

Summary Report

Time Filter:

August 5, 2021 12:00 AM - August 6, 2021 12:00 AM

Computer Filter:

All Computers

Tag Filter:

All

Generated By:

MasterAdmin

Generated On:






August 6, 2021 8:30 AM

Summary

Managed Computers:	16
Alerts Raised:	12
Malware Detections:	0
Uncleanable Malware:	0
Web Reputation Events:	0
Firewall Events (Prevent Mode):	0
Firewall Events (Detect Mode):	0
Scans Detected by Reconnaissance:	0
Intrusion Prevention Events (Prevent Mode):	0
Intrusion Prevention Events (Detect Mode):	0
Integrity Monitoring Events:	108
Log Inspection Events:	15036
System Events:	261

Event Statistics

Top 5 Alerts

Number of Alerts	Alert
4 (33.3%)	 New Pattern Update is Downloaded and Available
3 (25%)	 Anti-Malware Component Update Failed
2 (16.7%)	 Smart Protection Server Connection Failed
1 (8.3%)	 CPU Critical Threshold Exceeded
1 (8.3%)	 Memory Critical Threshold Exceeded

Top 5 Infected Computers

# of Events	Computer
No Information	

Top 5 Malware

# of Events	Malware
No Information	

Top 5 Web Reputation URLs

# of Events	URL
No Information	

Top 5 Firewall Events (Prevent Mode)

# of Events	Rule
No Information	

Top 5 Firewall Events (Detect Mode)

# of Events	Rule
No Information	

Top 5 Scans Detected by Reconnaissance

# of Events	Rule
No Information	




Top 5 Intrusion Prevention Events (Prevent Mode)

# of Events	Rule
No Information	

Top 5 Intrusion Prevention Events (Detect Mode)



# of Events	Rule
No Information	

Top 5 Integrity Monitoring Events






# of Events	Rule
54 (50%)	 1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
51 (47.2%)	 1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
3 (2.8%)	 1008720 - Users and Groups - Create and Delete Activity (ATT&CK T1136)

Top 5 Log Inspection Events

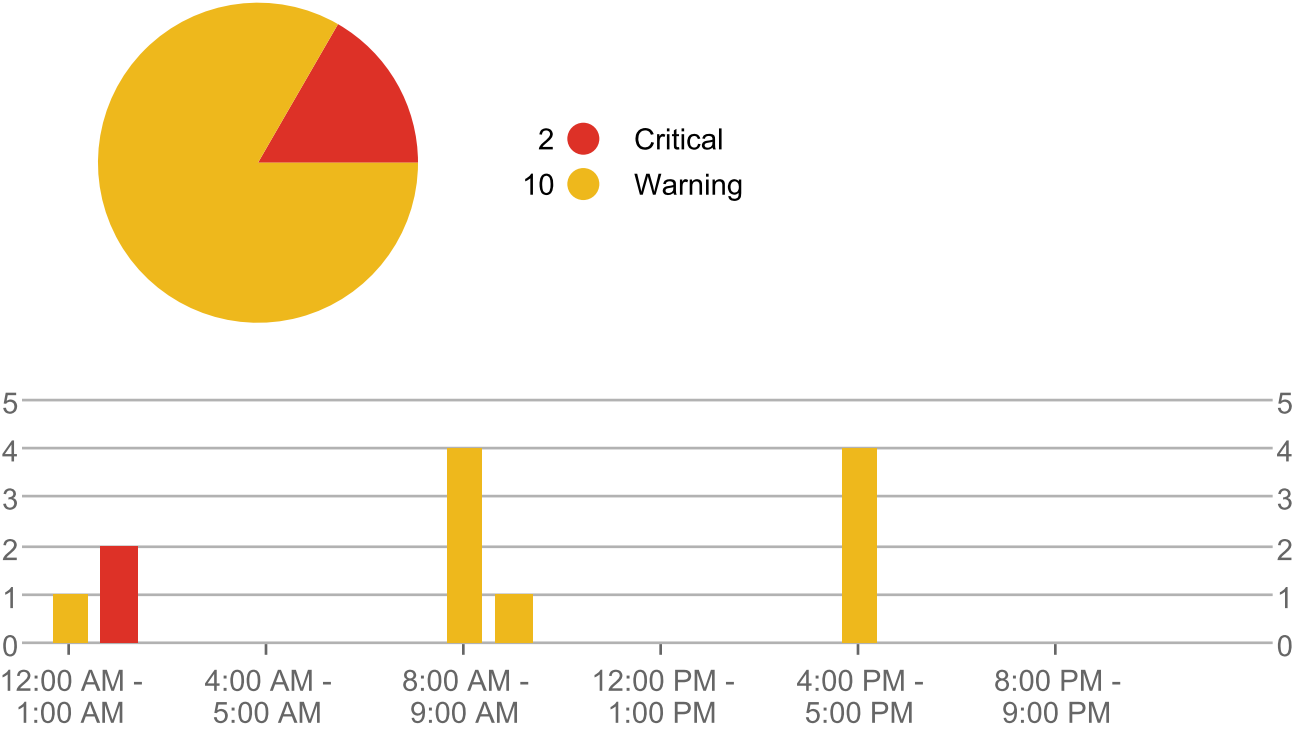
# of Events	Rule
-------------	------

12,787 (85%)	 1004057 - Microsoft Windows Security Events - 1
1,125 (7.5%)	 1002795 - Microsoft Windows Events
1,103 (7.3%)	 1003987 - Microsoft Windows Security Events - 2
13 (0.1%)	 1004488 - Database Server - Microsoft SQL
7 (0%)	 User created

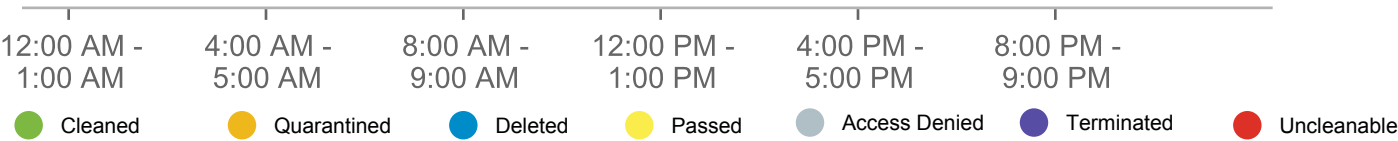
Top 5 System Events

# of Events	Event
44 (16.9%)	 Smart Protection Server Connected for Smart Scan
29 (11.1%)	 Events Retrieved
18 (6.9%)	 Scheduled Task Started
18 (6.9%)	 Alert Emails Sent
16 (6.1%)	 Computer Updated

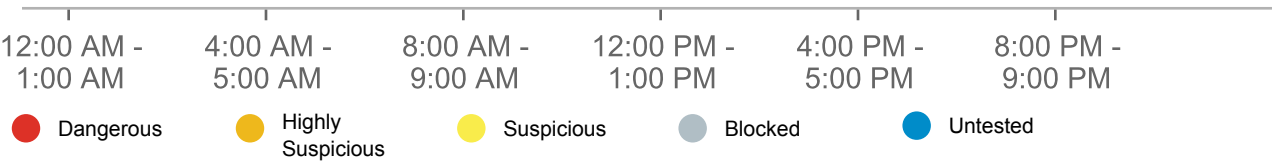
Alerts



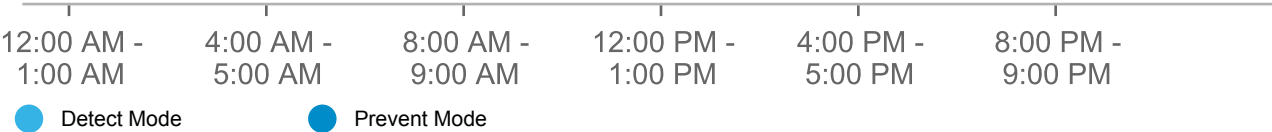
Anti-Malware Event History



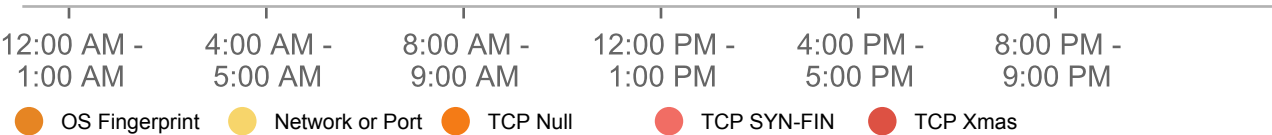
Web Reputation Event History



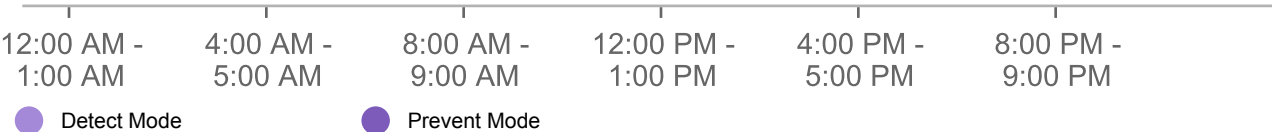
Firewall Event History



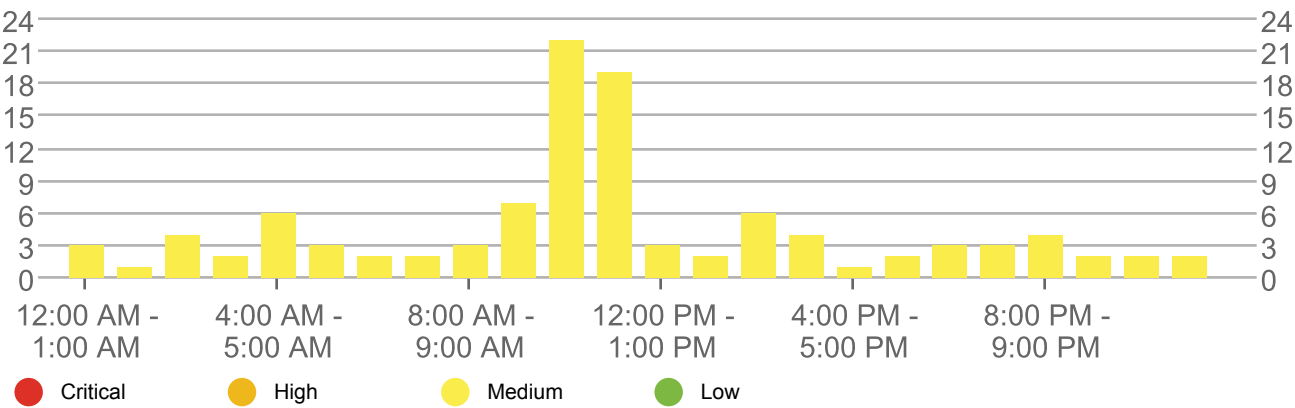
Reconnaissance History



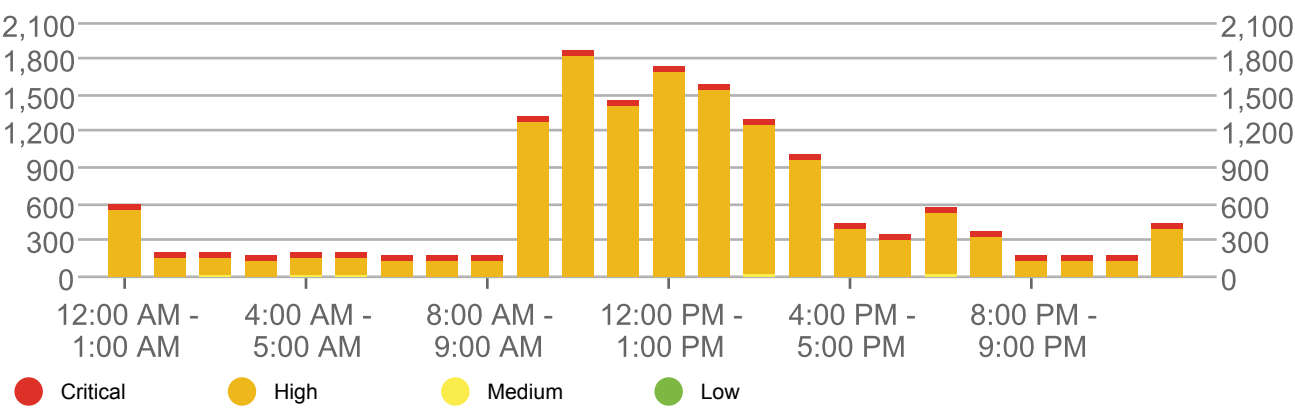
Intrusion Prevention Event History



Integrity Monitoring Event History



Log Inspection History



System Events

