

Time	Name	Severity	Status	Verdict	Assignee	Actions
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	Closed	True Positive	You (L1)	
<div> <div>Description:</div> <div>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.</div> <div>Host:</div> <div>LPT-HR-009</div> <div>Process Name:</div> <div>chrome.exe</div> <div>Process User:</div> <div>S.Conway</div> <div>Target File:</div> <div>C:\Users\S.Conway\Downloads\cats2025.mp4.exe</div> <div>File MotW:</div> <div>https://freecatvideoshd.monster/cats2025.mp4.exe</div> <div>File MD5:</div> <div>14d8486f3f63875ef93cfd240c5dc10b</div> <div>Comment:</div> <div> - Provide training to prod - Block email </div> </div>						
Mar 21st 2025 at 13:30	Potential Data Exfiltration	Critical	Closed	False Positive	You (L1)	
<div> <div>Description:</div> <div>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.</div> <div>Destination:</div> <div>*.zoom.us</div> <div>Source IP:</div> <div>192.168.45.66</div> <div>Source Network:</div> <div>UK04/MEETINGROOM</div> <div>Sent Data:</div> <div>5.8 GB</div> <div>Received Data:</div> <div>5.2 GB</div> <div>Comment:</div> <div> - Who: Clients and managers - When: March 21, 2025 - Where: Meeting Room Facility - Why: The Data are from data consumed by online meeting bandwidth. </div> </div>						
Mar 21st 2025 at 13:02	Download from GitHub Repository	Low	Closed	False Positive	You (L1)	
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)	

Alert Simulations – Triage, False Positive/True Positive Identification, and Resolving and Closing Tickets

Time	Name	Severity	Status	Verdict	Assignee	Actions
1 Mar 21st 2025 at 11:53	2 Bruteforce Attack from External	3 Medium	4 Closed	5 True Positive	6 J.Adams (L2)	
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	Awaiting action	None	None	
<div> <div>Description:</div> <div>7 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.</div> <div>Host:</div> <div>LPT-HR-009</div> <div>Process Name:</div> <div>chrome.exe</div> <div>Process User:</div> <div>S.Conway</div> <div>Target File:</div> <div>C:\Users\S.Conway\Downloads\cats2025.mp4.exe</div> <div>File MotW:</div> <div>8 https://freecatvideoshd.monster/cats2025.mp4.exe</div> <div>File MD5:</div> <div>14d8486f3f63875ef93cfd240c5dc10b</div> </div>						

Alert Structure