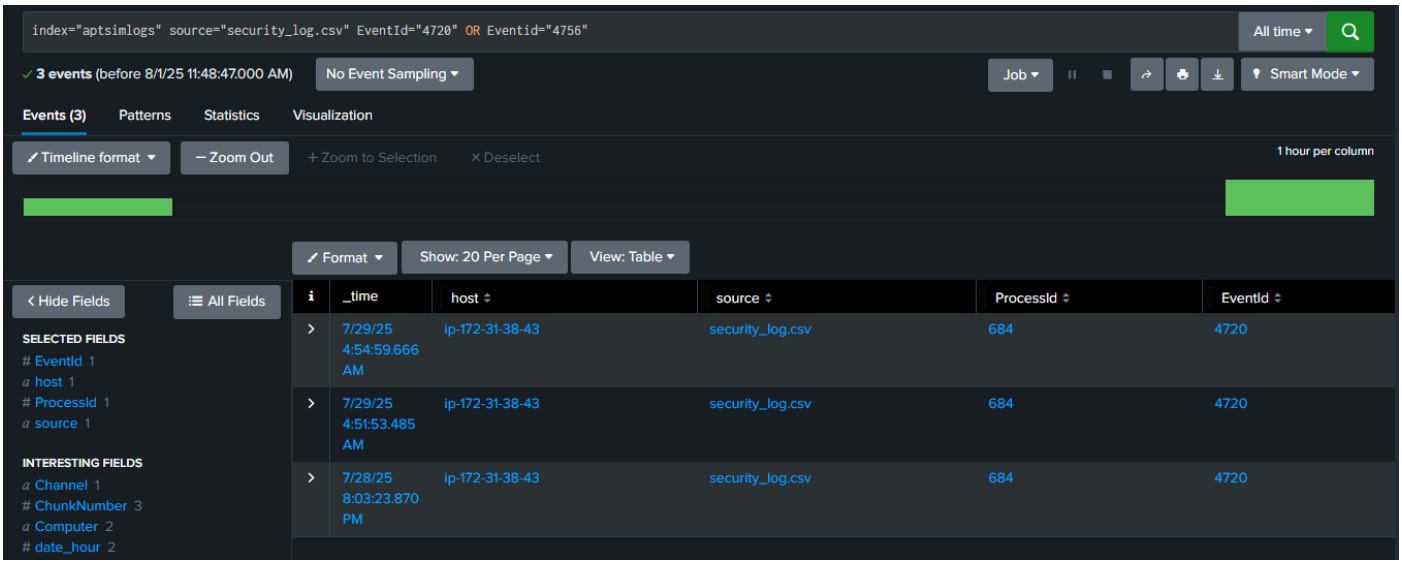
Query used : `index=”aptsimlogs” source=”security_log.csv” Eventid=“4672”`

Afterward the logs were added to a panel named: **Privileged Log-Ons**

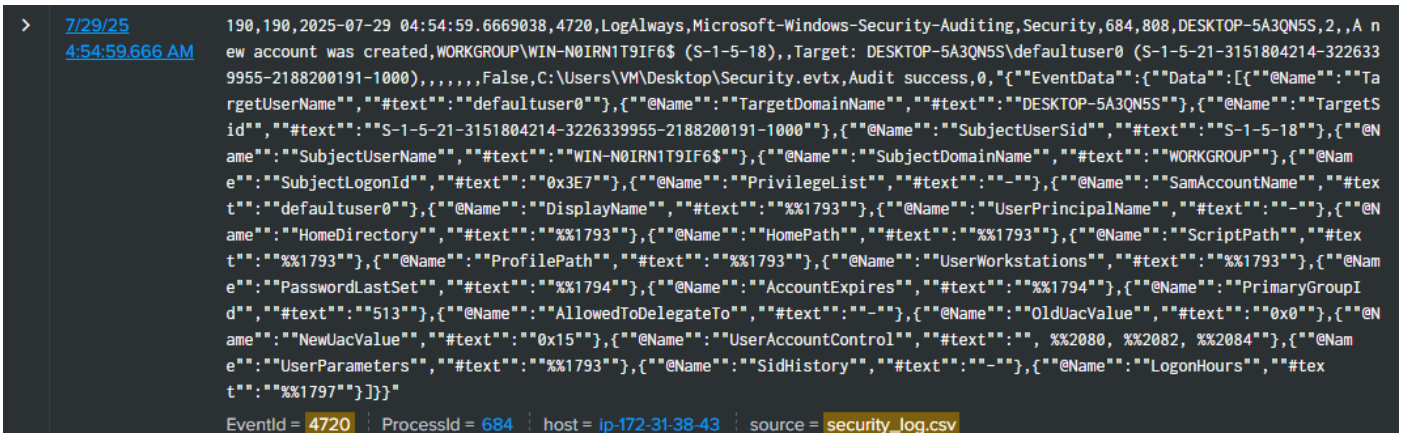
Panel 2: New User Creation (4720) and Group Addition (4732 / 4756)

Purpose: Detect new users and privilege group memberships (Admins, Domain Admins).

Query used: `index=”aptsimlogs” source=”security_log.csv” Eventid=“4720” OR Eventid= “4756”`



This was added to the panel: **New User Creation and Group Addition.** Closer Inspection showed this as the contents of the event:



Panel 3: High-Risk Command Execution (4688)

Purpose: Track suspicious processes like PowerShell, cmd.exe, or Mimikatz being spawned.

A panel was created for this event ID as shown above.

Panel 4: New Services Installed (7045 & 4697)

Purpose: Services can be used to gain SYSTEM-level access.

A panel was created for this event ID as shown above.

MITRE ATT&CK Mapping

The data and dashboards created in Splunk were then used to map the privilege escalation attack conducted using APTSimulator.

Source	Event ID	Tactic	Technique ID	Technique Name	Procedure
security_log.csv	4624	Initial access	T1078.001	Valid Accounts: Default Accounts	A successful logon occurred using a default account.
security_log.csv	4648	Privilege Escalation	T1134.002	Access Token Manipulation: Create Process with Token	Shows an attempt to log on using explicit credentials.
security_log.csv	4672	Access Token Manipulation	T1134.002	Access Token Manipulation: Create Process with Token	A user was assigned privileges at log. Potential token impersonation.
security_log.csv	5379	Credential Access	T1555.004	Credentials from Password Stores: Windows Credential Manager	Credential Manager credentials were accessed.
security_log.csv	4798	Defense Evasion	T1564.002	Hide Artifacts: Hidden Users	Local group memberships were enumerated.
security_log.csv	4720	Create Account	T1136.001	Create Account: Local Account	A new local user account was created on the system.
security_log.csv	4732	Create Account	T1136.001	Create Account: Local Account	A user account was added to a security-enabled local group
security_log.csv	4688	Access Token Manipulation	T1134.001	Token Impersonation/Theft	An attempted to register a security privilege by user or process
system_log.csv	7045	Task/Job	T1053.005	Scheduled Task/Job: Scheduled Task	A new service created via PowerShell to run code.

Key Findings

- **Privilege Escalation (TA0004, T1037.001):** Logon scripts were manipulated to automate unauthorized system access, demonstrating persistence techniques.
- **Credential Access (TA0006, T1555.004):** Attackers extracted credentials from Windows Credential Manager, highlighting vulnerabilities in credential storage.

Mitigations

- **For privilege escalation:** incorporate tough authentication (use strong passwords and multi factor authentication), conduct regular updates, educate users and use different strategies of least privilege control to combat privilege escalation.
- **Credential access:** ensure logs are monitored and audited regularly, enforce the use of strong password policies, limit access to credential storage and implement multi-factor authentication (MFA). Train users on phishing and password security to reduce threat.
- **Enhance Logging:** Enable and validate all critical logs (Security, Windows Defender, etc.).
- **Continuous Training:** Regular MITRE ATT&CK training and simulated attack drills for SOC teams.
- **Automate Threat Detection:** Implement Splunk alerts and playbooks for high-risk TTPs.
- **Strengthen Mitigations:** Enforce MFA, strict password policies, and monitor registry changes.

Lessons Learned

- **MITRE ATT&CK Mapping:** Essential for structured threat analysis and response prioritization.
- **Mitigation Strategies:** Strong passwords, MFA, and least privilege controls are critical.
- **Tooling and Configuration:** Proper Sysmon and Splunk setup is necessary for accurate threat hunting.
- **SOC Dashboard Utility:** Dashboards improve visibility but require complete log data for effectiveness.

Conclusion

This exercise demonstrated the power of combining SIEM tools with the MITRE ATT&CK framework for proactive threat hunting. In addition, it refined the ability to simulate cyberattacks in a controlled environment, collect evidence in the form of logs, use a SIEM tool to aggregate data, build dashboards and also map attacks using event IDs in the MITRE ATT&CK Framework. Lastly, it highlighted the

importance of security best practices such as strong passwords, proper SIEM setup and security training in order to hunt threats and observe their effects.