Customer:Sample Customer

Monthly Report

Reporting Period:1/Mar/24 - 30/Mar/24

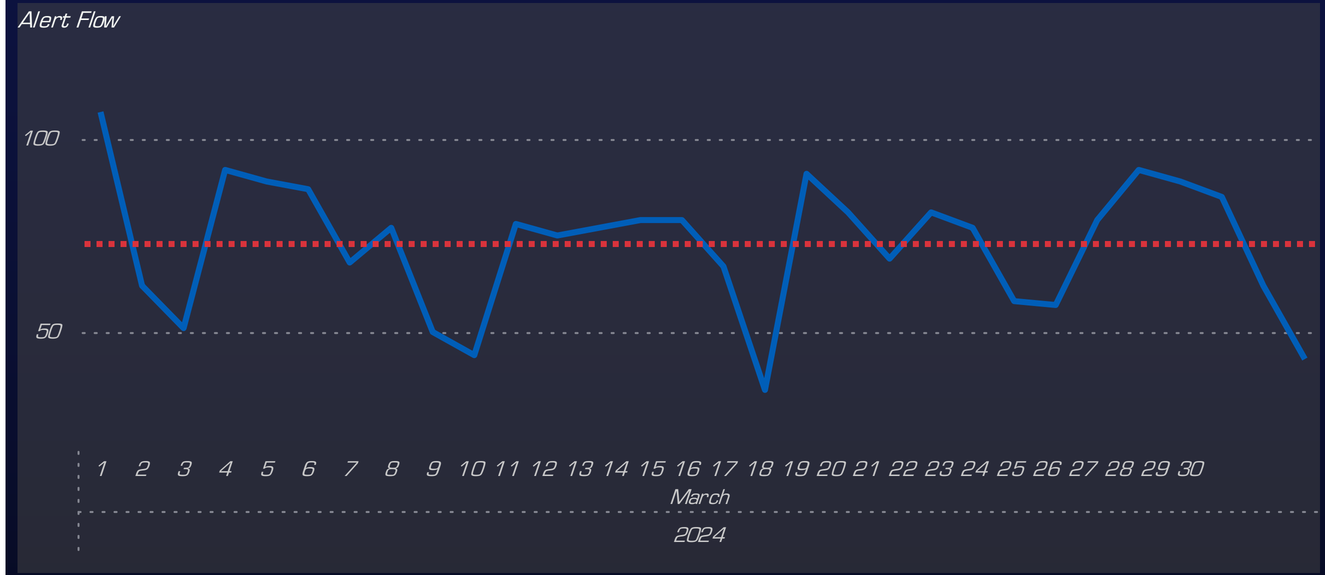
Event Pipeline (Reporting Period)

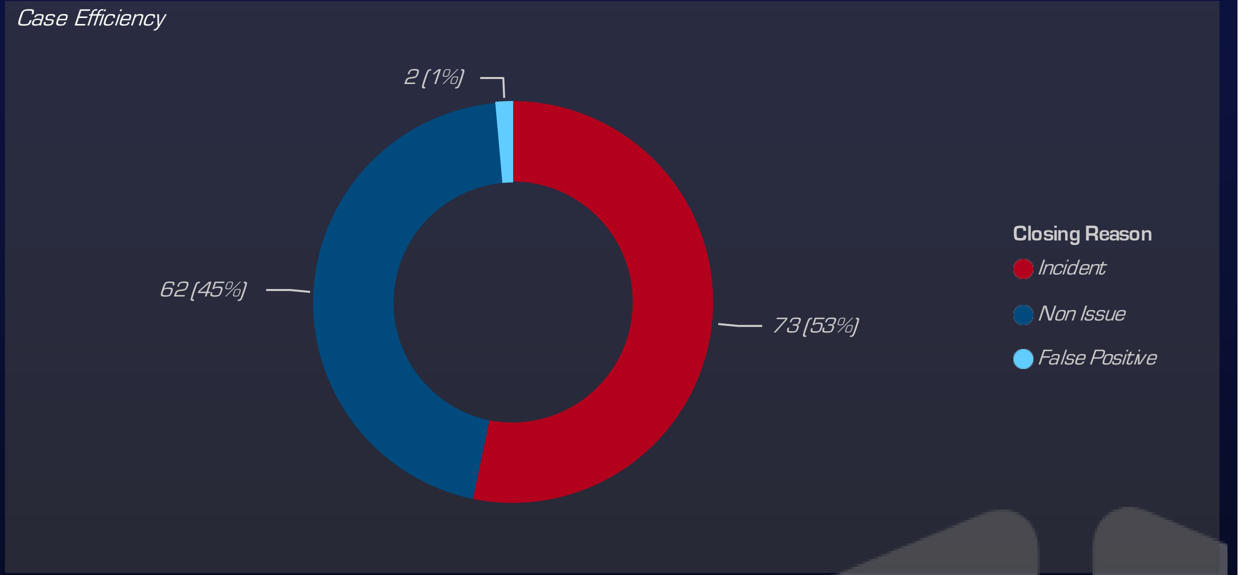
2,294	/	2,143	/	148
Alerts		Triaged		Created Cases

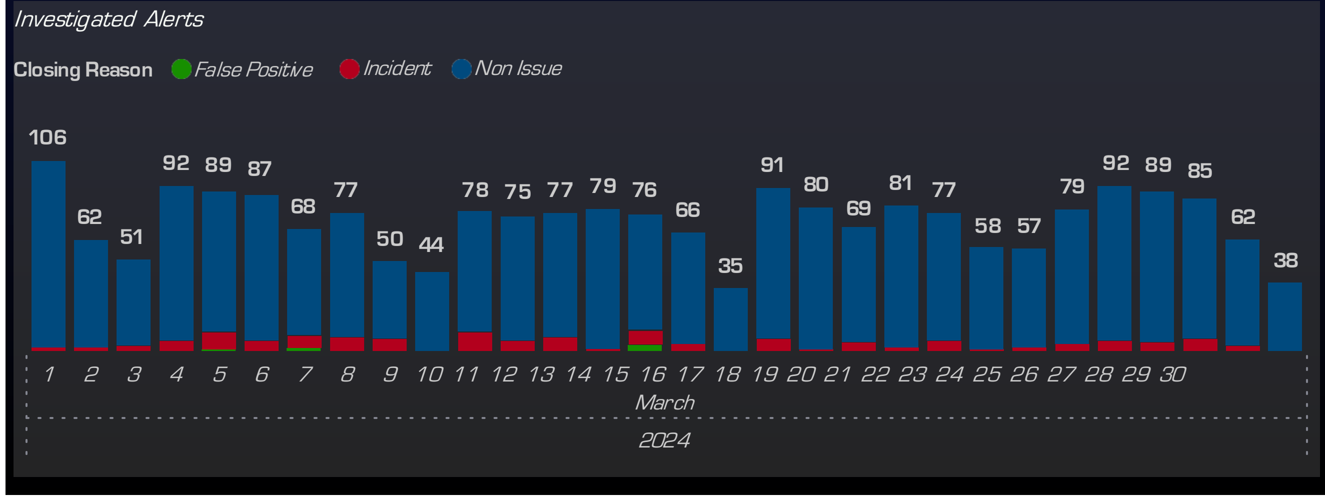
Response Time in minutes (Reporting Period)

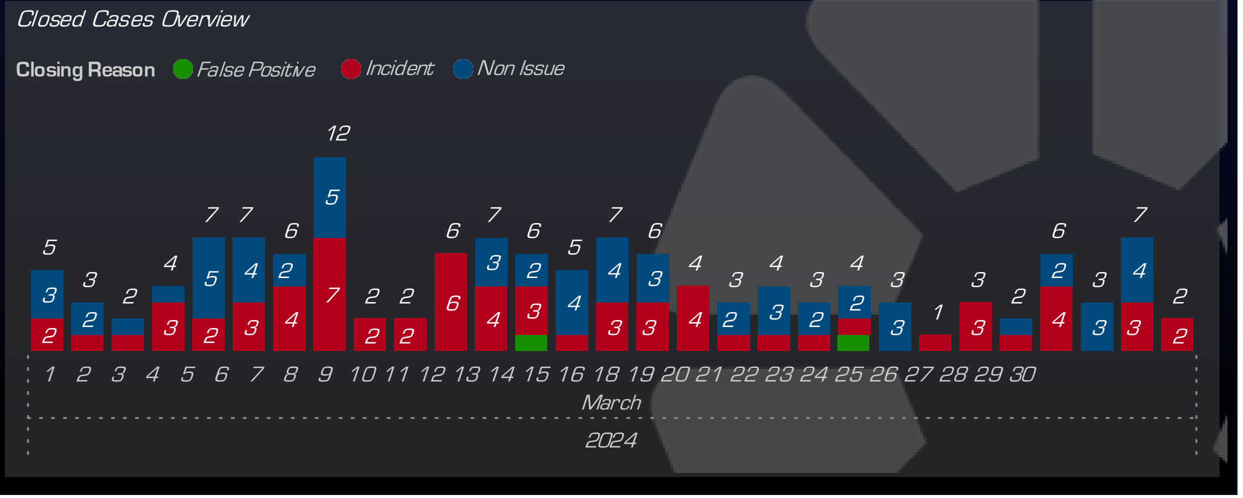
For Very High (30) and High (60) Cases

35.0	5.0	5.1
Mean Time to Report (SLA)	Mean Time to Acknowledge	Mean Time to Contain (Days)









Last 6 months trends

18,085 Alerts / 17,174 Triaged / 862 Created Cases

Response Time in minutes

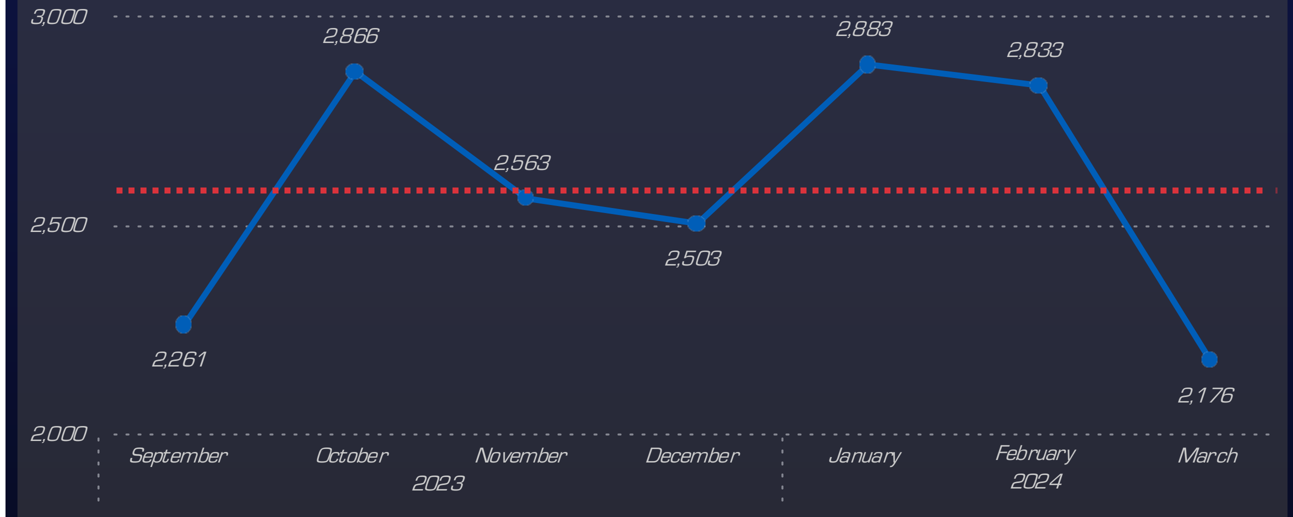
For Very High (30) and High (60) Cases

35.3 Mean Time to Report (SLA)

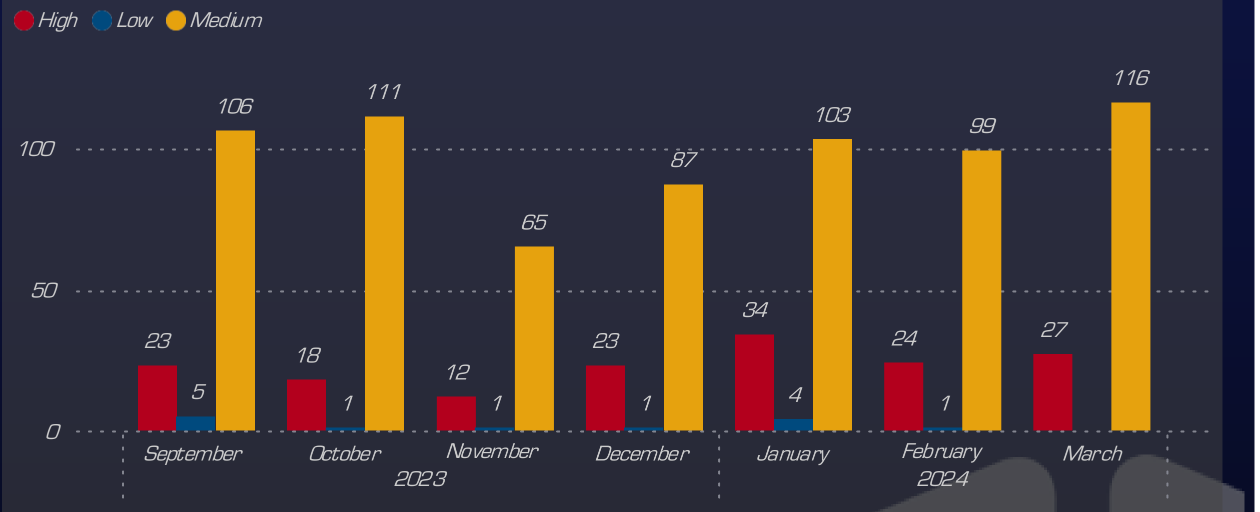
4.0 Mean Time to Acknowledge

4.6 Mean Time to Contain (Days)

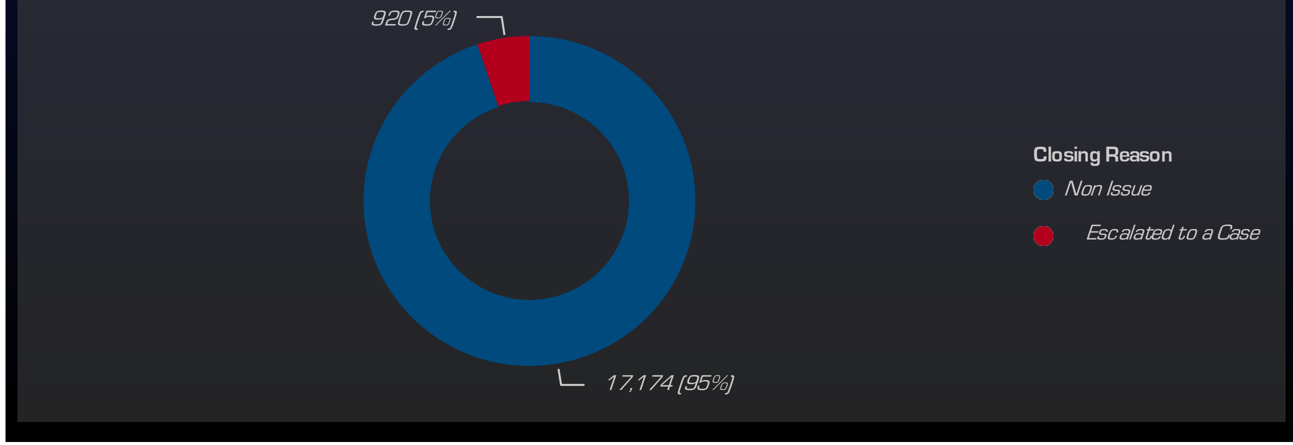
Alerts Flow



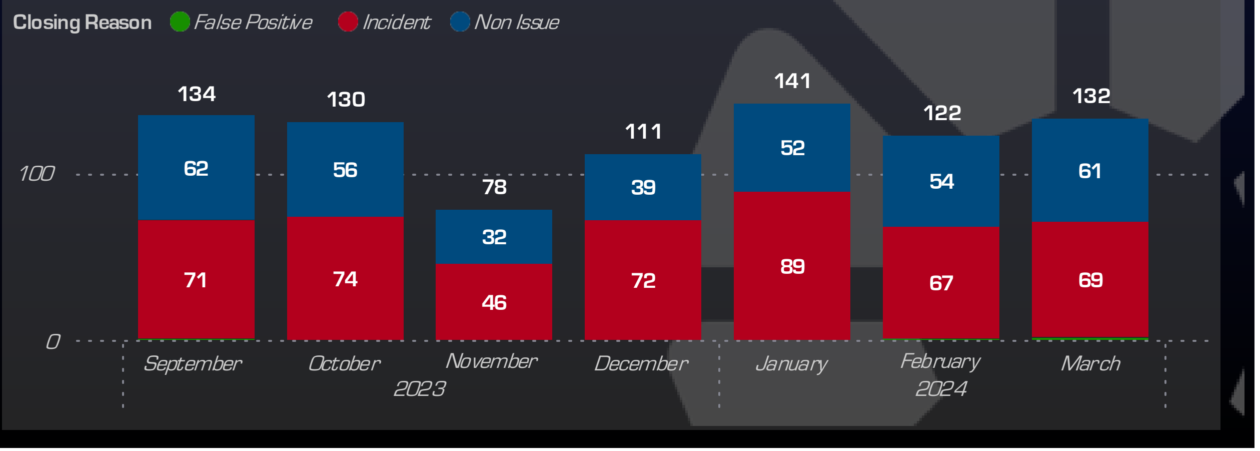
Cases Severity



Alert Efficiency

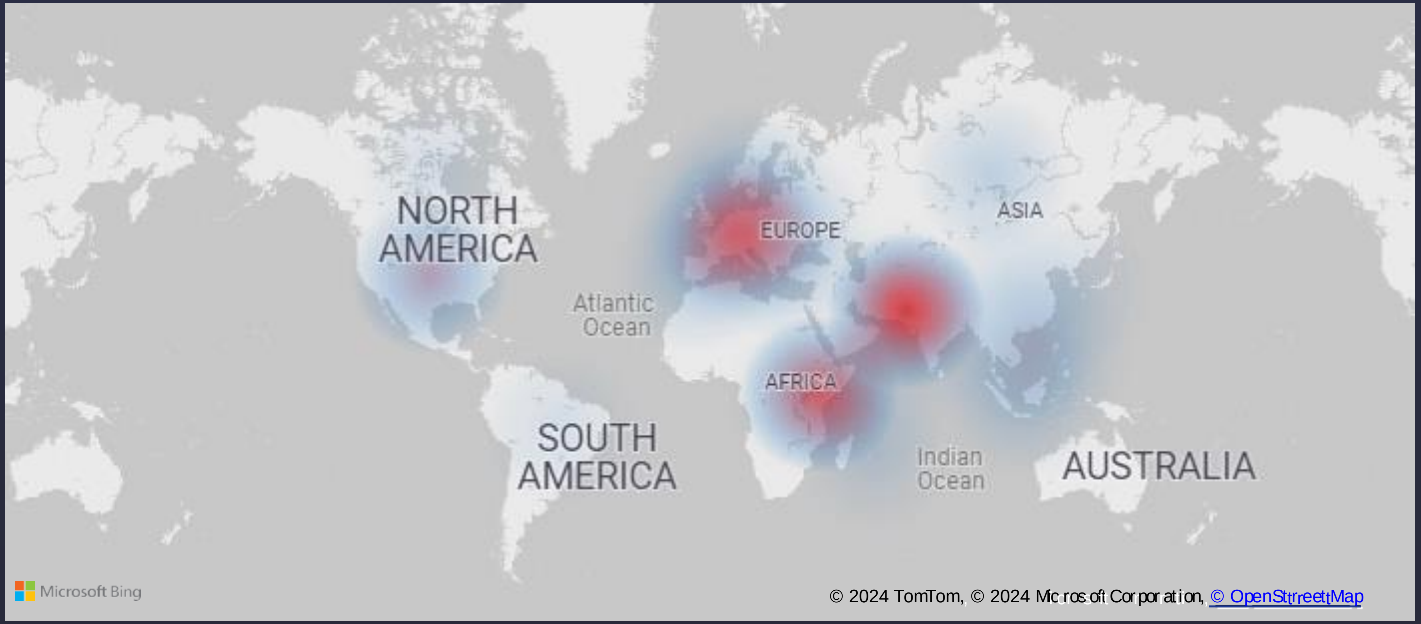


Closed Cases Overview



Attack Surface (Reporting Period)

Attack Heatmap



© 2024 TomTom, © 2024 Microsoft Corporation, © OpenStreetMap

Top Attacking Countries

Country	%
Pakistan	42.50%
Kenya	31.23%
United States	17.84%
Germany	3.10%
Russia	2.97%
United Kingdom	2.35%

Risk Assessment

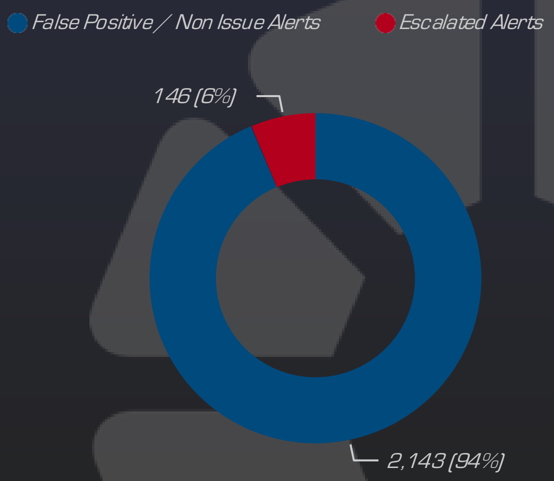
Top Source Networks

Source Network	False Positive	Incident	Non Issue
Network.Zone 1	2	30	445
Wireless_One		51	341
ZoneX	4	10	305
Data_Wired_ServerVlan	1	1	222
DATACENTER_5			216
Device_Management		4	124

Top Target Networks

Destination Network	False Positive	Incident	Non Issue
DATACENTER_5	1	1	391
Default_Domain.Net	4	34	350
Data_Wired_ServerVlan	1	3	273
Private_zones		21	222
Device_Management_PABX		6	200
DATACENTER_3	1	35	125
PABX_Room		1	134

Investigations



Service Coverage

EPS Coverage

13,601
Current EPS Rate

14,000
Contracted EPS Rate

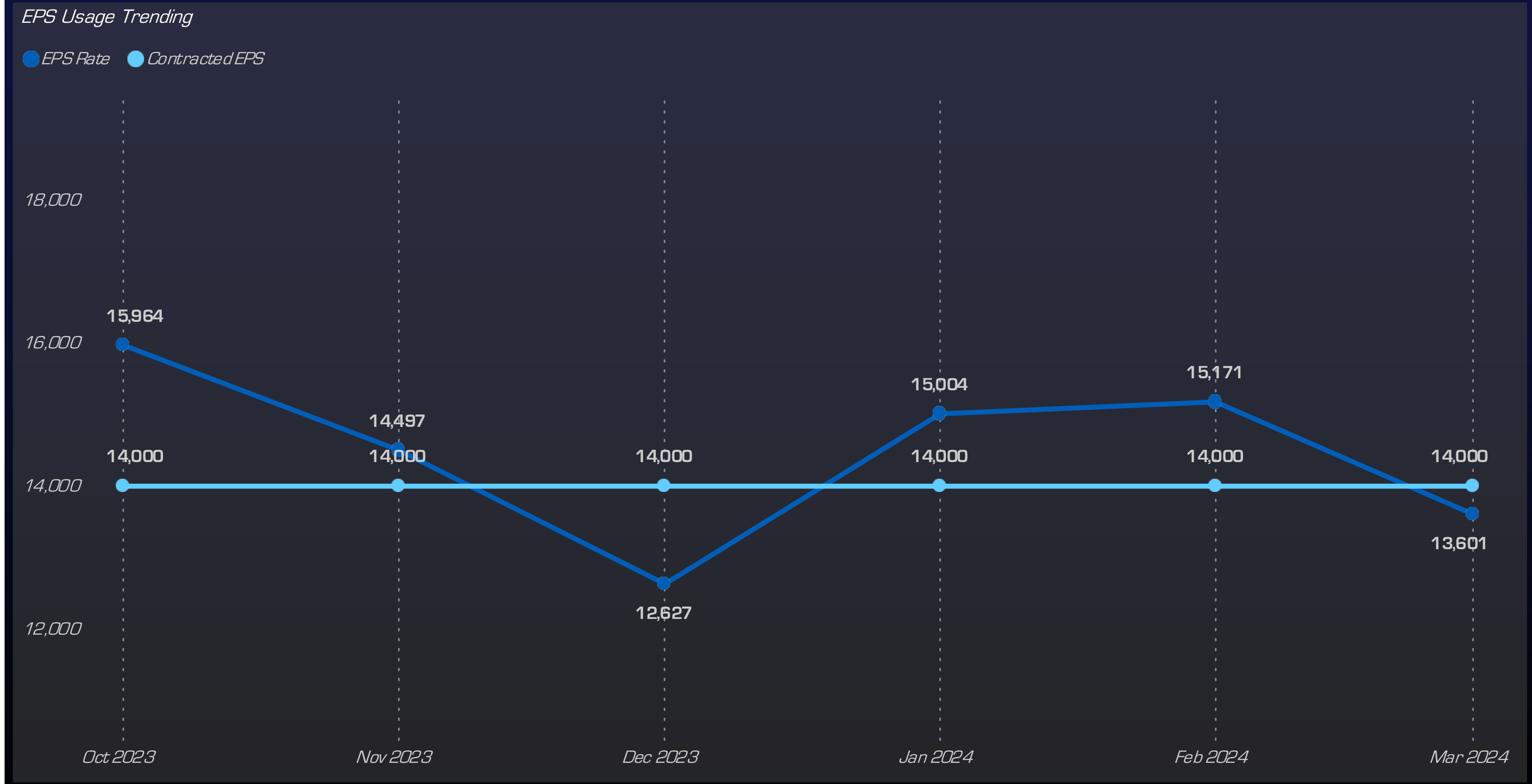
EDR Coverage

856
Current EDR

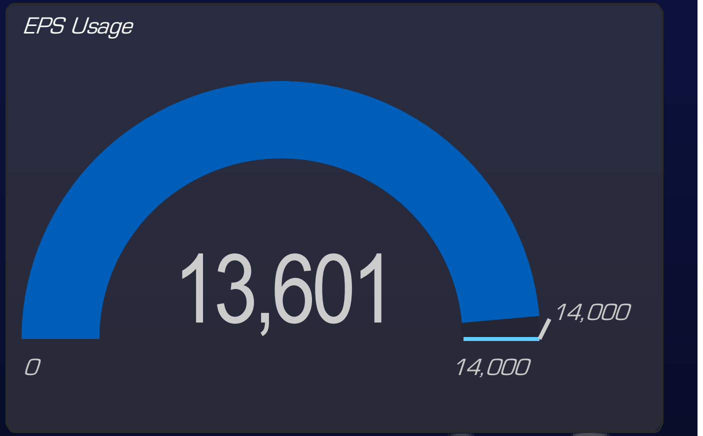
1,100
Contracted EDR

February 15, 2021
Monitoring Start Date

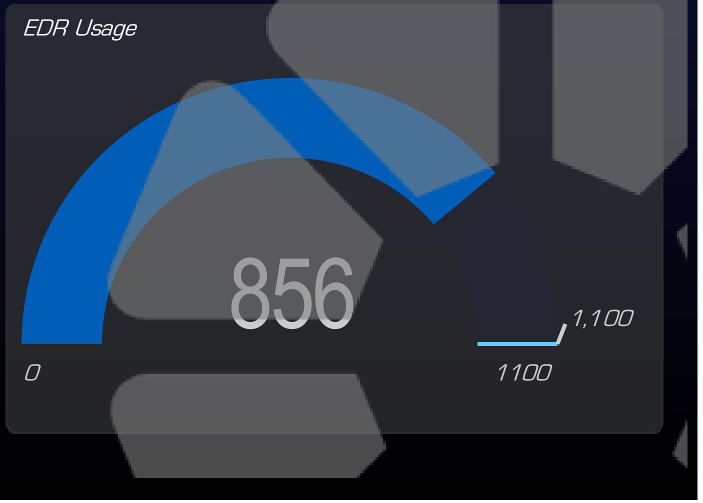
EPS Usage Trending



EPS Usage



EDR Usage



Incident Cases Statistics (Reporting Period)

137
Closed Cases

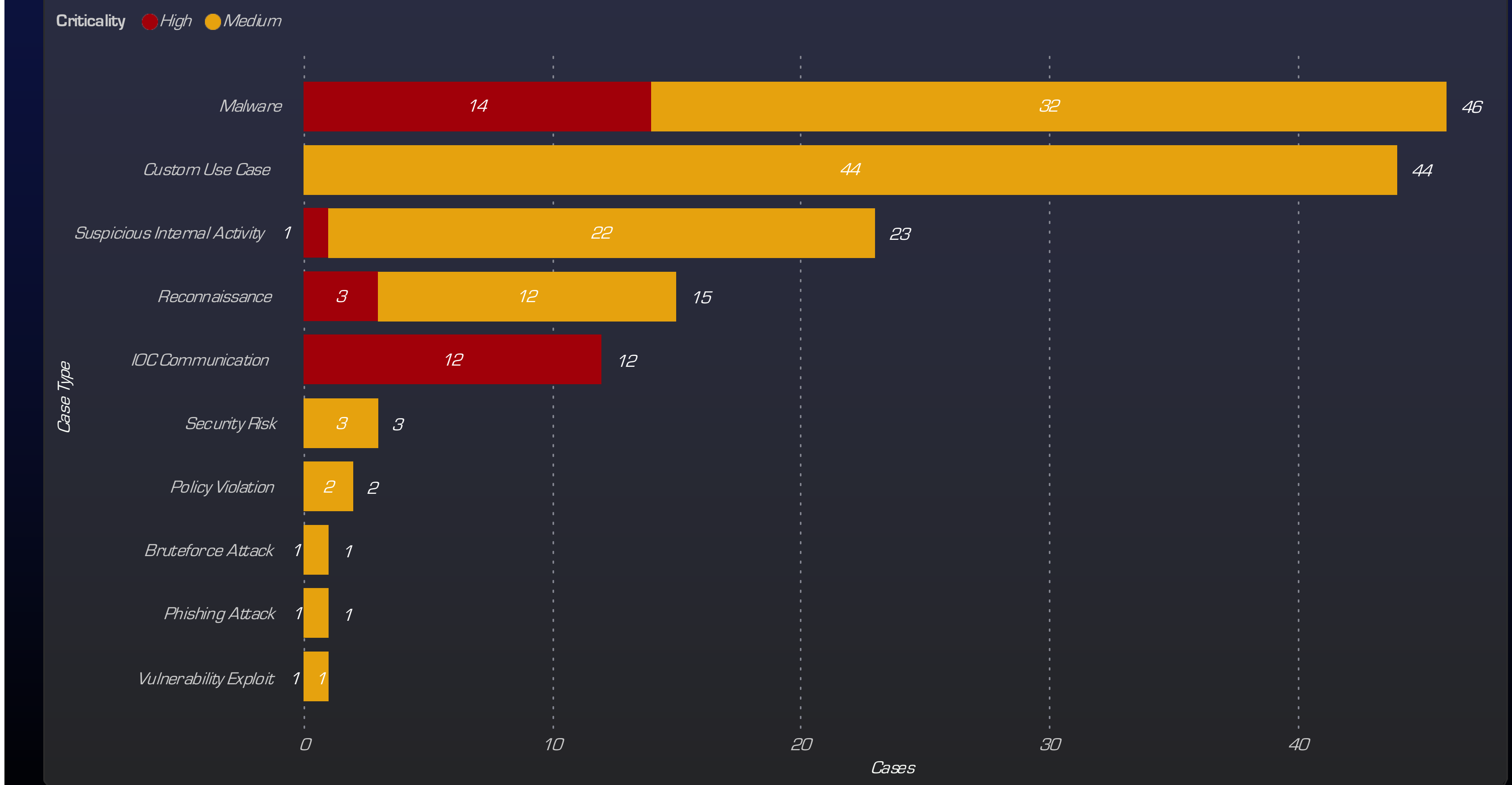
11
Handled Cases

0
Unhandled Cases

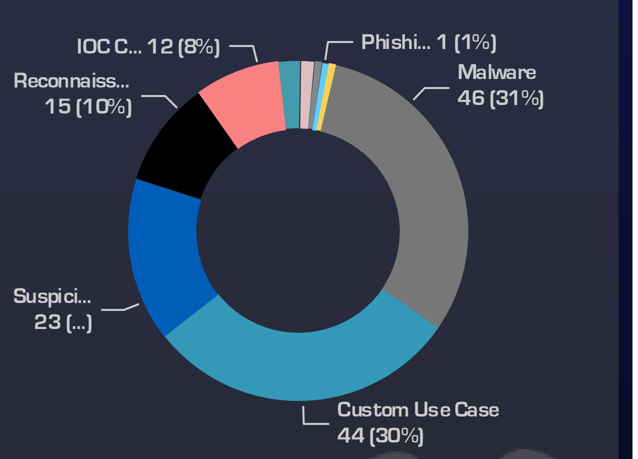
3
Open High Cases

148
Created Cases

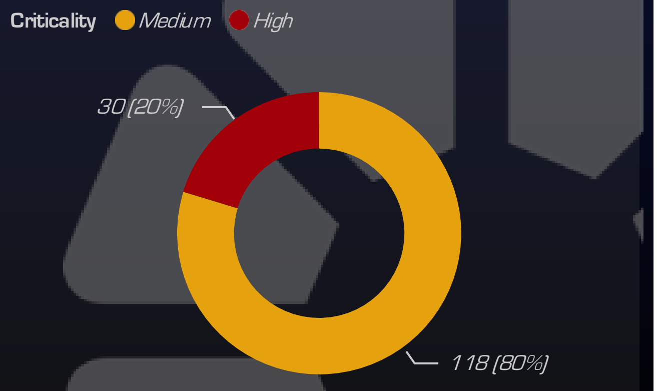
Cases by Case Type and Criticality



Incident Categories



Incident Criticality



Custom Use Cases Statistics (Reporting Period)

43
Closed Cases

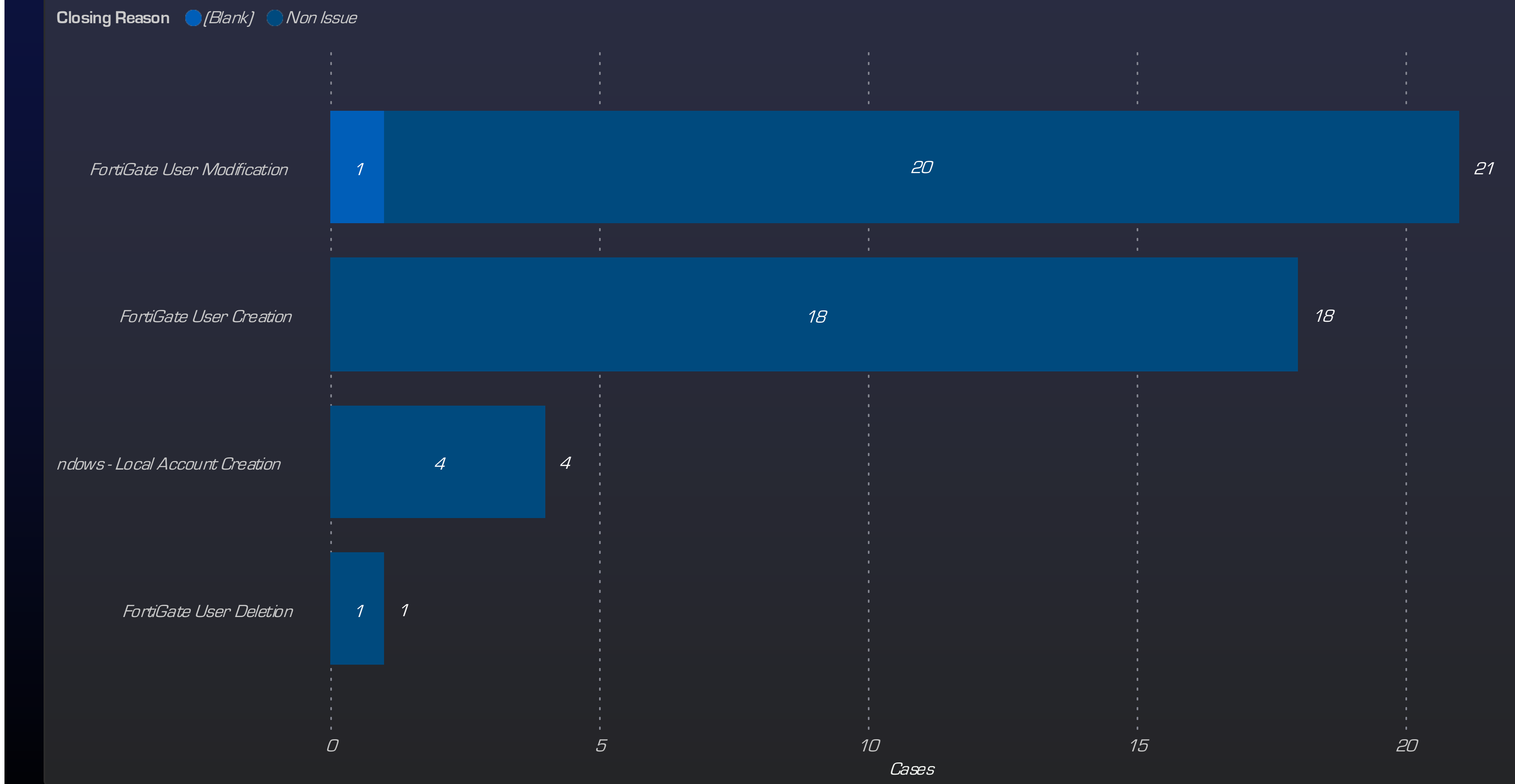
1
Handled Cases

0
Unhandled Cases

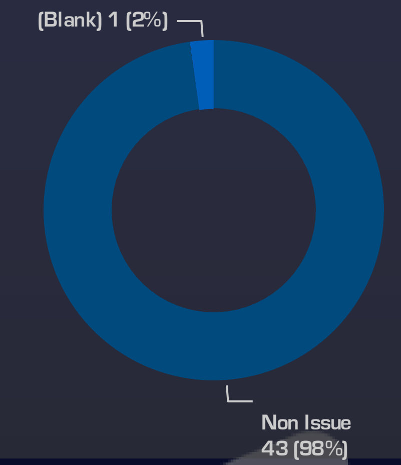
0
Open High Cases

44
Created Cases

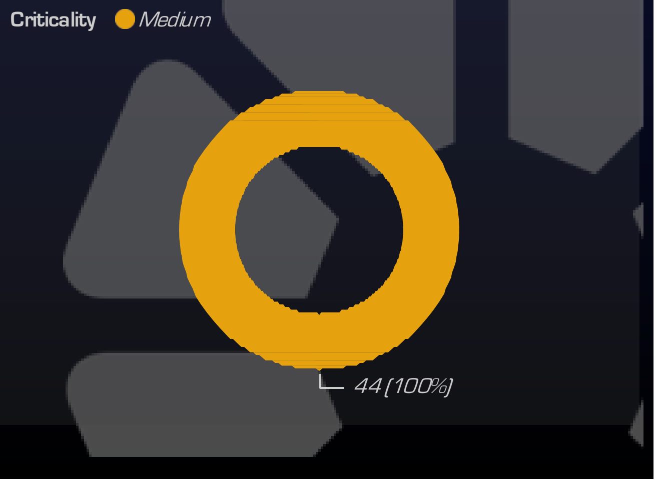
Use Cases and Closing Reason

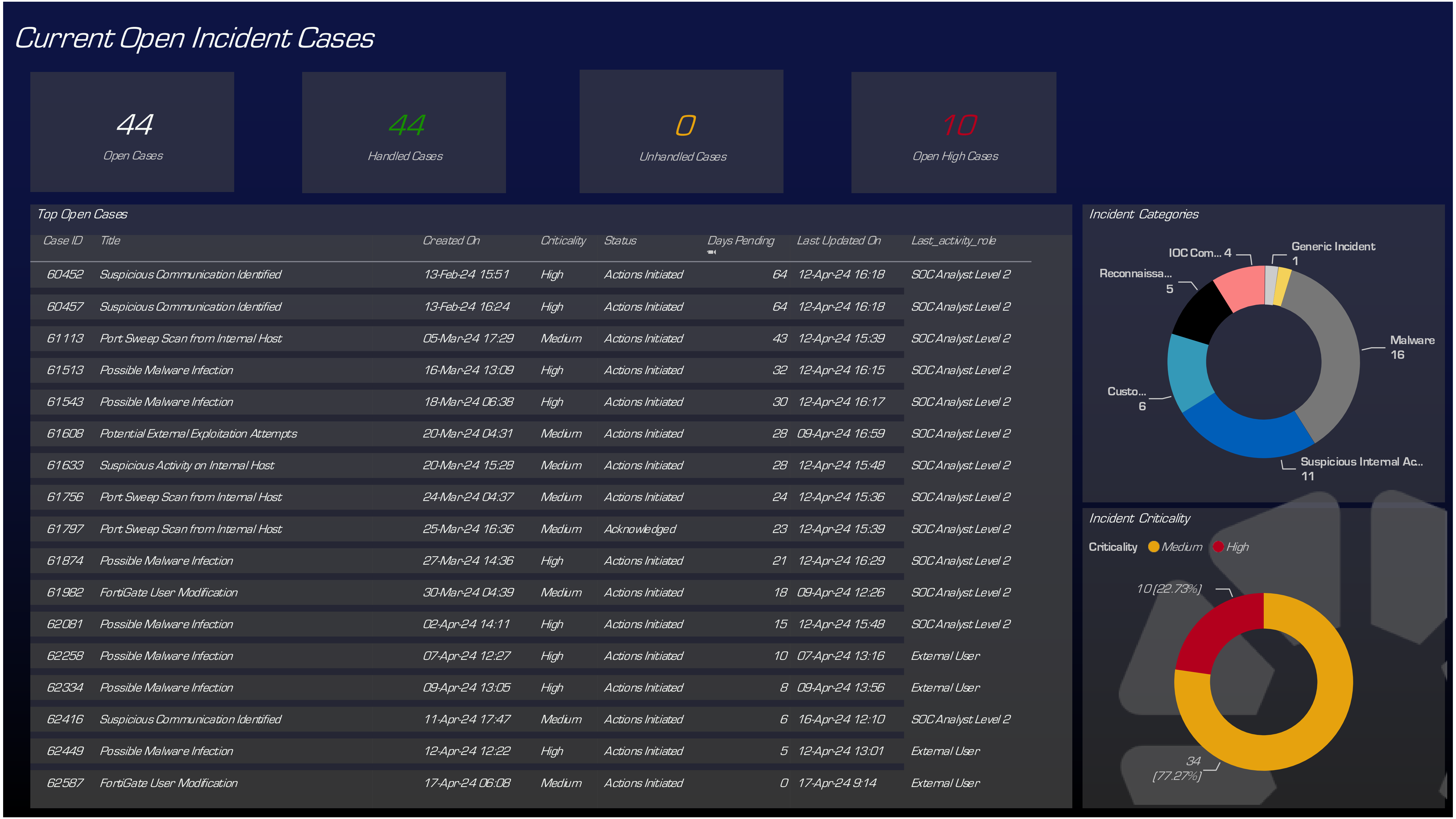


Closing Reason



Incident Criticality





Current Open Incident Cases

44	44	0	10
Open Cases	Handled Cases	Unhandled Cases	Open High Cases

Top Open Cases

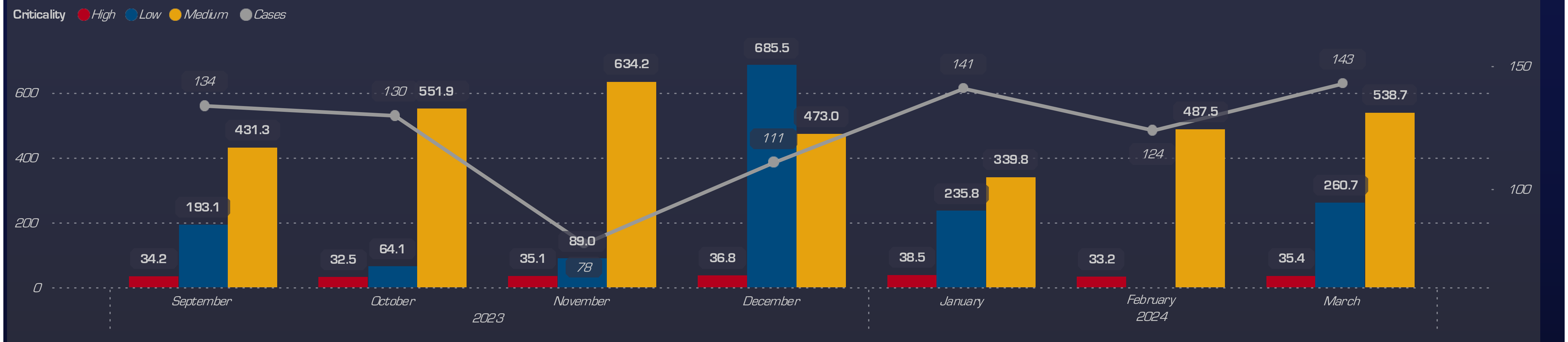
Case ID	Title	Created On	Criticality	Status	Days Pending	Last Updated On	Last_activity_role
60452	Suspicious Communication Identified	13-Feb-24 15:51	High	Actions Initiated	64	12-Apr-24 16:18	SOC Analyst Level 2
60457	Suspicious Communication Identified	13-Feb-24 16:24	High	Actions Initiated	64	12-Apr-24 16:18	SOC Analyst Level 2
61113	Port Sweep Scan from Internal Host	05-Mar-24 17:29	Medium	Actions Initiated	43	12-Apr-24 15:39	SOC Analyst Level 2
61513	Possible Malware Infection	16-Mar-24 13:09	High	Actions Initiated	32	12-Apr-24 16:15	SOC Analyst Level 2
61543	Possible Malware Infection	18-Mar-24 06:38	High	Actions Initiated	30	12-Apr-24 16:17	SOC Analyst Level 2
61608	Potential External Exploitation Attempts	20-Mar-24 04:31	Medium	Actions Initiated	28	09-Apr-24 16:59	SOC Analyst Level 2
61633	Suspicious Activity on Internal Host	20-Mar-24 15:28	Medium	Actions Initiated	28	12-Apr-24 15:48	SOC Analyst Level 2
61756	Port Sweep Scan from Internal Host	24-Mar-24 04:37	Medium	Actions Initiated	24	12-Apr-24 15:36	SOC Analyst Level 2
61797	Port Sweep Scan from Internal Host	25-Mar-24 16:36	Medium	Acknowledged	23	12-Apr-24 15:39	SOC Analyst Level 2
61874	Possible Malware Infection	27-Mar-24 14:36	High	Actions Initiated	21	12-Apr-24 16:29	SOC Analyst Level 2
61982	FortiGate User Modification	30-Mar-24 04:39	Medium	Actions Initiated	18	09-Apr-24 12:26	SOC Analyst Level 2
62081	Possible Malware Infection	02-Apr-24 14:11	High	Actions Initiated	15	12-Apr-24 15:48	SOC Analyst Level 2
62258	Possible Malware Infection	07-Apr-24 12:27	High	Actions Initiated	10	07-Apr-24 13:16	External User
62334	Possible Malware Infection	09-Apr-24 13:05	High	Actions Initiated	8	09-Apr-24 13:56	External User
62416	Suspicious Communication Identified	11-Apr-24 17:47	Medium	Actions Initiated	6	16-Apr-24 12:10	SOC Analyst Level 2
62449	Possible Malware Infection	12-Apr-24 12:22	High	Actions Initiated	5	12-Apr-24 13:01	External User
62587	FortiGate User Modification	17-Apr-24 06:08	Medium	Actions Initiated	0	17-Apr-24 9:14	External User

Incident Categories

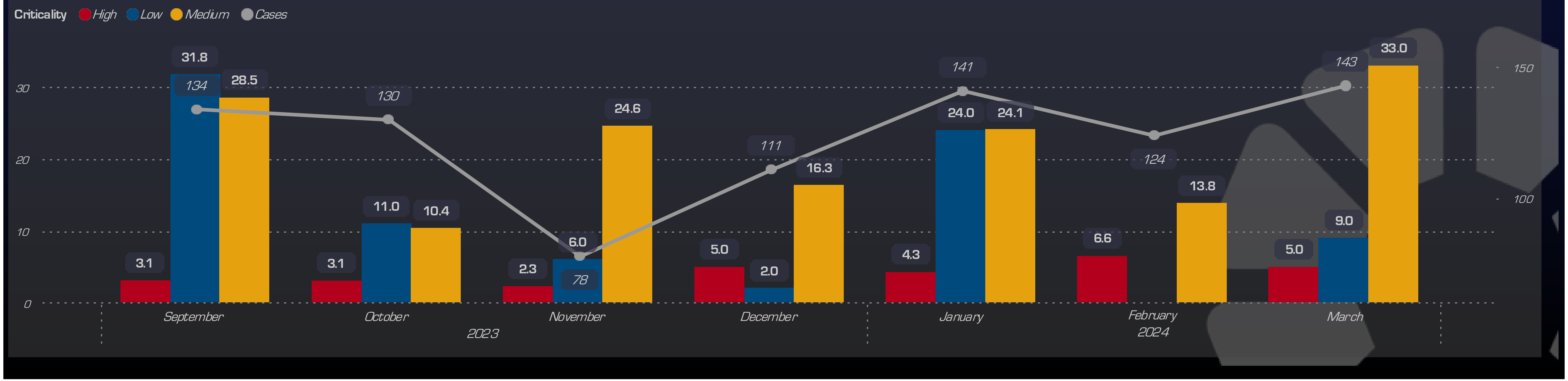
Incident Criticality

SOC Performance Metrics

Mean Time to Report (in minutes)



Mean Time to Acknowledge (in minutes)



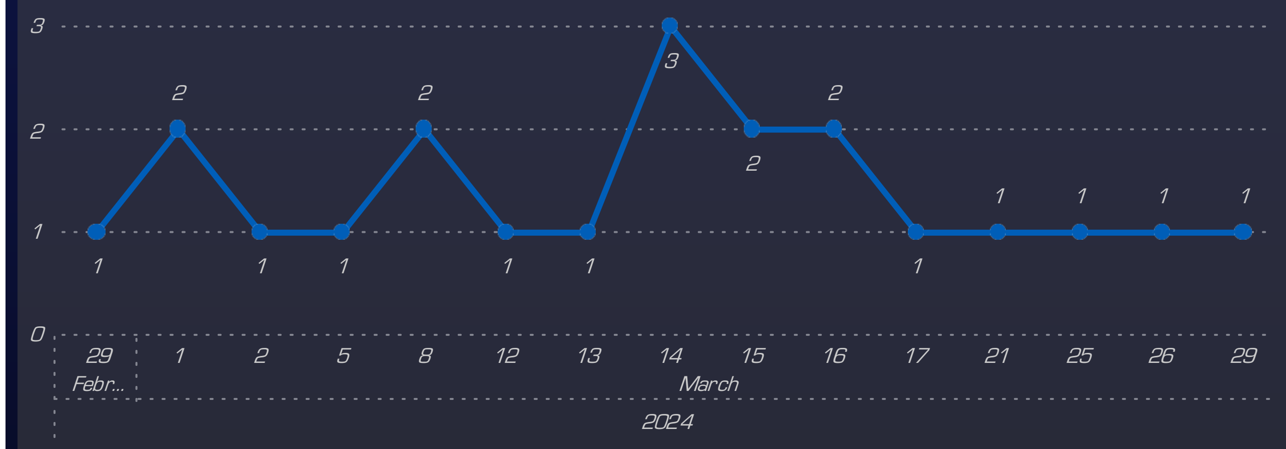
Ticket Metrics

813
Total Created Tickets

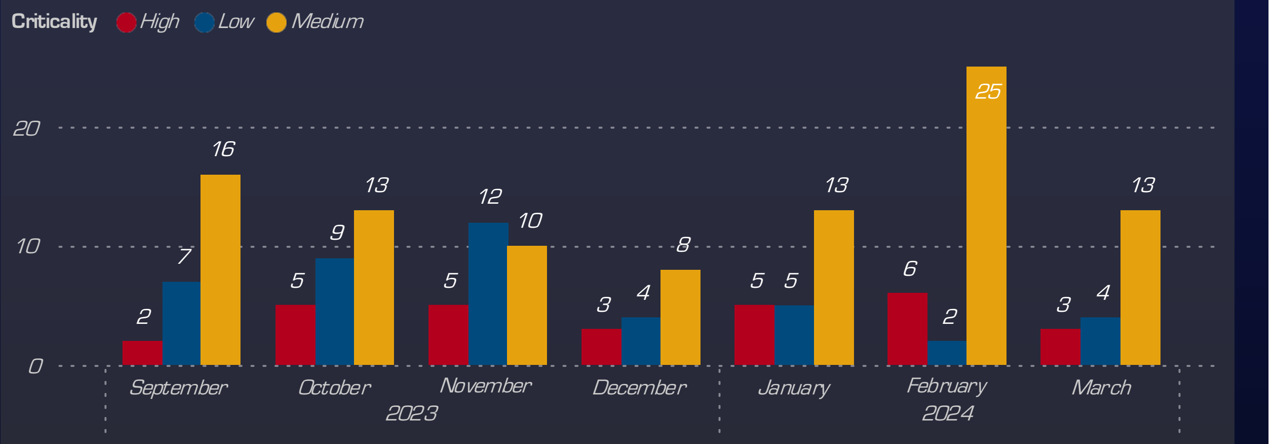
21
Tickets Created (Reporting Period)

28
Current Open Tickets

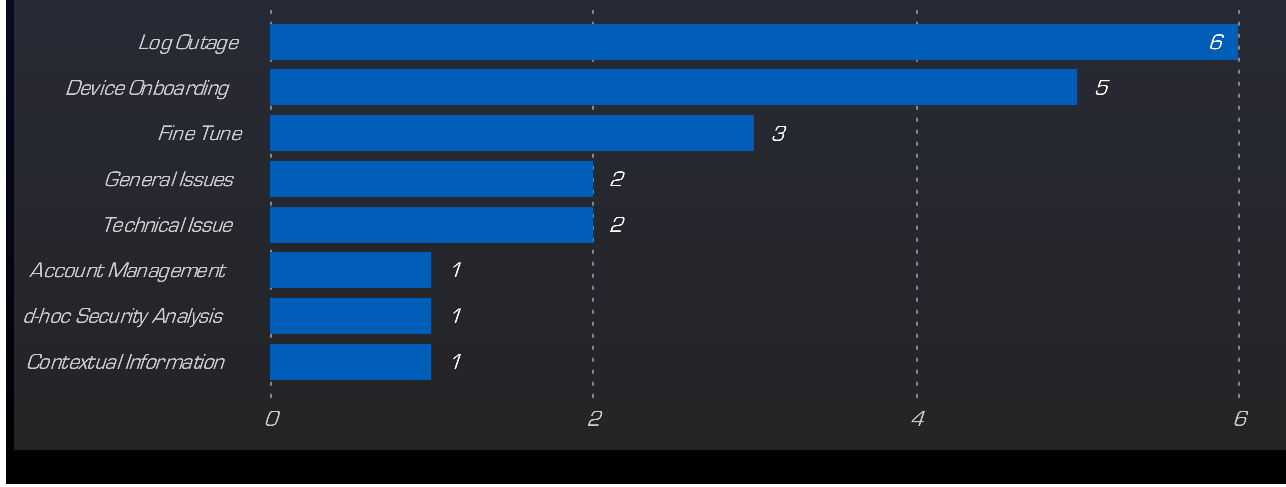
Tickets per Day



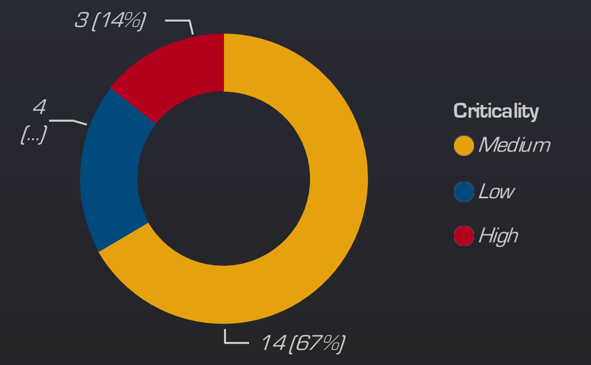
Tickets per Month



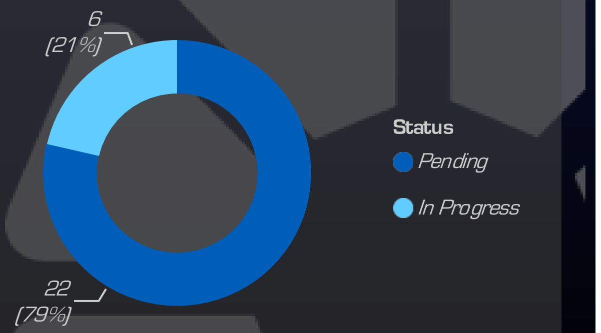
Ticket Types (Reporting Period)



Tickets per Criticality (Reporting Period)



Open Tickets Status



Intel Updates for Germany and Industrial Goods & Services

Last Active	Primary Tag	Primary Tag Type	Threat Level	Activity Level	Threat Level Reason	Summary
16-Apr-24 17:10	ALPHV	SPECIFIC_TTP	HIGH	RECENT	ALPHV is a sophisticated and persistent ransomware group whose attacks can inflict significant damage on organizations, crippling critical functions and leading to significant financial losses. The impact of these attacks extends beyond single companies to potentially affect numerous users and organizations, given the sensitive nature of the data compromised. Although the group may have ceased operations, its affiliates likely remain a substantial threat, as they transition to other ransomware activities.	ALPHV, also known as BlackCat, AlphaV, and AlphaVM, is a ransomware-as-a-service (RaaS) operation active since November 2021. It is notably the first group to deploy ransomware written in Rust. The group gained notoriety for its triple extortion tactics, which include deploying ransomware, exfiltrating data, and conducting DDoS attacks, as well as its unique extortion tactics, including reporting victims to the SEC.
16-Apr-24 15:30	Akira	SPECIFIC_TTP	HIGH	VERY	The Akira ransomware group represents a high-level threat, particularly due to its ability to adapt and employ sophisticated techniques such as SQL database manipulation, firewall deactivation, and the exploitation of legitimate remote-access tools. Its targeted attacks on varied business sectors with sensitive information underscore its continued potential for significant disruption and data compromise.	Akira is a ransomware group that was first discovered in March 2023 and targets corporate networks primarily in North America, in various sectors, including education, finance and insurance, real estate, manufacturing, and business consulting. The group practices double extortion, exfiltrating data before encrypting the devices of the compromised entities to demand a ransom. The group has compromised has also been linked with the now-disbanded Russian "Conti" ransomware operation.
16-Apr-24 15:30	LockBit	SPECIFIC_TTP	HIGH	VERY	LockBit poses a high threat due to its double extortion tactic, sophisticated evasion techniques, and continuous evolution. Its adaptability and targeting of critical sectors underline the significant security and financial risks it presents. Despite the temporary setback from Operation Cronos, LockBit swiftly resumed its operations by launching a new data leak site and still poses a high threat.	Since its discovery in September 2019, LockBit ransomware has evolved into a sophisticated ransomware-as-a-service (RaaS) operation, known for its double extortion tactic of stealing data before encrypting it and threatening to publish the data if ransoms are not paid. Continuously developing new variants to target various operating systems, LockBit primarily targets global entities within the government, healthcare, financial services, and industrial sectors, employing methods like brute force attacks and exploiting vulnerabilities. Over the years, LockBit has remained one of the most active and formidable ransomware groups.
16-Apr-24 15:30	Play	SPECIFIC_TTP	HIGH	VERY	The threat from Play ransomware is regarded as high. Its operators are technically proficient and favor vulnerability exploitation, as well as phishing, to gain initial access.	The Play (aka PlayCrypt) ransomware group was first observed using its eponymous ransomware in June 2022. The group uses the double extortion technique: exfiltrating data before encryption to post on the group's data-leak site if a ransom is not paid.

OBRELA

THANK YOU

London | Athens | Dubai | Frankfurt | Riyadh

www.obrela.com