

Alert Triage

Now that you know how alerts are generated, it's time to review their content. While the details differ for every SIEM or security solution, the alerts generally have a few main properties you must understand before taking them. Don't worry if you find some confusing, as you will hear more about some in the upcoming tasks.

Time	Name	Severity	Status	Verdict	Assignee	Actions
Mar 21st 2025 at 11:53	Bruteforce Attack from External	Medium	Closed	True Positive	J.Adams (L2)	
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	Awaiting action	None	None	

Description: This rule detects a creation of a double-extension file like ".pdf.exe" or ".gif.lnk", often used by hackers in phishing attacks to trick users into opening the malicious executable.

Host: LPT-HR-009

Process Name: chrome.exe

Process User: S.Conway

Target File: C:\Users\S.Conway\Downloads\cats2025.mp4.exe

File MD5: 14d8486f3f63875ef93cfd240c5dc10b

1. Alert Time – Shows alert creation time.
2. Alert Name – Provide a summary of what happened, based on the detection rule's name.
3. Alert Severity – Defines the urgency of the alert (set by detection engineers)

- () Low / Informational
- () Medium / Moderate
- () High / Severe
- () Critical / Urgent

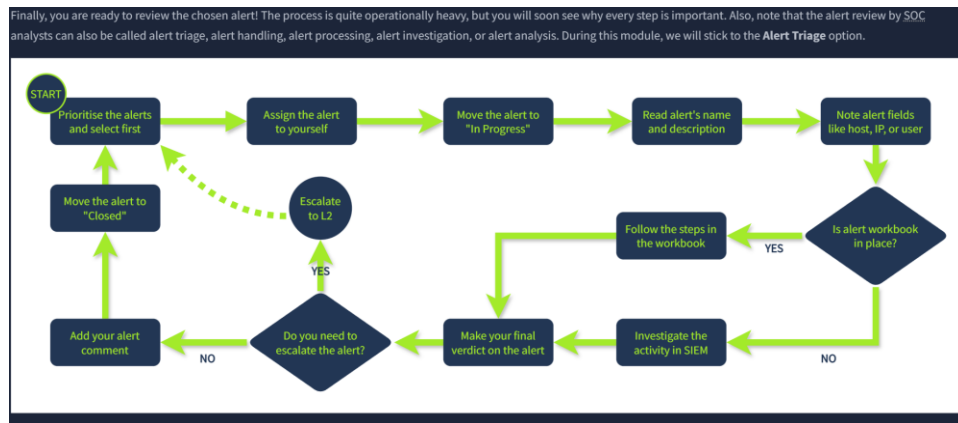
4. Alert Status – Inform if somebody is working on the alert or if the triage is done.

- () New / Unassigned
- () In Progress / Pending
- () Closed / Resolved
- And often other custom statuses

5. Alert Verdict – Also called alert classification, explains if the alert is a real threat or noise.

- () True Positive / Real Threat
- () False Positive / No Threat
- And often other custom verdicts

6. Alert Assignee – Shows the analyst that was assigned or assigned themselves to review the alert
7. Alert Description – Explains what the alert is about, usually in three sections on the right.
8. Alert Fields – Provides SOC analysts' comments and values on which the alert was triggered



Report Format

Report Format

Imagine yourself as an L2 analyst, a DFIR team member, or an IT professional who needs to understand the alert. What would you want to see in the report? We recommend you follow the **Five Ws** approach and include at least these items in the report:

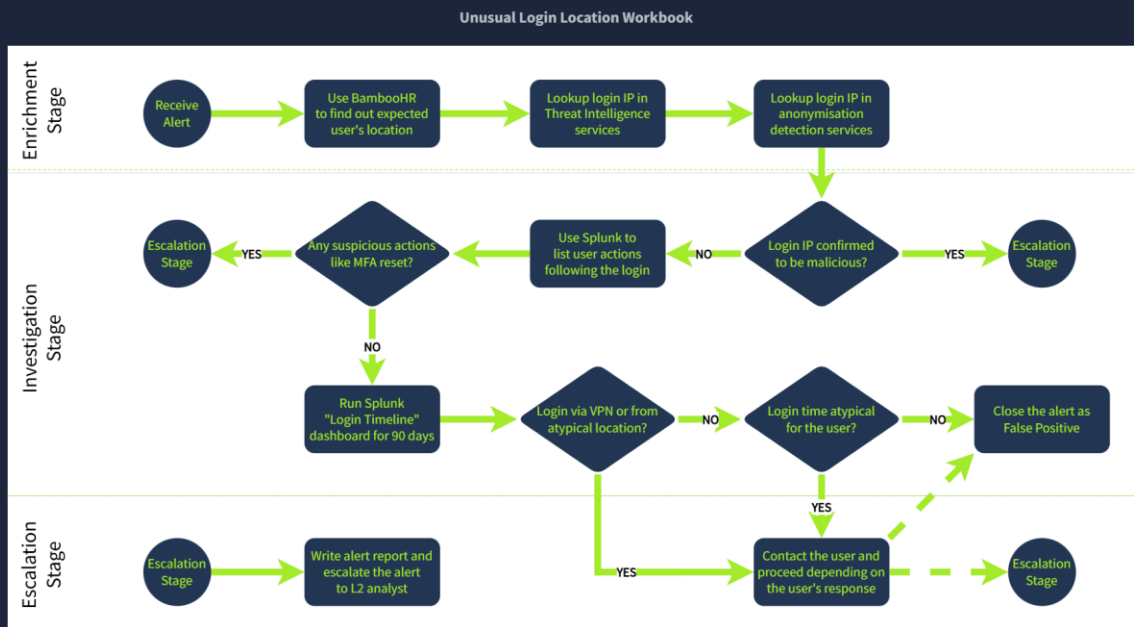
- **Who:** Which user logs in, runs the command, or downloads the file
- **What:** What exact action or event sequence was performed
- **When:** When exactly did the suspicious activity start and ended
- **Where:** Which device, IP, or website was involved in the alert
- **Why:** The most important W, the reasoning for your final verdict

ALERT REPORT CHECKLIST	
✓ All SIEMs are included in the report	
✓ Alert report is clear and precise	
✓ Alert report forms a single timeline	
✓ Evidence and indicators are attached	
✓ Escalation reason to L2 is explained	

Double-Extension File Creation	
Status	Verdict
Closed	True Positive
Severity	Assignee
High	J.Adams (L2)
Comment	
<p>At 13:56 UTC, the user S.Conway (Susan Conway, HR Coordinator) accessed the phishing website freecatvideoshd[.]monster from their LPT-HR-009 Windows laptop. At 13:58 UTC, the user downloaded a file from there named cats2023.mp4.exe, likely mistaking it for a legitimate video.</p> <p>VirusTotal reports confirm that the file is LummaStealer malware, aimed to exfiltrate sensitive data and establish a C2 channel. Further malware actions require deeper investigation, so escalating the alert to L2 and sharing the SIEM findings:</p> <p>> https://siem.tryhackme.thm/jggnU</p>	

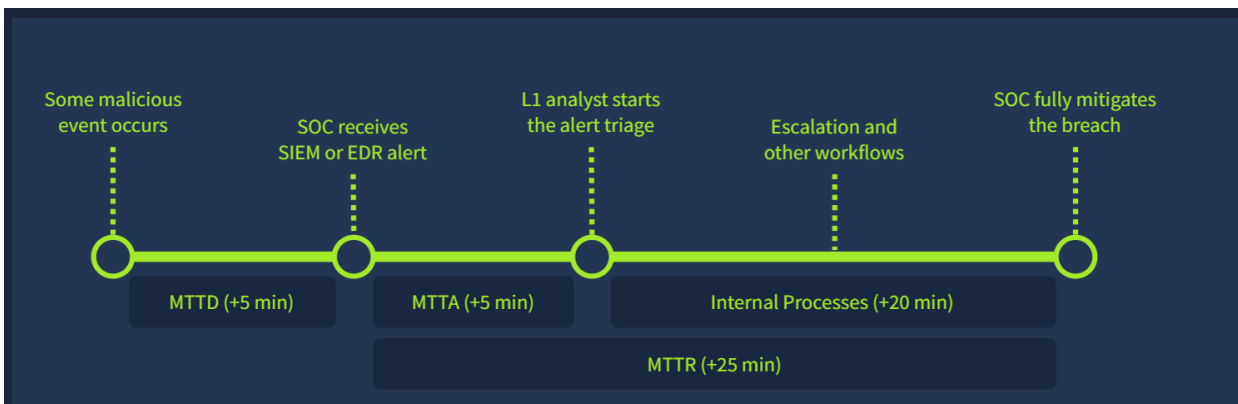
Workbook Example

Workbook Example



The diagram above is a typical example of an investigation workbook aimed to help L1 analysts triage alerts about atypical email, web, or corporate VPN login. Most workbook diagrams are supplemented with a detailed textual guide and links to the mentioned resources. Also, note how the workbook is divided into three logical groups. By following the steps in the correct order, you can guarantee high-quality alert triage and eliminate cases where the verdict is made without enough evidence:

Response Time within a EDR (Endpoint Detection Response)



SIEM (Security Information and Event Management) Tools

Splunk (Leading Tool in the Market)

Collect, Analyze and Correlate network and machine logs in real-time.

- Splunk Forwarder* – intended to monitor and collect data and direct it to Splunk instances.
- Splunk Indexer* – processes the data it receives from the forwarder.
- Search Head in Splunk (Search and Reporting App)* – users can search logs in “index=<log-file>”

Examples:

Index=<log-file> | stat count

Index=<log-file> Username=<username>

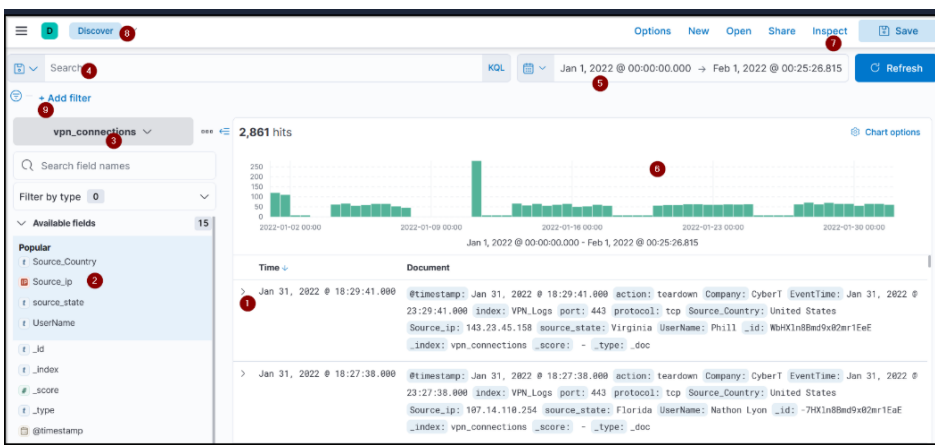
Index=<log-file> <source_ip>

Index=<log-file> Source_ip=<IPv4 ip address>

Elastic Stack - Elastic Search, Logstash, Beats, Kibana

A collection of different open-source tools that collect, store, search, and visualize data in real-time.

- Elastic Search* – full text search and analytics for JSON-formatted documents.
- Logstash* – a data processing engine that takes data from different sources, filters or normalizes it and then sends it to a destination like Kibana or any other destination for deeper analysis.
- Beats* – host-based agent that ships/transfer data from the endpoint to Elastic Search.
- Kibana* – a web-based data tool that works with Elastic Search to analyze, investigate and visualize data streams in real-time.

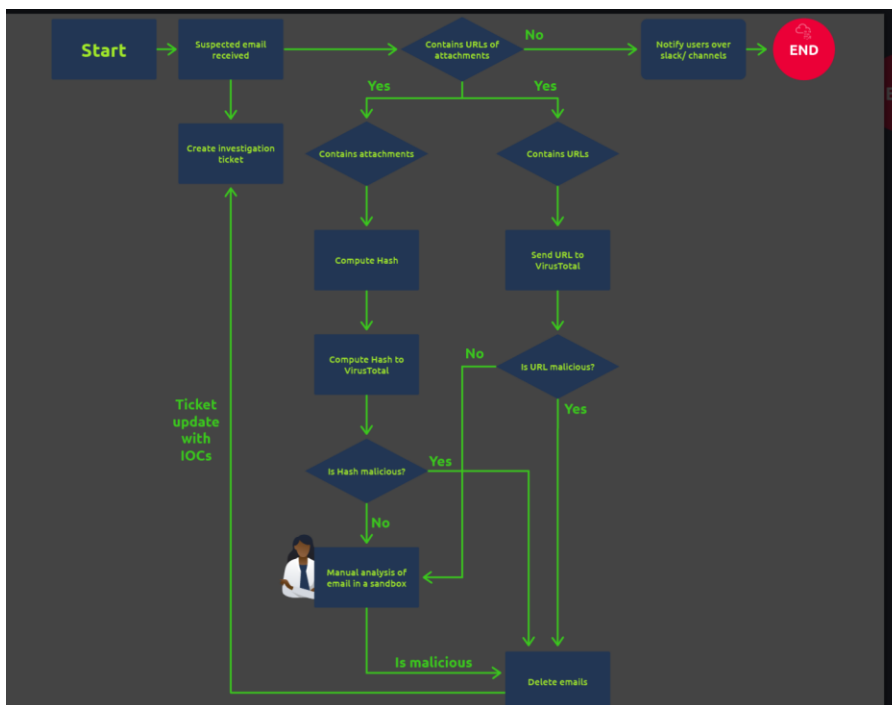


SOAR (Security Orchestration, Automation, and Response)

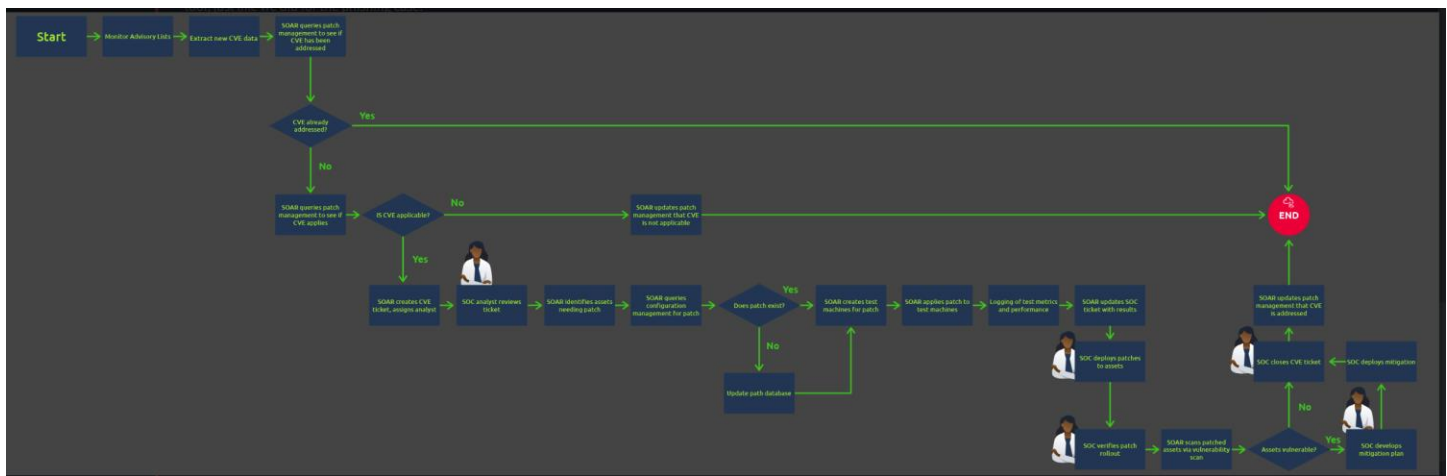
Unifies all tools that are used in a SOC (SIEM, EDR, and Firewall). Can operate all tools within a single SOAR environment.

- Security Orchestration* – link different tools within the SOAR interface
- Automation* – can run tools based on the playbook the Detection Engineer place to triage potential malicious activity.
- Response* – the ability to take actions based on the playbook the Detection Engineer placed to reduce the hassle on manually analyzing every bit of information from the malicious links, attachments, payload.exe and more.

Example: Phishing Playbook



Example: CVE (Common Vulnerability Exposers) Playbook



Pyramid of Pain

These are the initial steps an adversary may take to attempt to get a foot hold in a victim's machines whether it is a host or network based malicious operation.

- a. *Hash-Values* – its critical to identify hashes to interpret rather is it a malicious activity or not. The main hash values that can be identified are MD5 or a SHA256 using online tools – such a Virus Total.

How to find hash values? There are online tools that can be used to interpret what the hash values are, or you can manually interpret the hash values through Windows PowerShell or Ubuntu/Linux terminal.

Windows PowerShell Command – Once In Working Directory or `.\working\directory\path.doc\`

`Get-FileHah <space>-Algorithm MD5 <Doc>`

`Get-FileHah <space> .\working\directory\ path.doc\ -Algorithm MD5 <Doc>`

`Get-FileHah <space>-Algorithm SHA256<Doc>`

`Get-FileHah <space> .\working\directory\ path.doc\ -Algorithm SHA256<Doc>`

Ubuntu/Linux Terminal - Once in Working Directory or `/working /directory /path.doc`

`MD5sum<space>file.doc`

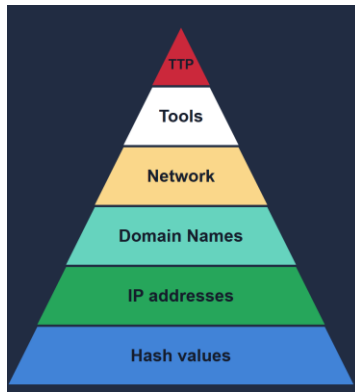
`SHA256sum<space>file.doc`

`MD5sum<space>/working/directory/path/file.doc`

`SHA256sum <space>/working/directory/path/file.doc`

- b. *IP Address (IPv4)* – Used to identify any devices on the network rather it's a desktop, server or a remote machine
- c. *Domain Names* – Can be used to map and ip address. Domains can have a sub-domain that houses an executable link to a payload that can or maybe in the background of a html format “href”
- d. *Network* – Can be a user agent string, C2-INformation or a URL pattern followed by a HTTP.GET or HTTP.POST request that can be analyzed deeper with Wireshark or brim or manually in the Ubuntu/Linux Command Lines in Terminal.
- e. *Tools* – Attackers can use utilities to implement macro malicious documents for spear phishing or backdoor using C2 infrastructures.

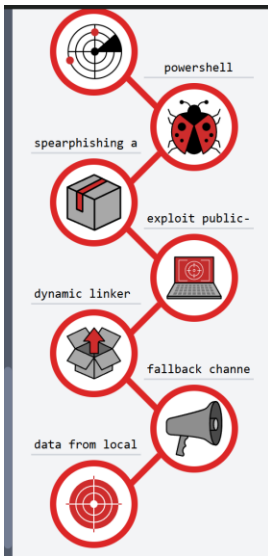
- f. *TTP (Tactic, Technique, Procedures)* - includes an entire MITRE ATT&CK MATRIX. This is the rigorous phase an attacker may use.



Kill Chain

A military concept that was adopted to use to implement a Cyber Kill Chains by LockHeed Martin.

- a. *Reconnaissance Passive (no interaction) or Active (interaction)* - gathering Information about the target.
- b. *Weaponization* – using the information gathered to create a tool that can be bought from the dark web or hand crafted to a specific target.
- c. *Delivery* – This is when phishing emails, malicious USB drops, or watering holes comes into action.
- d. *Exploitation* – once the delivery of the malware was double-clicked, downloaded or inserted to a USB port, when the malware was executed.
- e. *Installation* – this is when the malware is now on the victim's machine.
- f. *C2 (Command and Control)* – After the installation, there is a remote communication between the victim machine and the attacker (the external server setup by the attacker) using port 80 for http, port 443 for https or DNS tunneling.
- g. *Actions and objectives* – this is when the attacker can achieve their goals and the attackers have access to the machine such as MitM (Man-in-the-Middle), steal credentials, have permanent back-door access, monitoring, conducting a ransomware, crypto mining attack, and many more.



Unified Kill Chain – Theat Modeling

A Unified Kill Chain is a more thorough, high-level overview of the attacker procedure of attack. It encourages threat modeling and helps interpret potential attack methodologies. There is a total of 18 steps in the Unified Kill Chain. The screenshot from TryHackMe briefly explains below.

The Unified Kill Chain



1	Reconnaissance	Researching, identifying and selecting targets using active or passive reconnaissance.
2	Weaponization	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	Delivery	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	Social Engineering	Techniques aimed at the manipulation of people to perform unsafe actions.
5	Exploitation	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	Persistence	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	Defense Evasion	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	Command & Control	Techniques that allow attackers to communicate with controlled systems within a target network.
9	Pivoting	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	Discovery	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	Privilege Escalation	The result of techniques that provide an attacker with higher permissions on a system or network.
12	Execution	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	Lateral Movement	Techniques that enable an adversary to horizontally access and control other remote systems.
15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration.
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network.
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

MITRE ATT&CK

MITRE ATT&CK framework is a globally accessible website that is the base knowledge of an attackers Tactic, Techniques and Procedures on is based on Real-World Scenarios. This can be used as a SOC analyst to determine how an attacker occurred and what the additional measures taken the attacker uses to reach its goals.

about

Mustang Panda (G0129)

Enterprise techniques used by Mustang Panda, ATT&CK group G0129 (v2.1)

domain

Enterprise ATT&CK v17

platforms

Windows, Linux, macOS, Network Devices,
ESXi, PRE, Containers, IaaS, SaaS, Office Suite,
Identity Provider

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control				
Acquire Infrastructure	Phishing	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Execution Guardrails	OS Credential Dumping	File and Directory Discovery	Replication Through Removable Media	Archive Collected Data	Application Layer Protocol				
Establish Accounts	Replication Through Removable Media	Exploitation for Client Execution	Event Triggered Execution	Event Triggered Execution	Hide Artifacts		Process Discovery		Automated Collection	Encrypted Channel				
Obtain Capabilities					Hijack Execution Flow									
Stage Capabilities					Scheduled Task/Job						Hijack Execution Flow	Indicator Removal	Masquerading	Software Discovery
														System Information Discovery
	System Network Configuration Discovery													
Obfuscated Files or Information	System Network Connections Discovery	Data Staged	Ingress Tool Transfer											
				Non-Application Layer Protocol										
				Proxy										
							Remote Access Tools	Web Service						