Security Incident & Threat Management Report

INTERVAL between Nov 01, 2020 05:00AM (UTC) and Dec 01, 2020 06:00AM (UTC)
SUBSCRIBER: YOUR ORGANIZATION

1 TERMINOLOGY

TERM	DEFINITION
SIEM	Security Information and Event Management technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. (a)
Event	Any observable occurrence in a network or system. (b)
Incident	A violation or imminent threat of violation of computer security policy, acceptable use policy, or standard security practices. (b)
Detection	The process of identifying the presence of potential suspicious or malicious activities.
Triage	A phase in the security incident response process where the security analyst defines if the event is related to the detection, characterizes a valid detection, or detects a false-positive.
Investigation	A phase in the security incident response process where the security analyst investigates the events related to the detection in order to provide, if necessary, further information about the potential incident and the recommended remediation action(s).

References:
(a) Gartner http://www.gartner.com/it-glossary/security-information-and-event-management-siem/
(b) NIST http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2 PURPOSE AND AUDIENCE

2.1 PURPOSE

The purpose of this report is to provide the stakeholders with a visual representation of the organization's security posture. This report also helps the stakeholders in charge of Information Security Management Systems (ISMS) to understand the main security incidents and their corresponding status.

2.2 AUDIENCE

Executives, management team, auditors, and technical staff who oversee technology implementation, operation, and maintenance team may leverage this report in order to understand the threat landscape of their organization.

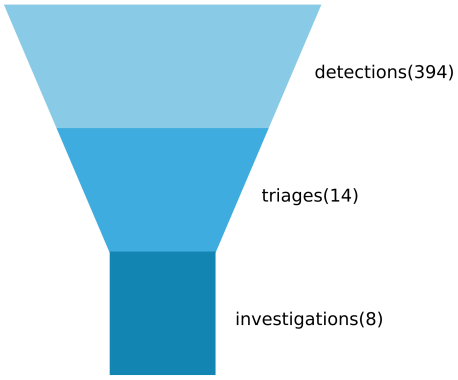
3 EXECUTIVE SUMMARY

This report includes information related to events collected from in-scope monitored devices (Appendix A) between **Nov 01, 2020 05:00AM (UTC)** and **Dec 01, 2020 06:00AM (UTC)**. The SIEM platform received a total of **18,797,323** events and generates a total of **394** detections. Of these **394** detections, **14** were converted into triage tickets. Upon triage of these **14** tickets, **8** were flagged for further investigation by analysts at our Security Operations Center. Out of these **8** investigation tickets, **0** were regarded as high severity incidents (**0%**). Over the duration of this time interval, **8** investigations tickets were opened and **9** were closed.

4 GRAPHS AND CHARTS

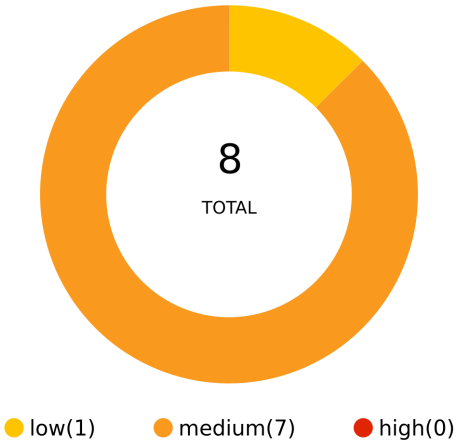
4.1 INCIDENT FUNNEL

The funnel illustrates how the detections sent by the SIEM platform are converted into relevant investigation tickets after the triage and investigation activities are performed by the Security Operations Center.



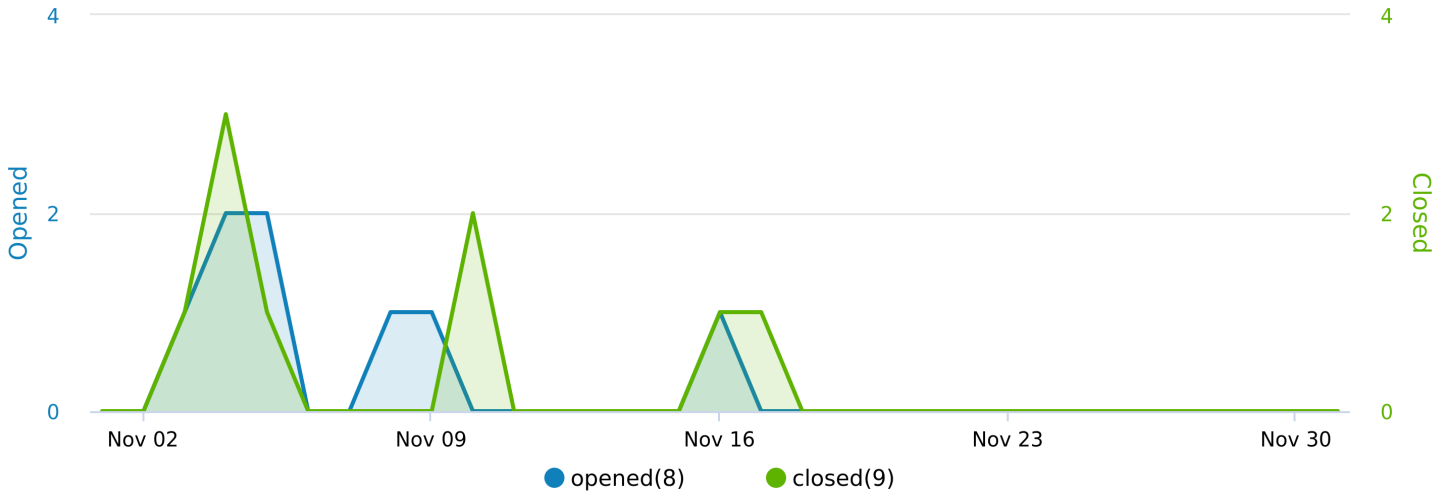
4.2 INVESTIGATIONS BY SEVERITY

This graph displays the total number of investigation tickets by severity. **0** security incidents were high or critical. There were **1** low and **7** medium security incidents.



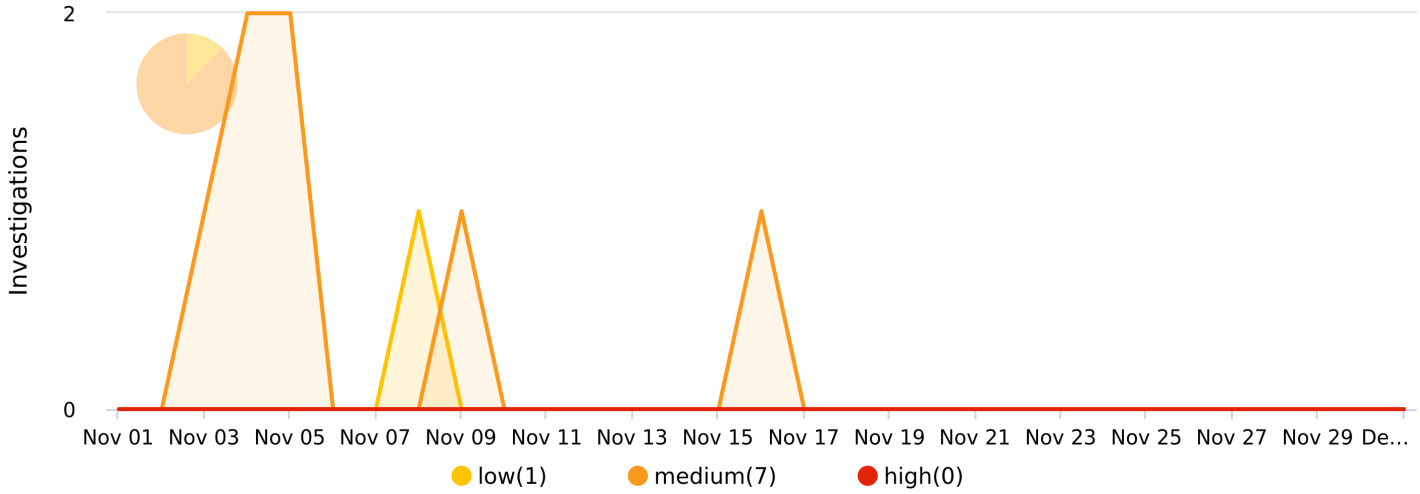
4.3 INVESTIGATIONS OVER TIME

The graph below displays the disposition between opened investigation tickets and closed investigation tickets over time. Over the duration of this time interval, **8** investigations tickets were opened and **9** were closed.


4
2
0
Opened
4
2
0
Closed
Nov 02
Nov 09
Nov 16
Nov 23
Nov 30
opened(8)
closed(9)

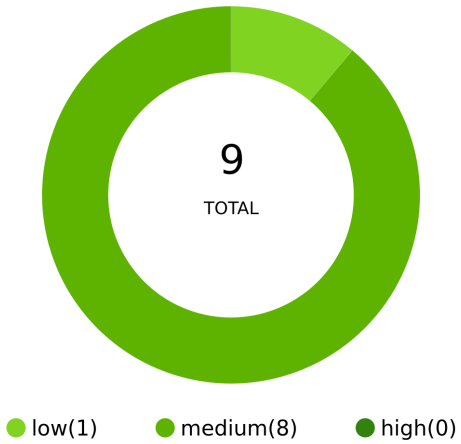
4.4 INVESTIGATIONS BY SEVERITY OVER TIME

This graph displays the number of investigation tickets by severity over time.



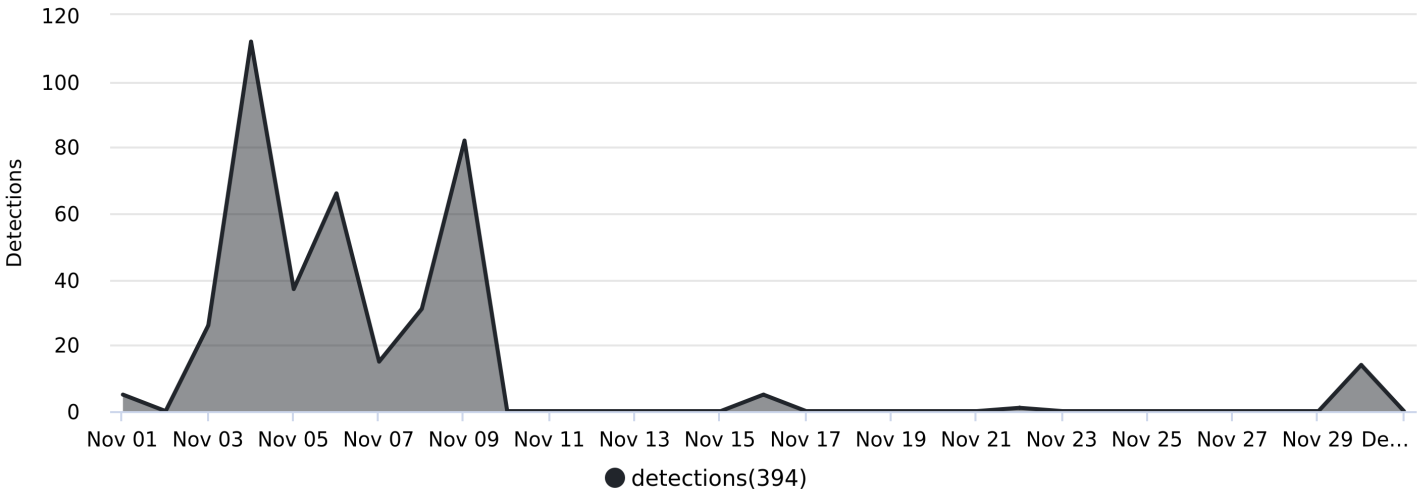
4.5 CLOSED INVESTIGATIONS

This graph shows the number investigation tickets by severity closed between **Nov 01, 2020 05:00AM (UTC)** and **Dec 01, 2020 06:00AM (UTC)**. Out of **9** investigations tickets closed, **0** were related to high severity incidents (**0%**).



4.6 DETECTIONS

This graph displays the number of detections performed by the SIEM platform over time.


120
100
80
60
40
20
0
Detections
Nov 01
Nov 03
Nov 05
Nov 07
Nov 09
Nov 11
Nov 13
Nov 15
Nov 17
Nov 19
Nov 21
Nov 23
Nov 25
Nov 27
Nov 29
De...
detections(394)

4.7 TOP 5 INVESTIGATIONS

This table contains the Top 5 most frequent detections sent by the SIEM platform. A total of **394** detections were sent by the SIEM platform between **Nov 01, 2020 05:00AM (UTC)** and **Dec 01, 2020 06:00AM (UTC)**.

	Subject	Counts
	Data exfiltration	7
	Threat Sensor operational incident	1

4.8 WORK IN PROGRESS

The following tickets are currently being worked on by the Managed Service Provider’s staff in collaboration with system owners.

#ID	Subject	Open date

The data have not been found.

5 APPENDIX A

5.1 MONITORED INFRASTRUCTURE DEVICES

Host Name	IP Address	Type	Vendor	Model/Edition
Firewall	X.X.X.X	Firewall	Fortinet	FG 300E
AD-Controller-1	X.X.X.X	Directory Service	Microsoft	Windows Server 2016 Standard
AD-Controller-2	X.X.X.X	Directory Service	Microsoft	Windows Server 2016 Standard

5.2 MONITORED ENDPOINT DEVICES

Host Name	Vendor	Model/Edition
The data have not been found.		

5.3 MONITORED OFFICE 365 USERS

First name	Last name	Email
The data have not been found.		