ALPHA 7 RESPONSE

 # Secure The Future With Alpha 7 Response

BIUE TEAM PLAYBOOK

Phishing | Data Exfiltration | Ransomware | Privilege Escalation

WWW.ALPHA7RESPONSE.COM

TABLE OF CONTENTS

INTRODUCTION

This playbook outlines the defensive actions taken by the Blue Team during a simulated cyberattack carried out by the Red Team, based on the MITRE ATT&CK framework. The goal of this exercise was to detect, investigate, and respond to a range of attack techniques, including malware execution, persistence via registry modification, reverse shell activity, and file encryption consistent with ransomware behaviour.
To defend against these threats, the Blue Team implemented a structured detection strategy using Splunk as the Security Information and Event Management (SIEM) platform. A Windows system was configured to log critical events such as process execution, registry changes, and file access, allowing the Blue Team to monitor malicious behaviour in real-time.

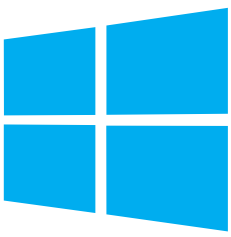
The simulated attack included:

- Execution of a malicious binary (VictimRansomware.exe)
- Registry key modification to establish persistence
- Potential reverse shell initiated via HTTP
- Encryption of user files in key folders like Documents and Downloads

This playbook documents the full defensive workflow, including:

- Deployment of monitoring infrastructure
- Configuration of Windows auditing policies
- Creation of MITRE-aligned Splunk alerts
- Investigation of attacker behaviour and system impact

Each detection step in this playbook is mapped to relevant MITRE ATT&CK techniques to ensure real-world relevance and a threat-informed defence approach.



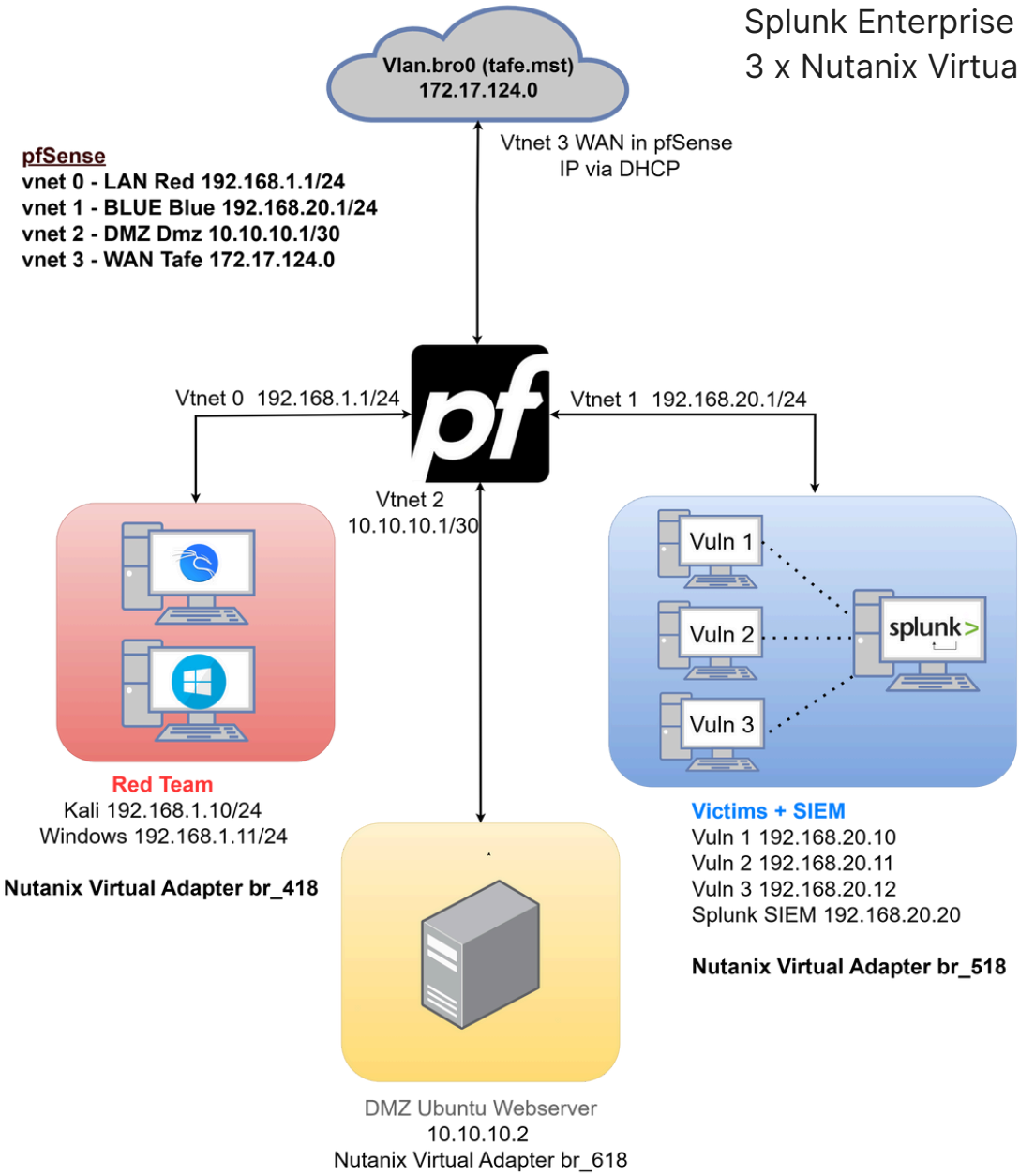
STEP 1: INFRASTRUCTURE AND SPLUNK SETUP

IP addressing and VM Roles

The Blue network is designed to simulate a typical exercise endpoint environment under defensive monitoring. It includes a Windows-based victim machine, which serves as the primary target of the attack, and another Windows-based machine configured as a Splunk SIEM server, responsible for collecting, storing, and analysing event logs.
These systems operate within the same virtual subnet, allowing seamless log forwarding via the Splunk Universal Forwarder installed on the victim machine.

IP addressing
Vuln 1 Windows 192.168.20.10
Vuln 2 Kali 192.168.20.11
Vuln 3 Ubuntu 192.168.20.12
Splunk SIEM Windows 192.168.20.13

Network Environment
4 x Virtual Machines
1 x Windows 10 PC Vuln 1
1 x Kali Vuln 2
1 x Ubuntu Vuln 3
1 x Windows 10 PC Splunk SIEM
Splunk Enterprise installed on Splunk SIEM
3 x Nutanix Virtual Network Connections



Installing Splunk Forwarder on the Victim Machine

1. Locate and run the Installer

The Splunk Universal Forwarder installer was already present in the Downloads folder on the Windows victim machine.
To begin installation:

- Double-click the installer file to launch the setup wizard.

2. Installation Configuration

During installation:

- Select Custom Options
- Set the installation directory to:
- C:\SplunkUniversalForwarder
- Skip the SSL certificate configuration step.
- Choose Local System as the account to run the forwarder.

In the next step, select:

- Application Logs
- Security Logs
- System Logs.

After we set the admin username and password, skip setting up the deployment server and set up the receiving Indexer with the IP address of the SIEM machine and with the port number 9997

3. Verify Forwarder Connection

- Open Command Prompt as Administrator

Navigate to the Splunk Forwarder's bin directory:
cd \SplunkUniversalForwarder/bin

Confirm it is Active
Splunk list forward-server -use the login credentials

To stop forwarding:
cd \SplunkUniversalForwarder/bin
Splunk.exe stop

Installing Splunk SIEM

1. Locate the Installer

The Splunk Enterprise installer was already downloaded to the Downloads folder on the Windows VM hosted in Nutanix.

2. Run the Installer

Double-click on the file to begin the installation process, follow the wizard and accept the license agreement. Select the default installation directory - C: \Spunk and set an admin username and password.
Open the Command Prompt:

Navigate to the Splunk directory:
cd c:\Program Files\Splunk

Verify that Splunk is running:
.\bin\splunk status

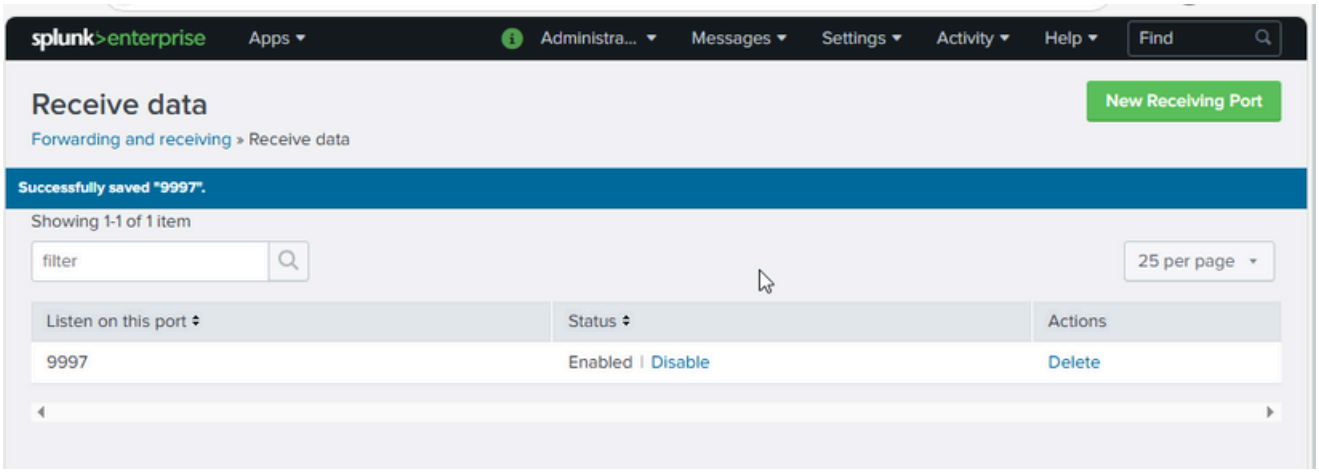
splunk start

3. Start Splunk Web Interface

After installation, the Splunk service will start automatically. Access the web interface by going to http://localhost:8000 and login with the admin credentials created in the previous steps.

4. Enable Data Input on Port 9997

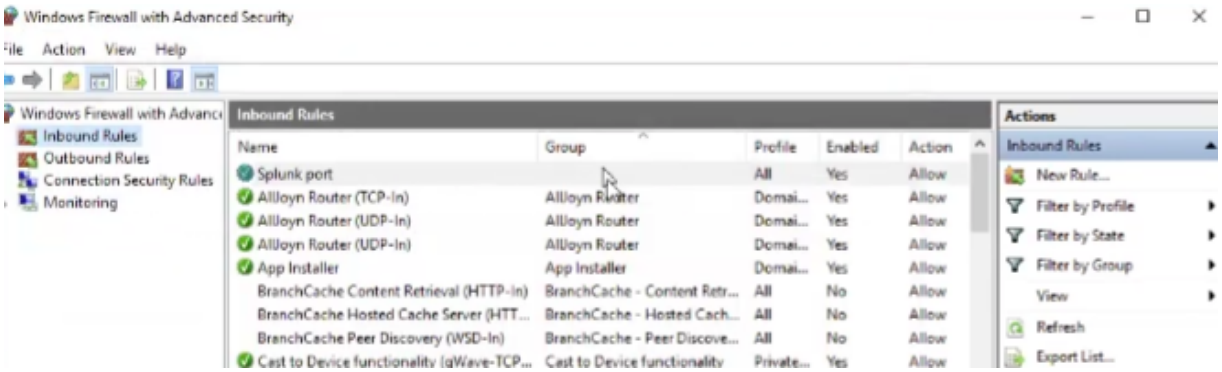
From the Splunk dashboard, go to:
Settings > Forwarding and receiving > Configure receiving
Click on New Receiving Port and enter 9997 as the port number and Save.



5. Enable port 9997 in firewall

To allow Splunk Forwarder to communicate with the Splunk SIEM over the network, port 9997 must be opened in the Windows Firewall on the Splunk SIEM machine.

- Open Windows Firewall Settings and click on Inbound Rules
- Add a New Rule, select Port and enter the specific port number 9997
- Name it as Splunk port and Save it



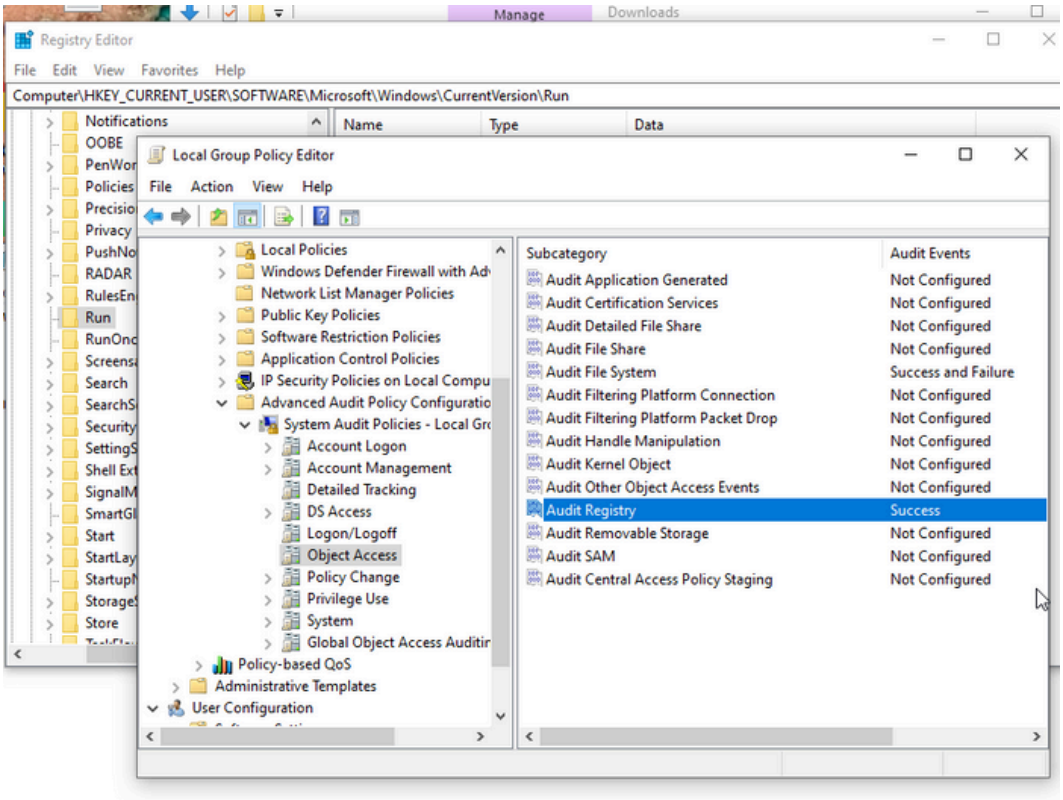
STEP 2: PREPARATION – AUDITING POLICIES CONFIGURATION

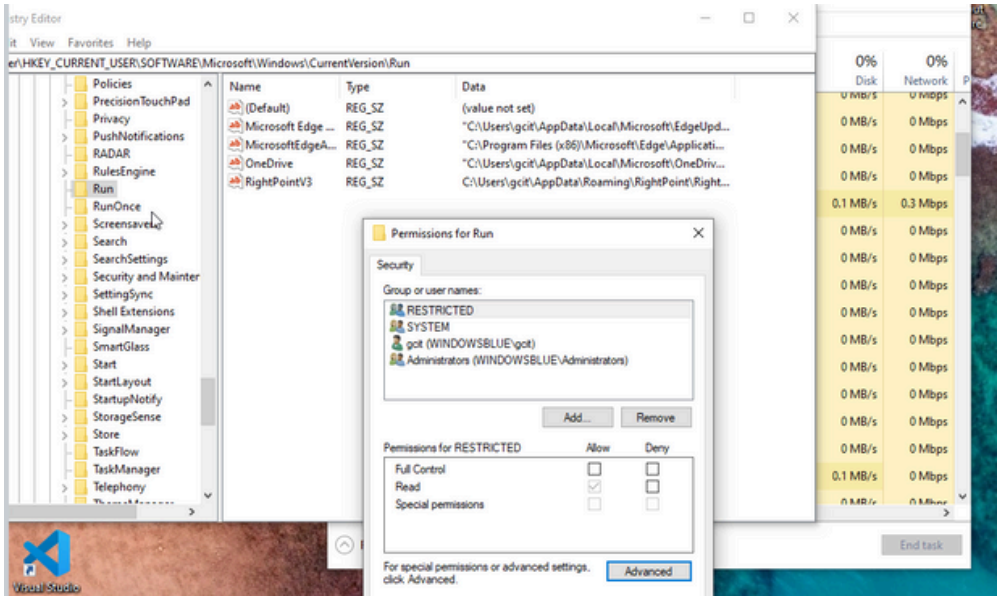
Before setting up Splunk alerts, Windows auditing policies were configured to ensure that critical system activities would be captured and available for analysis. Most configurations were applied using the Local Security Policy Editor under Advanced Audit Policy Configuration, which enabled logging for key events such as registry changes, file access, and process creation. In addition, auditing for Filtering Platform Connection was enabled using PowerShell to monitor network-level activity, allowing detection of suspicious outbound connections often associated with reverse shells or data exfiltration.

- **Audit Registry**

Audit Registry is a Windows security settings policy that logs any changes made to the Windows registry. This is a key visibility control for detecting the persistence mechanism used by attackers.
Once this setting is enabled and auditing is configured on specific registry keys (e.g., via regedit), Windows begins generating Event ID 4657 in the Security Event Log. This event indicates that a registry value was created, modified or deleted, which is critical for detecting persistence techniques used by attackers.
To manually set it up, use the Windows Registry Editor (regedit), navigate to:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run





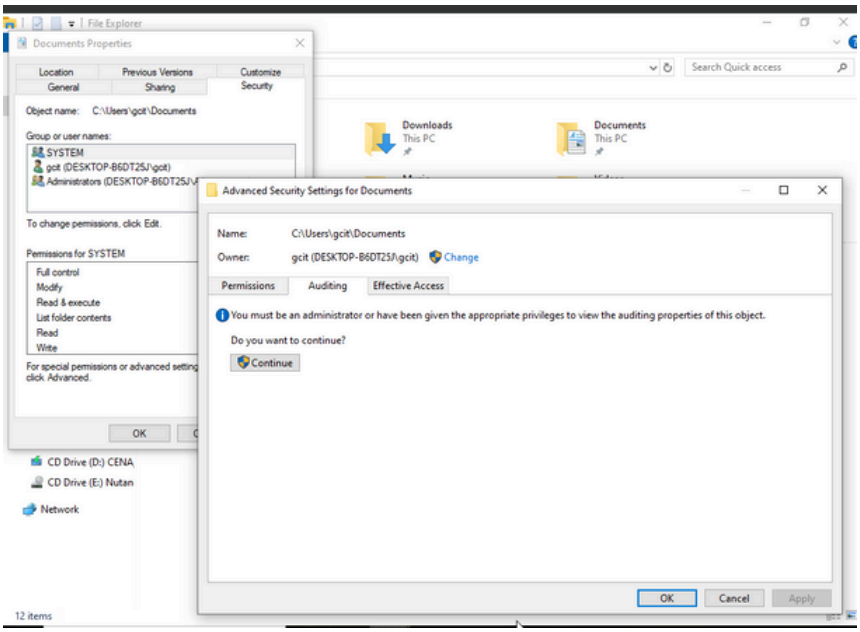
Rght-click the Run key and select Permissions → Advanced → Auditing. Add the principal 'Everyone' and select permissions such as 'Set Value', 'Create Subkey', and 'Delete'. This ensured that any changes to the key (such as malware adding an autorun entry) would trigger Event ID 4657 and be recorded in the Security log.

- **Audit Object Access**

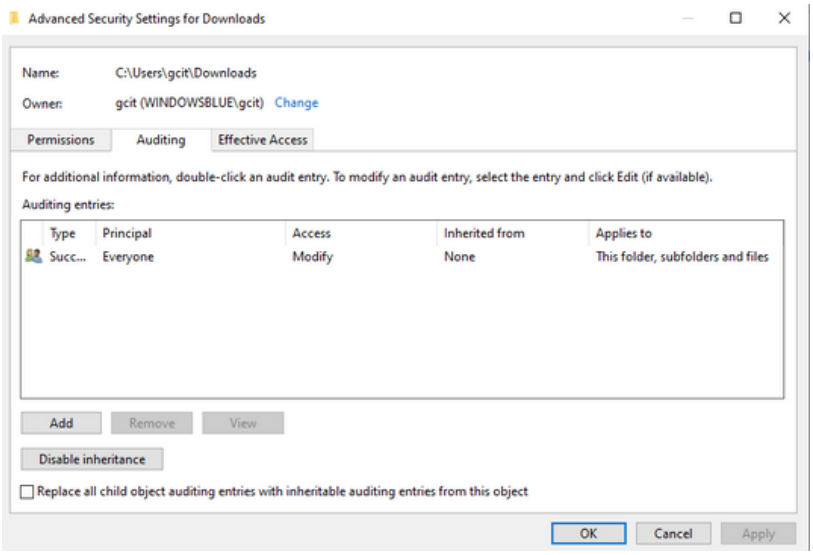
Audit Object Access is another Windows security policy that enables logging of interactions with file system objects, such as reading, writing, or deleting files and folders. This type of auditing is critical for detecting unauthorised access or modification of sensitive data, including ransomware behaviours or data exfiltration attempts.

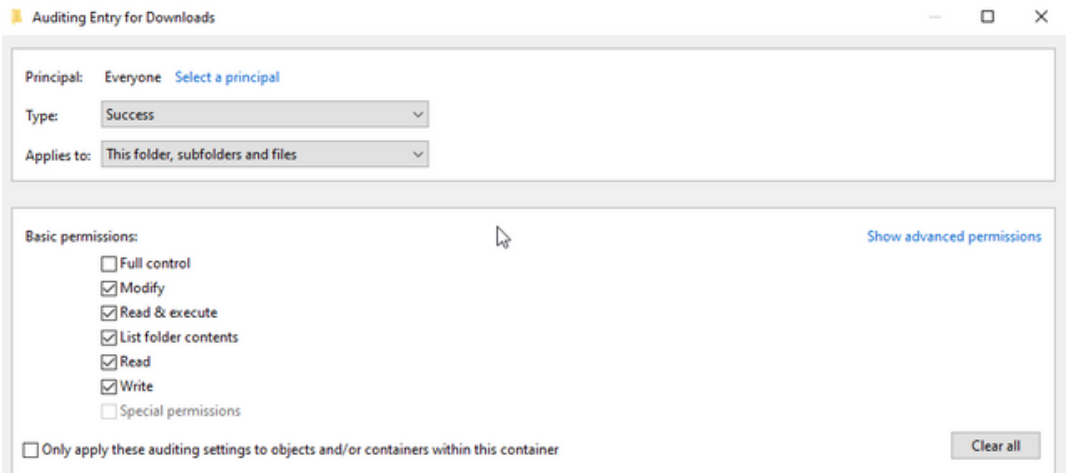
Using PowerShell Commad:
auditpol /set /category:"Object Access" /subcategory:"File System" /success:enable

This configured Windows to begin logging successful access events for files and folders that have auditing enabled. After this, manually navigate to the Downloads and Documents folders and configured auditing settings through Windows Explorer:



Right Click on each folder - Properties - Security - Advanced - Auditing



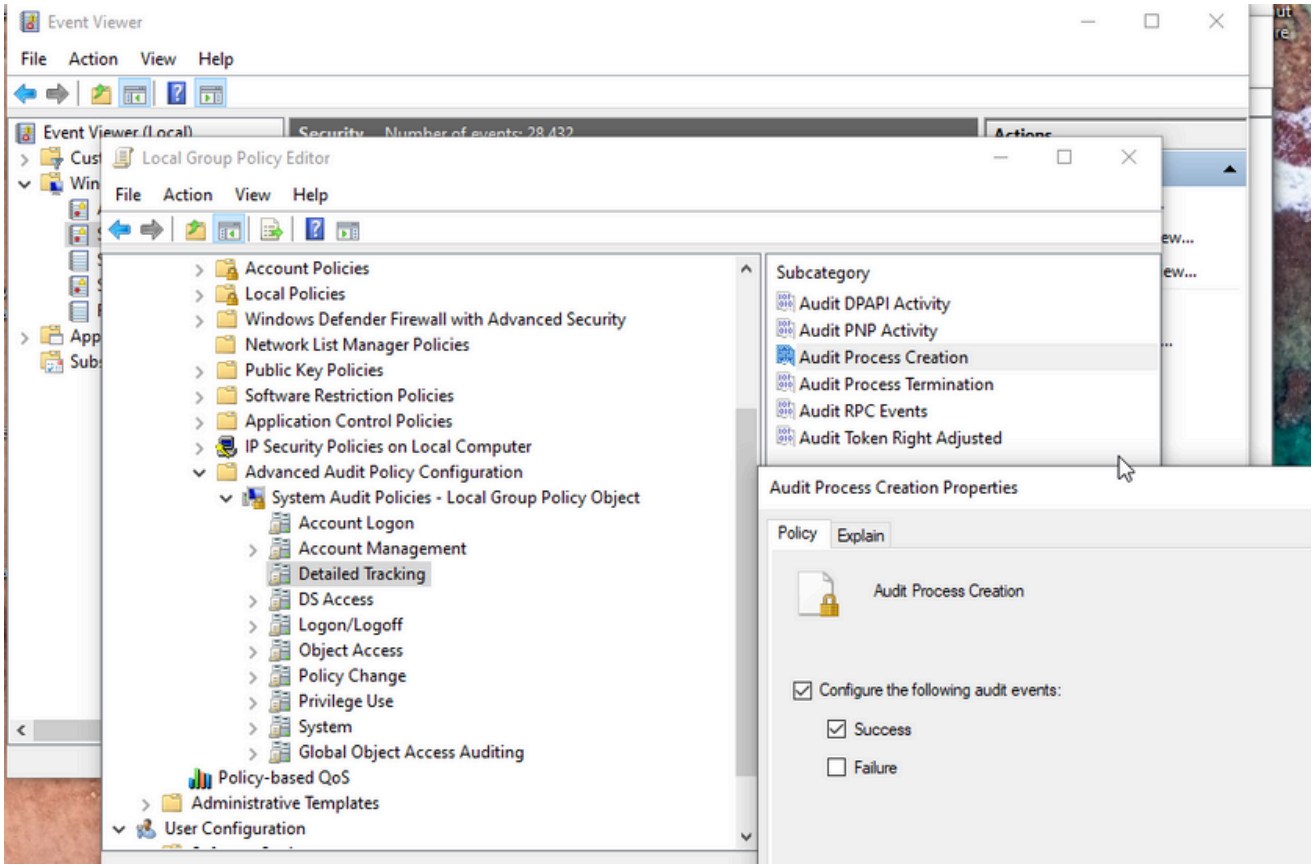


Added the Everyone group with permissions like Write, Create files, and Delete

This setup will generate Event ID 4663 whenever files in those directories were accessed or modified. These logs will later be forwarded to Splunk to help detect suspicious file access patterns, including those linked to ransomware activity.

- **Audit Process Creation**

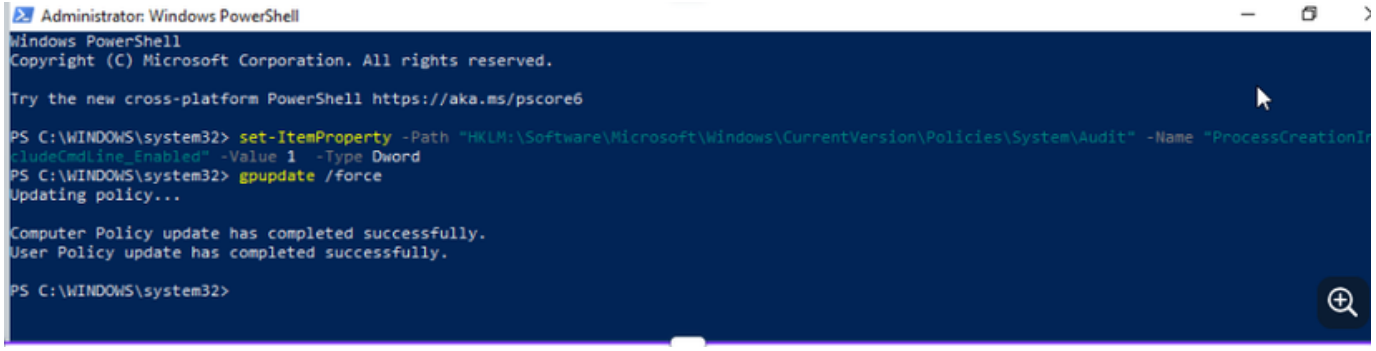
This will detect suspicious program execution, such as reverse shell or ransomware binaries. it will log if a new process starts on the system and helps identify potentially malicious behaviour.



Once this is configured, Windows will began generating Event ID 4688 which includes:

- The name of the executable that was run
- The command-line arguments (if additional logging is enabled)
- The user account that launched the process

To capture full command-line details for each process execution event, a registry setting can be modified also using PowerShell. This enables the inclusion of the ProcessCommnadLine field in Event ID 4688, allowing visability into the exact commands executed.



- **Filtering Platform Connection**

To monitor network activity associated with process behavior, auditing for Filtering Platform Connection was enabled. This setting logs Event ID 5156, which indicates that the Windows Filtering Platform has permitted a connection. It provides visibility into outbound or inbound connections initiated by executables — such as reverse shells, downloaders, or malware communicating with a command-and-control server.

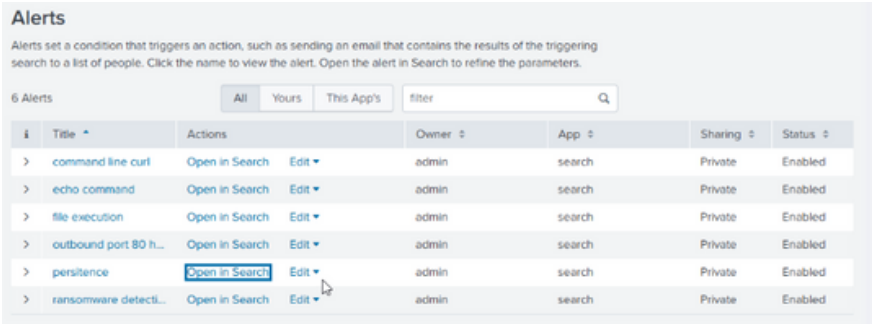
```
Use AuditPol <command> /? for details on each command
PS C:\WINDOWS\system32> AuditPol /set /subcategory:"Filtering Platform Connection" /success:enable
The command was successfully executed.
PS C:\WINDOWS\system32> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\WINDOWS\system32>
```

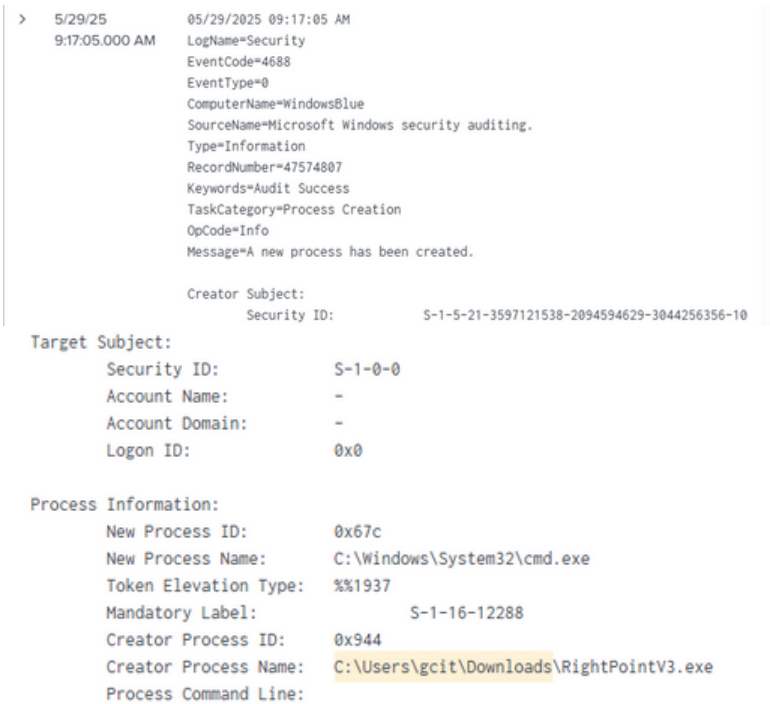
STEP 3: DETECTION: CONFIGURING SPLUNK ALERTS

With Windows auditing enabled and log forwarding in place, the next step involves configuring Splunk Alerts to detect suspicious behaviour used by the Red Team during the simulated attack. These alerts focus on key MITRE ATT&CK techniques such as process execution, registry persistence, and file system modification.
This step is critical for early detection and response, particularly when monitoring attacker behaviours aligned with MITRE ATT&CK tactics such as execution, persistence, defence evasion, and command and control.



Malicious File Execution

MITRE Technique: T1204.002: User Execution (Malicious File)
Event ID 4688 - A new process has been created
Red Team Action: The Red team manually executed RightjPointV3.exe from the Downloads folder
index=main EventCode=4688 “C:\\Users\\gcit\\Downloads”

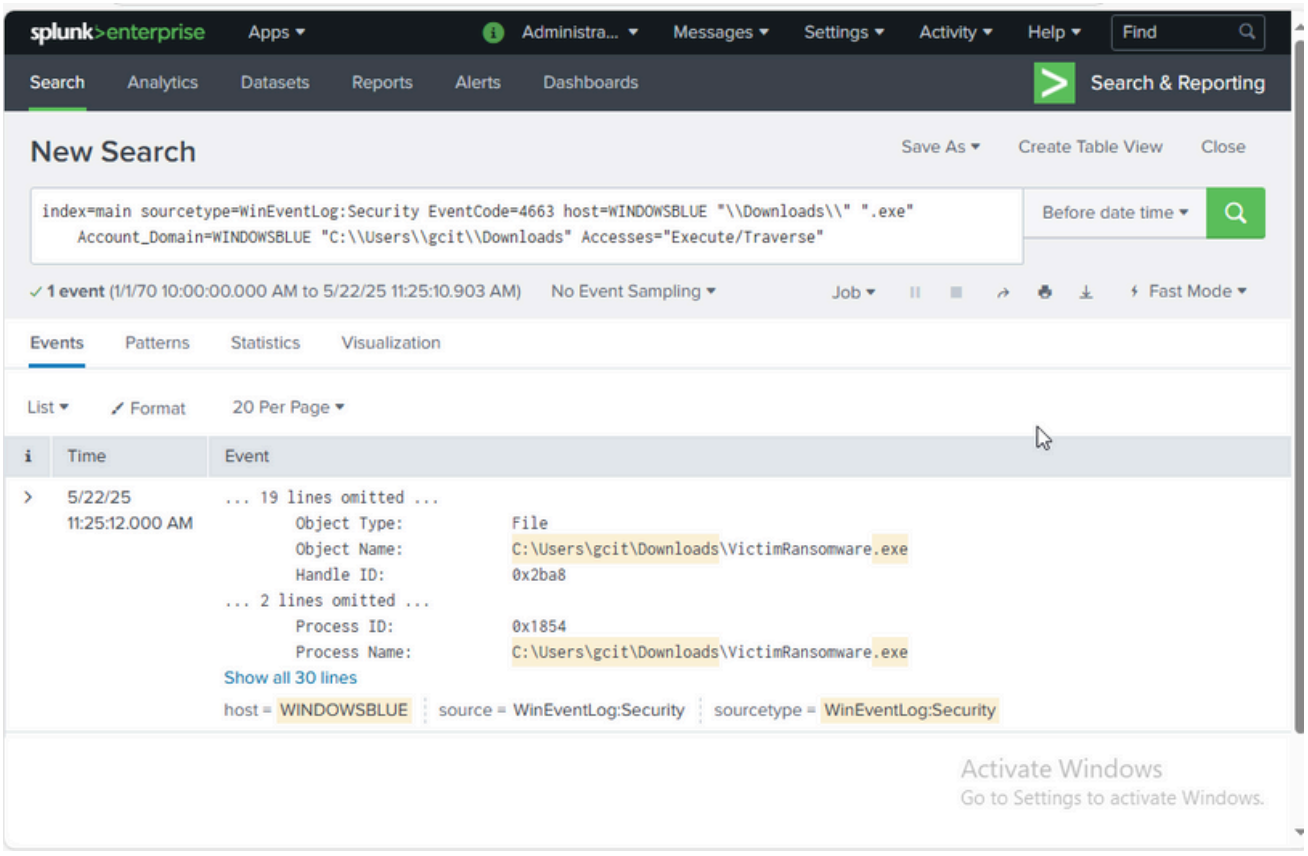


Ransomware Execution via File Access

MITRE Technique: T1059.003 - Command and Scripting Interpreter: Windows Command Shell
Event ID 4663 - File Access
Red Team Action: The Red Team manually executed VictimRansomware.exe from the Downloads folder. Upon execution, the ransomware accessed and encrypted multiple files on the victim system.

The Red Team were able to execute the file remotely via the reverse shell.

index=main sourcetype=WinEventLog:Security EventCode=4663 host=WINDOWSBLUE “\\Downloads\\“ “.exe.”



Registry Persistence Detection

MITRE Technique: T1547.001 - Registry Run Keys / Startup Folder

Event ID 4657 – Registry Value Modified

Red Team Action: Red Team created a registry Run key to maintain persistence. The key was added under HKCU\Software\Microsoft\Windows\CurrentVersion\Run and set to launch RightPointV3.exe automatically on user logon.

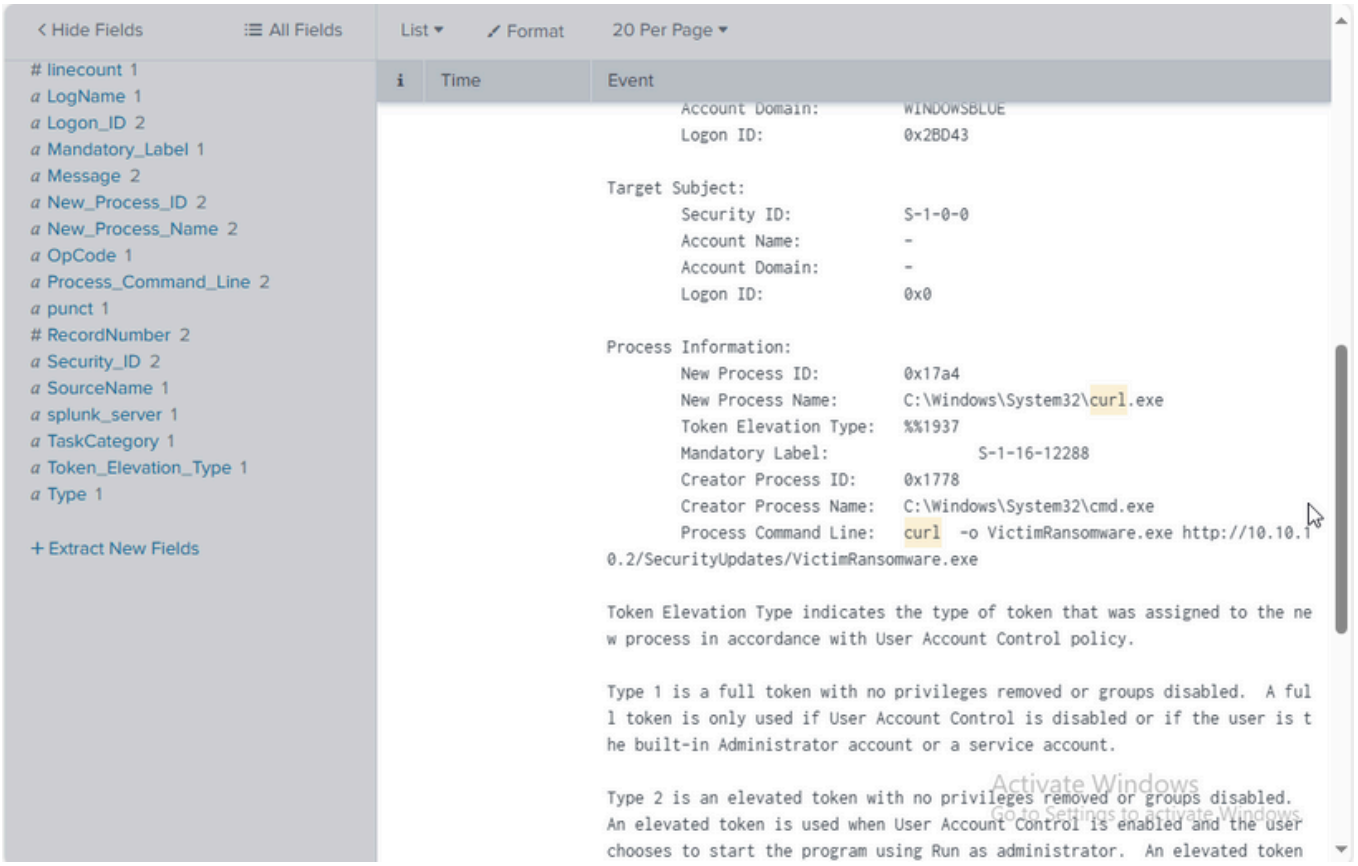
index=main EventCode=4657

Command-Line C2 Tool Usage

MITRE Technique: T1105 – Ingress Tool Transfer
Event ID 4688 – Process Creation
Red Team Action: The Red Team used curl.exe to download the ransomware payload (VictimRansomware.exe) from an external server (10.10.10.2).

This activity was recorded as Event ID 4688, which logs when a new program runs. In this case, cmd.exe launched curl.exe to connect to the attacker's server and download a file.

index=main EventCode=4688
|search New_Process_Name="curl.exe"

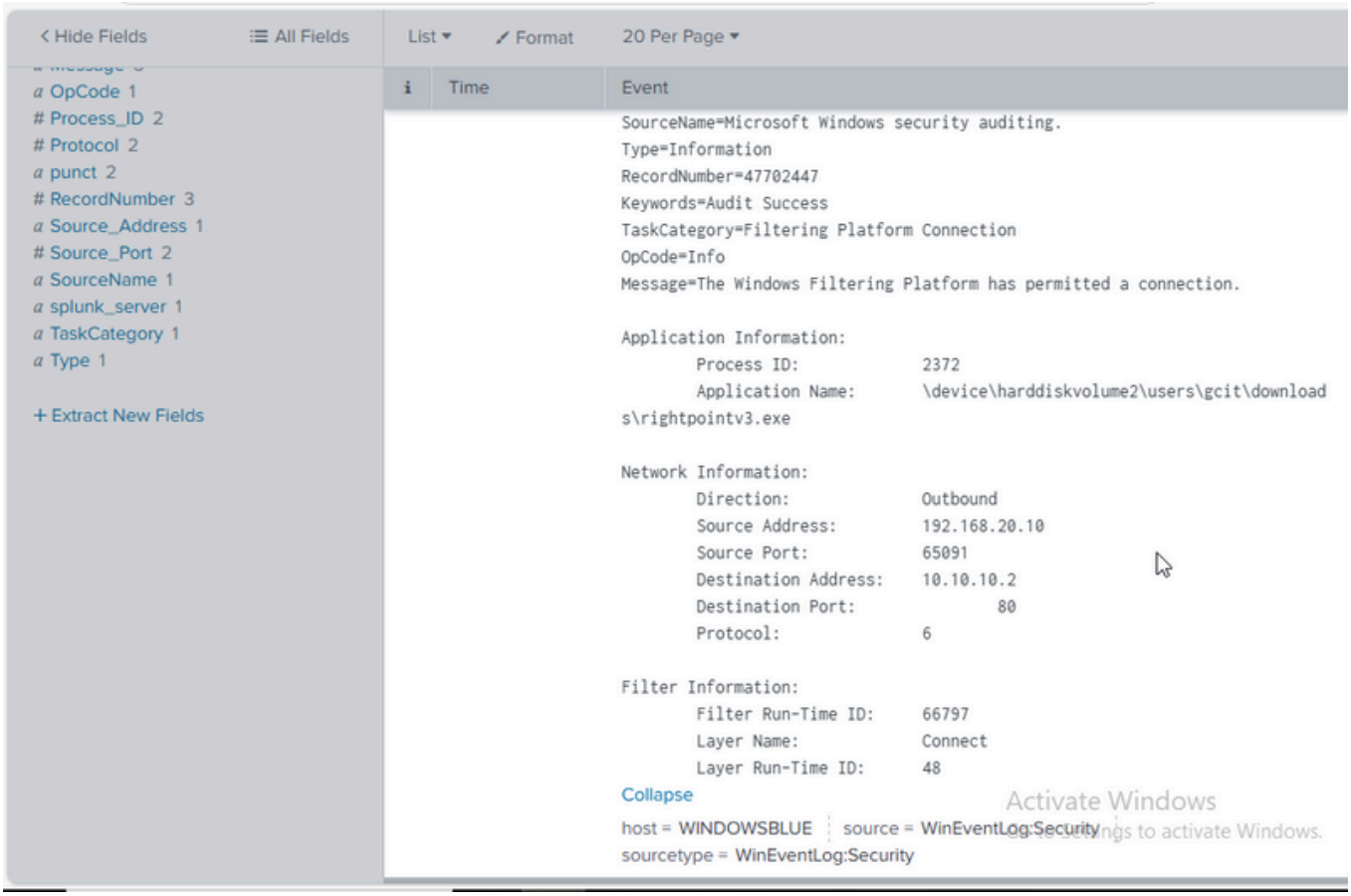


Outbound HTTP Communication (C2 Over Port 80)

MITRE Technique: T1071.001 – Application Layer Protocol: Web Protocols
Event ID 5156 – Network Connection Allowed
Red Team Action: Red Team simulated a reverse shell connection from the victim machine using HTTP over port 80 to a command-and-control (C2) server at 10.10.10.2. The payload (RightPointV3.exe) was responsible for establishing this communication.

This alert detects outbound HTTP traffic from endpoints to external IP addresses over port 80 — a known channel often leveraged for command-and-control (C2) communication. In modern enterprise environments, this type of outbound HTTP traffic is atypical for standard user behaviour and is generally treated as suspicious or indicative of potential malicious activity.

index=main EventCode=5156



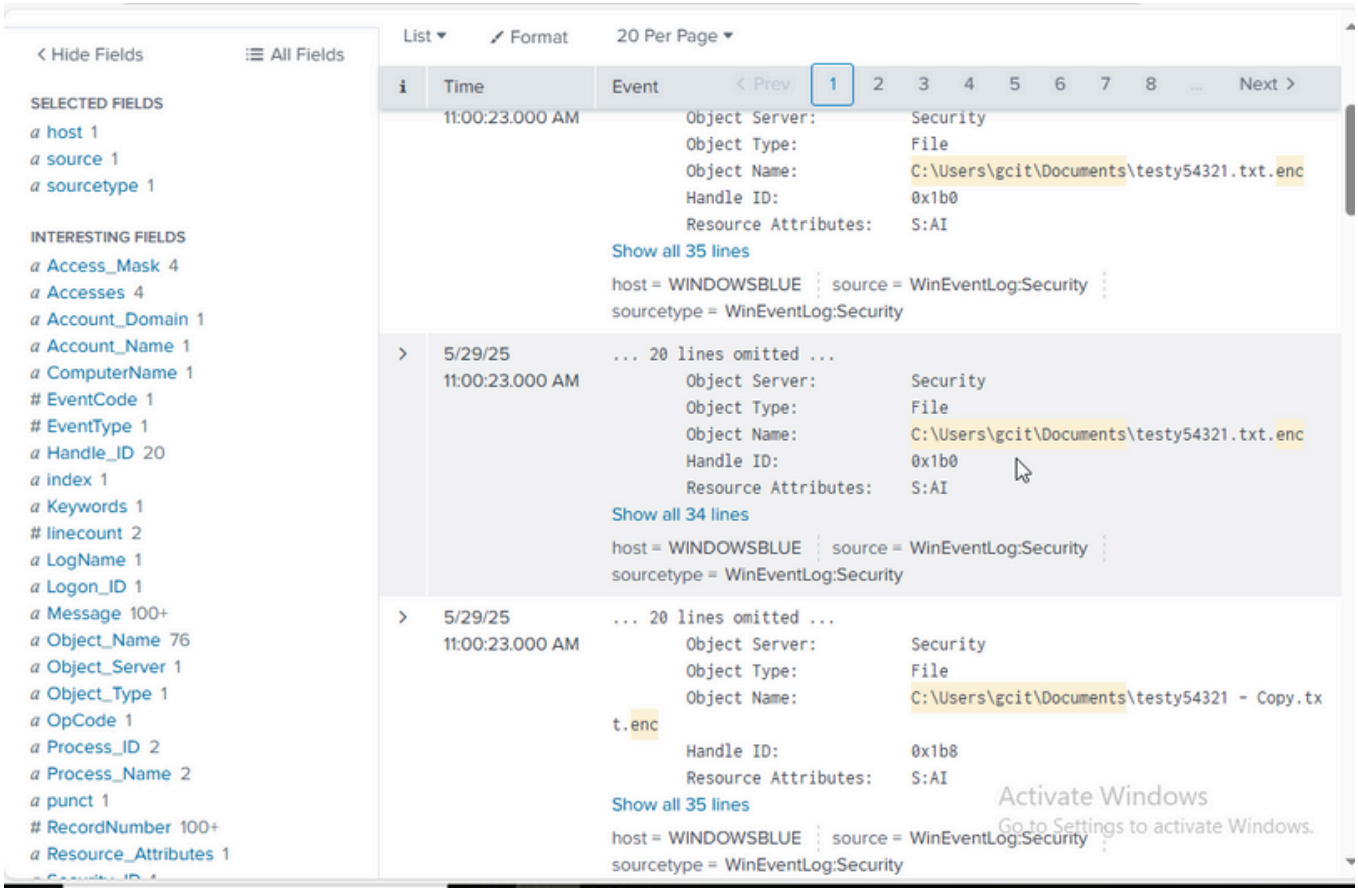
File Encryption Detected (Ransomware Impact)

MITRE Technique: T1486 – Data Encrypted for Impact

Event ID 4663 – File Access

Red Team Action: Red Team ran VictimRansomware.exe, which encrypted user files in the Documents folder. This resulted in file extensions changing to .enc.

index=main EventCode=4663 C:\\Users\gcit\Documents enc



STEP 4: CONTAINMENT ERADICATION & RECOVERY

Following the detection of the Red Team's activity, this phase focuses on stopping malicious activity, removing attackers' presence, and restoring affected systems. Prompt action is essential to minimise damage and prevent further compromise.
The following actions address MITRE ATT&ACK techniques:

- T1204.002 – User Execution: Malicious File
- T1059.003 – Command and Scripting Interpreter: Windows Command Shell (cmd.exe)
- T1059.001 – Command and Scripting Interpreter: PowerShell
- T1071.001 – Application Layer Protocol: Web Protocols (HTTP)
- T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys
- T1055 – Process Injection
- T1105 – Ingress Tool Transfer

Containment

The process begins with isolating the affected machine - in this case, the WindowsBlue machine - from the network to prevent further communication, particularly outbound HTTP traffic to suspicious IP addresses such as 10.10.10.2 over port 80.
Using Splunk alerts, identify and confirm the presence of unauthorised tools such as curl.exe or PowerShell download commands, and immediately terminate malicious processes, including VictimRansomware.exe, to prevent further execution.

Eradication

After the affected machine is isolated and malicious activity is stopped, the next step is to eliminate all traces of the attacker's presence from the system. This involves removing any malware files, registry modifications, and persistence mechanisms used to maintain their access.
On the WindowsBlue machine, inspect and delete known malicious executables such as VictimRansomware.exe from the Downloads directory. Use Splunk alerts (Event ID 4657) to identify registry changes used for persistence and remove associated entries, for example:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Check and remove unauthorised user accounts, scheduled tasks, or services that may have been created during the attack. This step ensures the attacker cannot re-establish control or reinitiate the attack after containment.

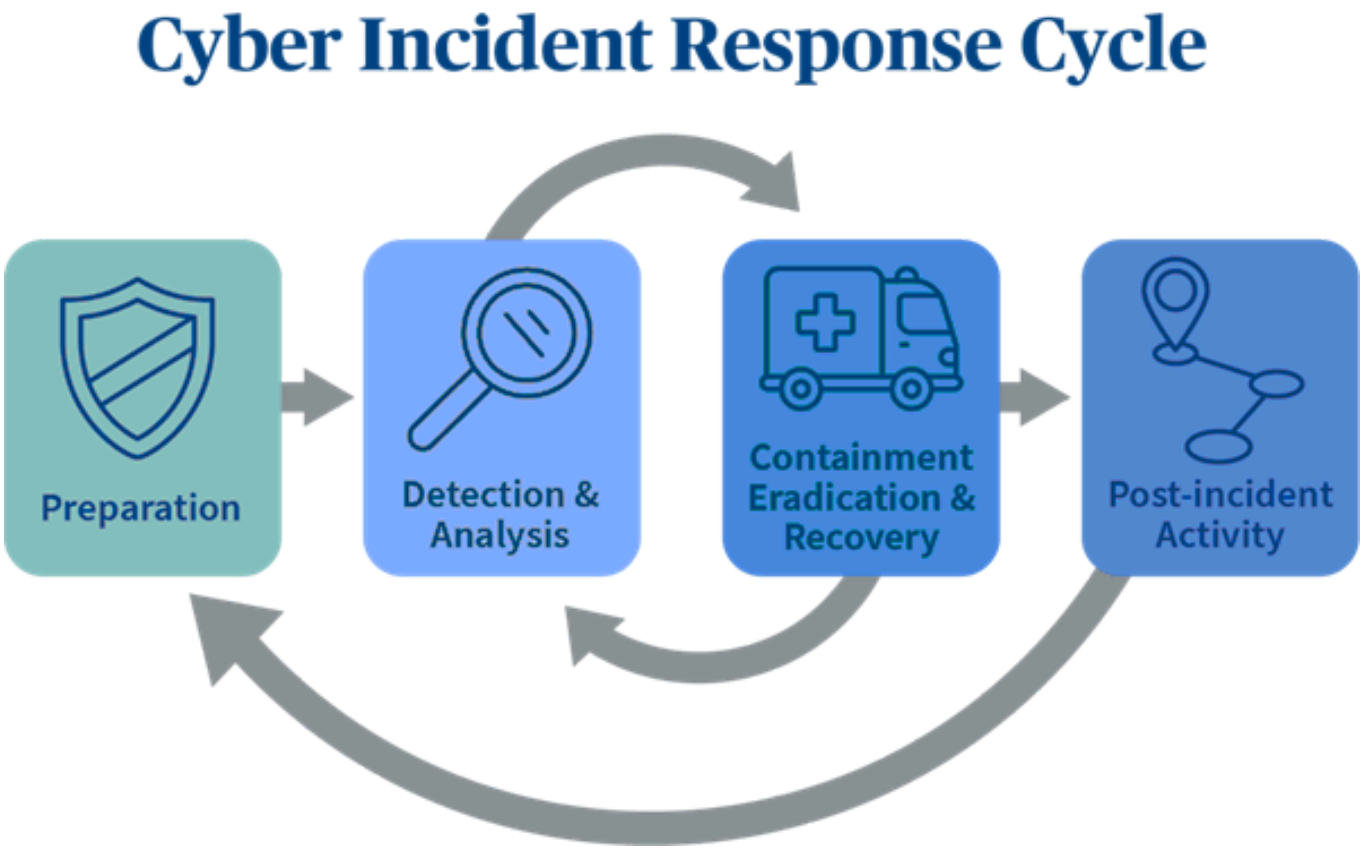
Recovery

Once eradication is complete and the system is free from malicious artifacts, the focus is now on restoring the system functionality. The WindowsBlue machine can now be reconnected to the network after confirming that no active threats remain.

System and event logs should be closely monitored to validate that:

- No unauthorised processes restart,
- Registry keys remain clean of persistence mechanisms,
- No more command-line executions are observed from suspicious sources - Event ID 4688 is monitored.

User accounts and permissions are checked to ensure no one gained extra access during the attack. If needed, the system can be restored using clean backups made before the attack happened. This will help return everything to normal while keeping a close watch for any signs the attacker might try to come back.



STEP 5: POST INCIDENT ACTIVITY

This phase is focused on learning from the incident, documenting lessons, and improving defences to prevent future attacks. It aligns with the NIST Cybersecurity Framework.

Debrief and Documentation

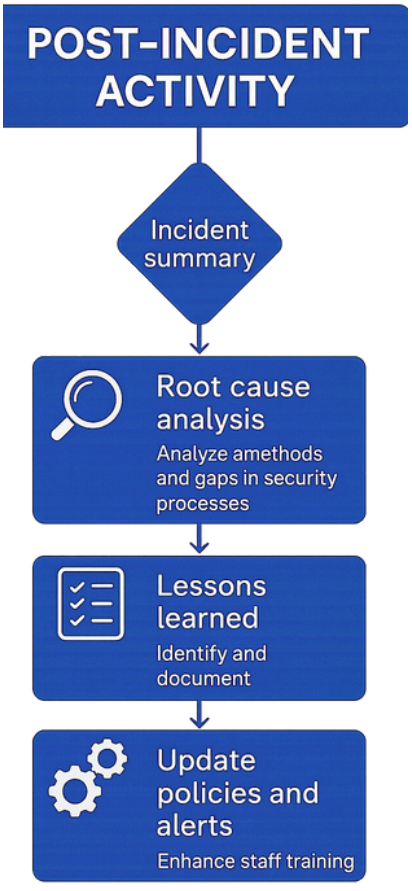
Document all findings, including timelines, attack vectors, and indicators of compromise (IoCs). It includes records of what was detected and when it occurred, and how it was addressed using the Splunk tool. These logs serve as a learning tool for improving incident response.

Root Cause Analysis

Investigate to determine how attackers gained access, which weaknesses were exploited, and which MITRE ATT&CK techniques were used. It may include reviewing process execution logs, any registry changes or network traffic anomalies. This helps identify gaps in defences and provides insights to prevent future recurrence.

Lessons Learned

Conduct a joint debrief with the Blue Team and Purple Team coordinators to analyse the incident response process. Identify what worked well - Splunk alerts that were triggered, and what detection gaps existed.



Update Detection Rules and Policies

Based on the findings, update Splunk alerts, Windows auditing policies, and firewall rules. Revise the incident response plan to reflect lessons learned. Schedule follow-up training and simulations to ensure continuous improvement.

Re-run the simulation to test new, improved response measures.

Staff Training and Awareness

Following the updates to detection rules and policies, conduct targeted training sessions to reinforce incident response procedures. Ensure that relevant staff are familiar with newly implemented Splunk alerts, audit configurations, and mitigation strategies.

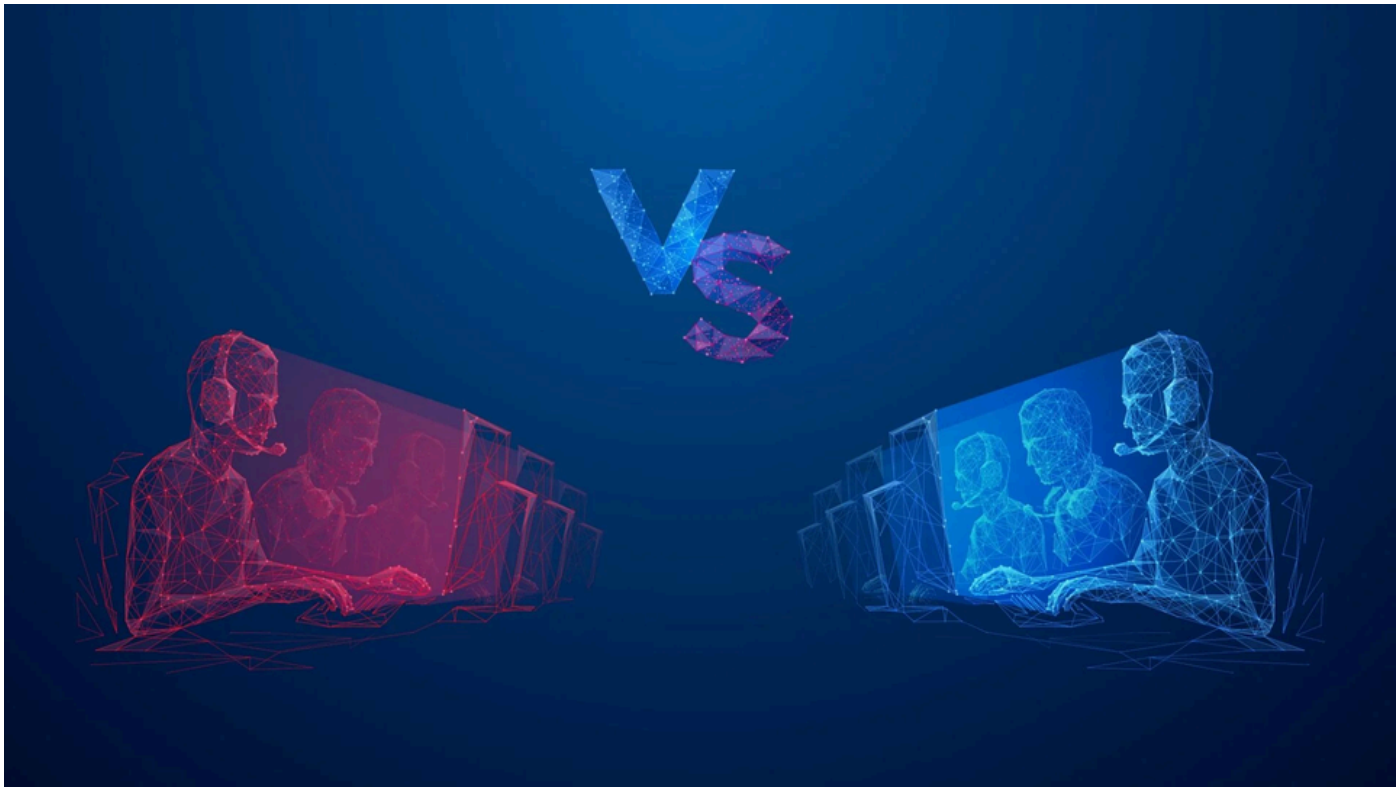
MITRE ATT&CK™ MAPPING AND DETECTION SUMMARY

MITRE Tactic	MITRE ATT&CK Technique ID	Technique	Event ID	Detection Description
Execution	T1204.002	User Execution: Malicious File	4688	RightPointV3.exe manually executed from Downloads
Persistence	T1547.001	Registry Run Keys/StartUp Folder	4657	Registry Run key created for persistence
Command & Control	T1105	Ingress Tool Transfer	4688	curl.exe used to download file from attacker C2
Command & Control	T1071.001	Web Protocols: HTTP	5156	Outbound HTTP traffic from victim to 10.10.10.2
Impact	T1486	Data Encrypted for Impact (Ransomware)	4663	VictimRansomware.exe encrypted files in Downloads

Post-Exercise Evaluation

The Blue Team successfully defended against simulated real-world cyberattacks based on MITRE ATT&CK techniques. The setup, including Windows auditing policies, Splunk alerts, and containment procedures, was tested across multiple stages of the cyber kill chain.
This exercise showed how important it is to detect threats early, trigger alerts quickly, and follow clear response steps. The Blue Team was able to act fast, reduce the damage, and stop the attack from spreading further.

Conclusion
The simulation helped us understand what parts of our response worked well and where we can improve. We will use these lessons to improve our settings, alerting, and update our incident response. Continued practice and training will make sure to stay ready for future attacks.



WWW.ALPHA7RESPONSE.COM