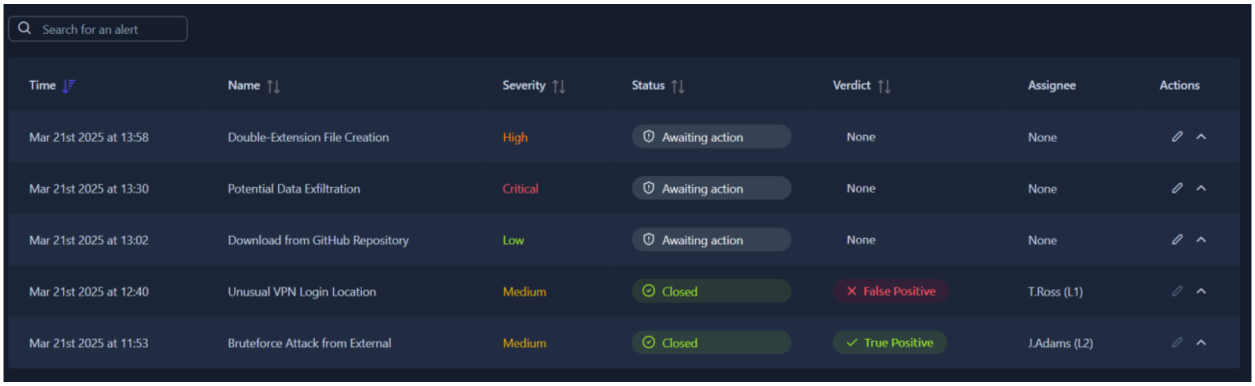
SOC ALERT 1 TRIAGE 2025/12/19

Events and Alerts

STEP 1: What is the number of alerts you see in the SOC dashboard?

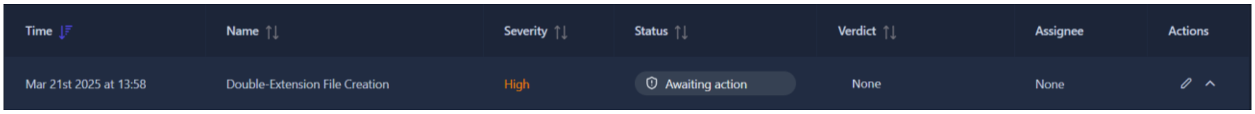


Search for an alert

Time	Name	Severity	Status	Verdict	Assignee	Actions
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	Awaiting action	None	None	
Mar 21st 2025 at 13:30	Potential Data Exfiltration	Critical	Awaiting action	None	None	
Mar 21st 2025 at 13:02	Download from GitHub Repository	Low	Awaiting action	None	None	
Mar 21st 2025 at 12:40	Unusual VPN Login Location	Medium	Closed	✕ False Positive	T.Ross (L1)	
Mar 21st 2025 at 11:53	Bruteforce Attack from External	Medium	Closed	✓ True Positive	J.Adams (L2)	

Looking at the dashboard, I identified 5 alerts.

STEP2: What is the name of the most recent alert you see?

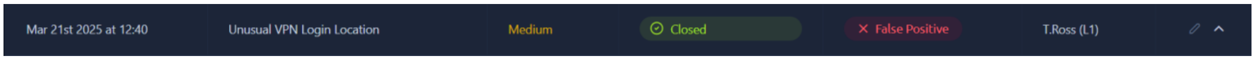


Time	Name	Severity	Status	Verdict	Assignee	Actions
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	Awaiting action	None	None	

The most recent identified alert was **Double-Extension File Creation**.

Alert Properties

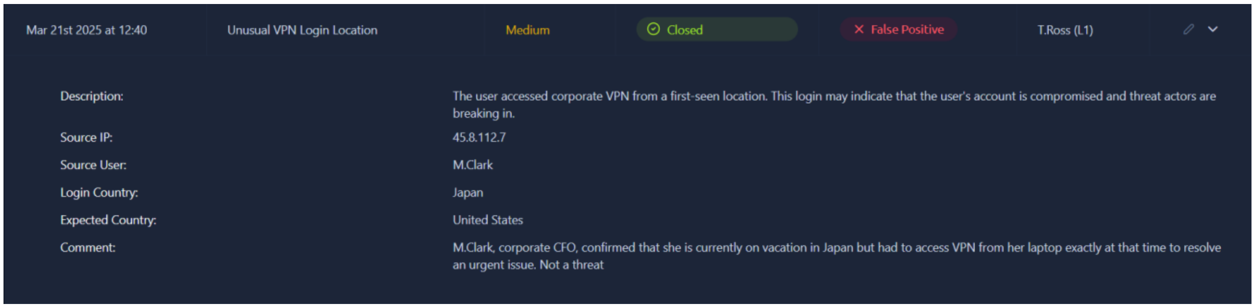
STEP 3: What was the verdict for the "Unusual VPN Login Location" alert?



Mar 21st 2025 at 12:40	Unusual VPN Login Location	Medium	Closed	✕ False Positive	T.Ross (L1)	

False Positive.

STEP 4: What user was mentioned in the "Unusual VPN Login Location" alert?



Mar 21st 2025 at 12:40 | Unusual VPN Login Location | Medium | Closed | ✕ False Positive | T.Ross (L1)

Description: The user accessed corporate VPN from a first-seen location. This login may indicate that the user's account is compromised and threat actors are breaking in.

Source IP: 45.8.112.7

Source User: M.Clark

Login Country: Japan

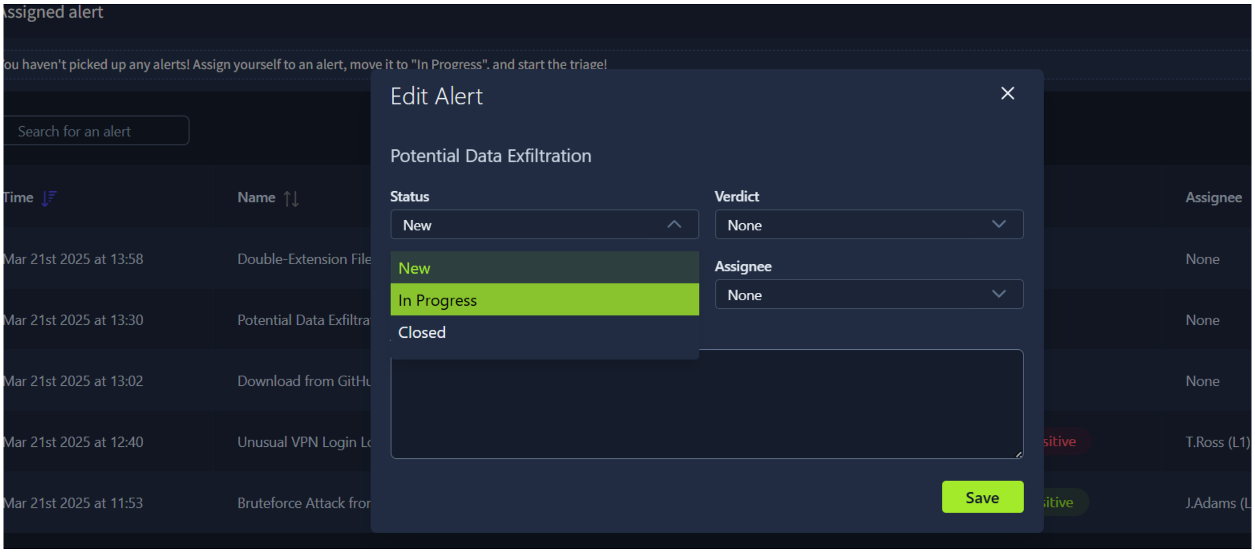
Expected Country: United States

Comment: M.Clark, corporate CFO, confirmed that she is currently on vacation in Japan but had to access VPN from her laptop exactly at that time to resolve an urgent issue. Not a threat

M.Clark.

Alert Prioritisation

STEP 5: Assign yourself to the first-priority alert and change its status to **In Progress**. The name of your selected alert will be the answer to the question.



ssigned alert

ou haven't picked up any alerts! Assign yourself to an alert, move it to "In Progress", and start the triage!

Time	Name		Assignee
Mar 21st 2025 at 13:58	Double-Extension File		None
Mar 21st 2025 at 13:30	Potential Data Exfiltra		None
Mar 21st 2025 at 13:02	Download from GitHu		None
Mar 21st 2025 at 12:40	Unusual VPN Login Lo	sitive	T.Ross (L1)
Mar 21st 2025 at 11:53	Bruteforce Attack fror	sitive	J.Adams (L

Edit Alert

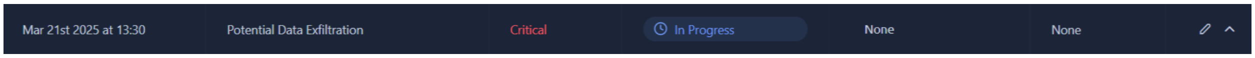
Potential Data Exfiltration

Status: New

- New
- In Progress
- Closed

Verdict: None

Assignee: None

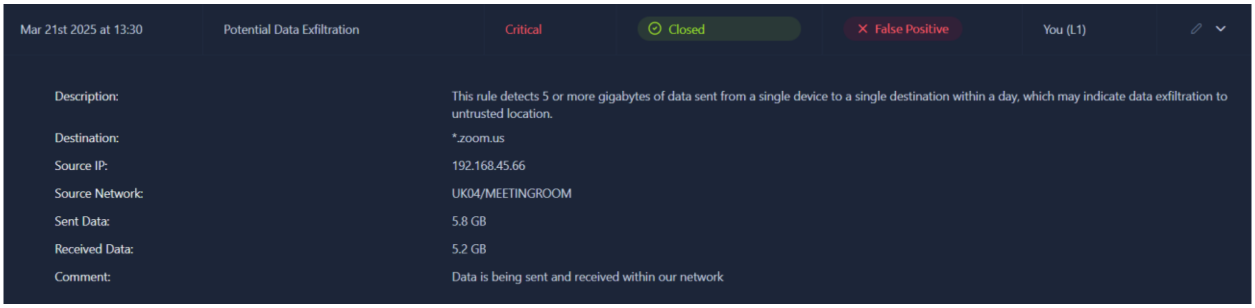


Mar 21st 2025 at 13:30 | Potential Data Exfiltration | Critical | In Progress | None | None

Potential Data Exfiltration.

Alert Triage

STEP 6: Which flag did you receive after you correctly triaged the first-priority alert?

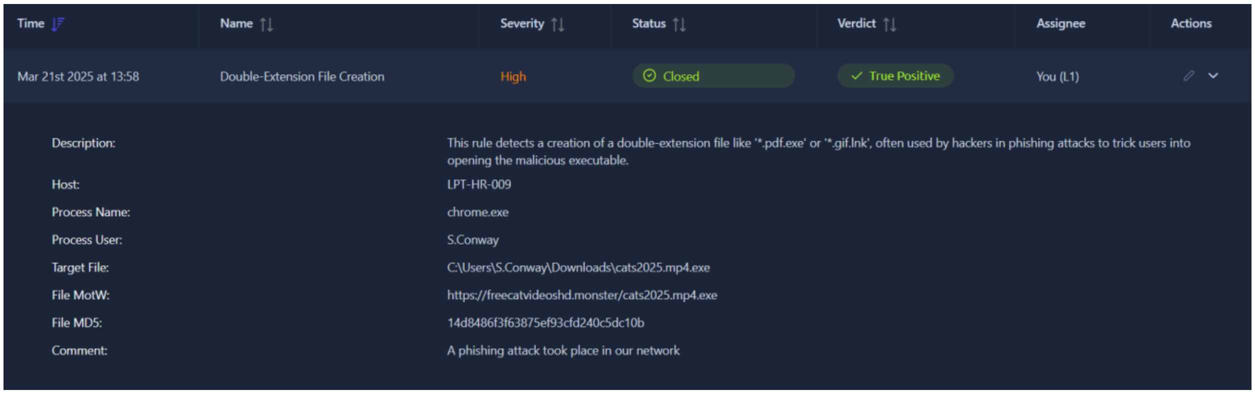


Mar 21st 2025 at 13:30	Potential Data Exfiltration	Critical	Closed	✕ False Positive	You (L1)	

Description:	This rule detects 5 or more gigabytes of data sent from a single device to a single destination within a day, which may indicate data exfiltration to untrusted location.
Destination:	*.zoom.us
Source IP:	192.168.45.66
Source Network:	UK04/MEETINGROOM
Sent Data:	5.8 GB
Received Data:	5.2 GB
Comment:	Data is being sent and received within our network

THM{looks_like_lots_of_zoom_meetings}

STEP 7: Which flag did you receive after you correctly triaged the second-priority alert?

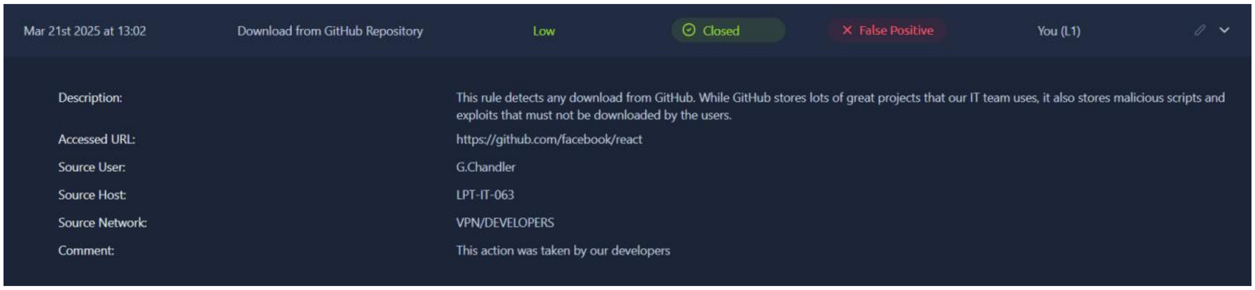


Time	Name	Severity	Status	Verdict	Assignee	Actions
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	Closed	✓ True Positive	You (L1)	

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 MotW:	https://freecatvideoshd.monster/cats2025.mp4.exe
File MD5:	14d8486f3f63875ef93cfd240c5dc10b
Comment:	A phishing attack took place in our network

THM{how_could_this_user_fall_for_it?}

STEP 8: Which flag did you receive after you correctly triaged the third-priority alert?



Mar 21st 2025 at 13:02	Download from GitHub Repository	Low	Closed	✕ False Positive	You (L1)	

Description:	This rule detects any download from GitHub. While GitHub stores lots of great projects that our IT team uses, it also stores malicious scripts and exploits that must not be downloaded by the users.
Accessed URL:	https://github.com/facebook/react
Source User:	G.Chandler
Source Host:	LPT-IT-063
Source Network:	VPN/DEVELOPERS
Comment:	This action was taken by our developers

THM{should_we_allow_github_for_devs?}

Conclusion Summary

In this SOC Alert 1 Triage exercise, I analysed and prioritised multiple security alerts within a SOC dashboard to simulate real-world alert handling. By reviewing alert volumes, identifying the most recent activity, and validating verdicts such as a false-positive unusual VPN login, I demonstrated effective alert assessment and contextual analysis. I then assigned ownership to high-priority alerts, updated their status appropriately, and performed structured triage to investigate potential threats, including data exfiltration and user-based security risks. Successfully resolving alerts and capturing all associated flags reinforced my ability to prioritise incidents, reduce alert noise, and apply analytical decision-making aligned with day-to-day SOC operations