

Monitoring

Log Management

Case Management

Endpoint Security

Email Security

Threat Intel

Sandbox

MAIN CHANNEL

INVESTIGATION CHANNEL

CLOSED ALERTS

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	Sep, 17, 2024, 12:05 PM	SOC326 - Impersonating Domain MX Record Change Detected	304	ThreatIntel	
High	Jun, 06, 2024, 03:12 PM	★ SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]	263	Web Attack	
Critical	Apr, 18, 2024, 03:09 AM	★ SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation [CVE-2024-3400]	249	Web Attack	
Medium	Mar, 07, 2024, 11:44 AM	SOC176 - RDP Brute Force Detected	234	Brute Force	
Medium	Jan, 01, 2024, 12:37 PM	SOC251 - Quishing Detected (QR Code Phishing)	214	Exchange	
Medium	Dec, 27, 2023, 11:22 AM	★ SOC250 - APT35 HyperScape Data Exfiltration Tool Detected	212	Data Leakage	
Medium	Dec, 12, 2023, 02:15 PM	SOC246 - Forced Authentication Detected	208	Web Attack	
High	Nov, 21, 2023, 12:24 PM	★ SOC239 - Remote Code Execution Detected in Splunk Enterprise	201	Unauthorized Access	

This is how a SIEM dashboard usually looks like. Here we can monitor logs, intrusions and suspicious activities, and take up a case if necessary

Monitoring

Log Management

Case Management

Endpoint Security

Email Security

Threat Intel

Sandbox

MAIN CHANNEL

INVESTIGATION CHANNEL

CLOSED ALERTS

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	Mar, 13, 2021, 08:20 PM	SOC138 - Detected Suspicious Xls File	77	Malware	» ✓
<div>This alert has been re-investigated</div> <div><div>EventID :</div><div>77</div></div> <div><div>Event Time :</div><div>Mar, 13, 2021, 08:20 PM</div></div> <div><div>Rule :</div><div>SOC138 - Detected Suspicious Xls File</div></div> <div><div>Level :</div><div>Security Analyst</div></div> <div><div>Source Address :</div><div>172.16.17.56</div></div> <div><div>Source Hostname :</div><div>Sofia</div></div> <div><div>File Name :</div><div>ORDER SHEET & SPEC.xlsm</div></div> <div><div>File Hash :</div><div>7ccf88c0bbe3b29bf9d877c4596a8d4</div></div> <div><div>File Size :</div><div>2.66 Mb</div></div> <div><div>Device Action :</div><div>Allowed</div></div> <div><div>File (Password:infected) :</div><div>Download</div></div>					

After taking up the case we can find the details of the case and necessary information in the dashboard. Here we can take the ownership of the case and start investigating

Incident Details	
Incident Name:	EventID: 77 - [SOC138 - Detected Suspicious Xls File]
Description:	EventID: 77
Incident Type:	Malware
Created Date:	Dec, 24, 2024, 01:09 PM
Start Playbook!	

After creating a case we go to the case management section, And fill the playbook. This helps us to make sure if the alert was a fake positive or not. The play book guides us through that helping us with the case.