Network Threat Report
CyberScore for Acme Corporation

Report generated on May 20, 2024

Read more about how to interpret this report →

Cyber Score

A cyber score of 612 or higher is your target based on other ThreatSync+ NDR users.

Continued use of ThreatSync+ NDR is aimed at improving your CyberScore and securing your critical IT devices. ThreatSync+ NDR identifies, detects, and responds to threats to your network without requiring any additional hardware, software or people. The ThreatSync+ NDR Cloud continuously analyzes the billions of conversations happening on your network, learns what is normal, and alerts when suspicious behaviors that users risk the security of your critical IT devices are detected.

Time Period

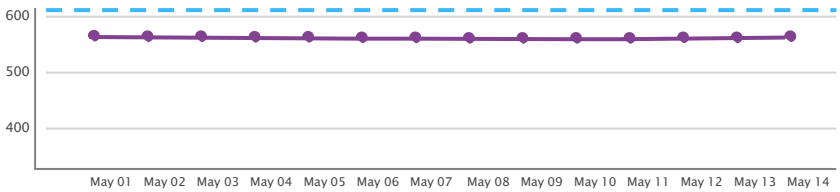
From:	MAY 01, 2024
To:	MAY 14, 2024
Generated:	MAY 20, 2024
Period:	14 Days

Legend

Target Cyber Score

No data available

Cyber Score History



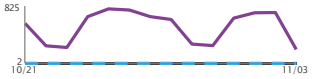
Threat Detection Summary

CYBER SCORE	SUMMARY	DESCRIPTION	14 DAY HISTORY
A	**Open Smart Alerts** 0 currently open	Smart Alerts are ThreatSync+ NDR' highest - priority alerts. They highlight potential active attack behavior.	
A	**Average Time to Close Smart Alerts** 0.0 Days (Using a trailing 7-day average)	Smart Alerts represent possible active attacks, investigating and closing them promptly is an important part of your organization's security process.	
A	**Detected Smart Alerts** 0 Smart Alerts	Smart Alerts represent possible active attacks. As ThreatSync+ NDR learns and vulnerabilities are addressed, you should see the total volume of smart alerts decrease. This metric counts the number of smart alerts were created or updated each day.	
A	**Log Collection Uptime** No active collectors and log agents available	ThreatSync+ NDR is only able to protect your network when collectors are receiving logs. Gaps in collection are a vulnerability.	

Network Visibility Summary

CYBER SCORE	SUMMARY	DESCRIPTION	14 DAY HISTORY
F	**Unidentified Devices** 75.0%	Unidentified Devices have not yet been labeled and rated in ThreatSync+ NDR. Labels and importance ratings help ThreatSync+ NDR highlight the threats that are most critical to you.	
A	**High Risk Devices** 0.0%	ThreatSync+ NDR identifies devices that are most likely to be the target of threatening behavior.	
A	**Unidentified Subnets or IP Ranges** 0.0%	Unidentified Subnets have not yet been labeled in ThreatSync+ NDR. Labels help ThreatSync+ NDR highlight known networks and identify new or rogue networks.	

Policy Assurance Summary

CYBER SCORE	SUMMARY	DESCRIPTION	14 DAY HISTORY
F	**Policy Alerts** 1152.1 Per day (Average of past 7 days)	Policy Alerts allow you to detect violations of your enterprise access policies, selected from pre-built policy definitions or custom-built by you.	

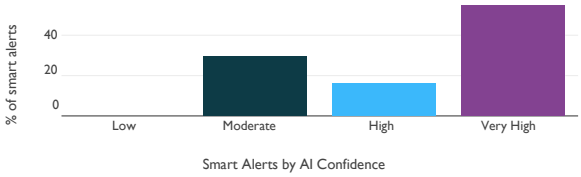
Threat Detection Detail

C

Open Smart Alerts

8 currently open.

Having less than 5 open alerts at any given time is a good indicator that you are addressing detected threats in a timely manner.



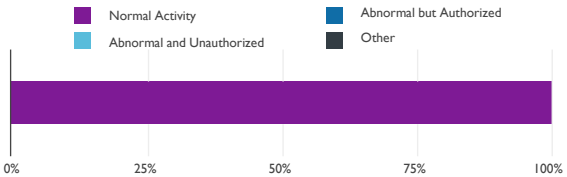
Smart Alerts by AI Confidence

F

Average Time to Close Smart Alerts

6.0 Days (Using a trailing 7-day average)

An average time to close of less than 2 days indicatesthat you are taking a proactive approach to assessing and remediating threats and vulnerabilities.



C

Detected Smart Alerts

Summary of Smart Alerts detected in your network during this report period.

SMART ALERT TYPE	COUNT	MAJOR ACTORS	TIME LAST TRIGGERED
Suspicious Tunneling Plus Port Scan	9	MMN-PCC-01.acme.com, PCC-PROBE-01.acme.com ,C-01.acme.com, TRD-C40500F.acme.com, PH.CAM.OT.acme.com, C-01.eu.acme.com	05/06/2024 @ 23:00:00 UTC
Probing or Reconnaissance Activity	3	10.10.10.10, 10.10.10.00, DC-02	05/06/2024 @ 23:00:00 UTC
RDP Tunneling Activity	1	USNBL-ESSUR-01	05/06/2024 @ 08:36:20 UTC
Internal to External Probing or Reconnaissance Activity	0	No threats of this type detected in your network	
Peer to Peer Exfiltration	0	No threats of this type detected in your network	
Suspected Lateral Movement Activity	0	No threats of this type detected in your network	
Suspicious Activity On an Asset	0	No threats of this type detected in your network	
Suspicious Activity On an Untrusted Private IP	0	No threats of this type detected in your network	
Suspicious Endpoint Activity	0	No threats of this type detected in your network	
Suspicious Tunneling Plus Data Exfiltration	0	No threats of this type detected in your network	

A

Log Collection Uptime

Your collectors were up for 100% of the last report period

CyGlass is only able to protect your network while your collectors and log agents are running. We suggest aiming for 99.9% uptime

UPTIME BY COLLECTOR AND LOG AGENT	
OPSAcme02|CAC-01	100.0
OPSAcme03|CAC-02	100.0
OPSAcmes04|CAC-03	100.0
OPSAcme05|CAC-04	100.0
OPSAcme01	100.0

DATA PROCESSED	
Netflow records processed	60,411,925
Events processed	297,001
Logs processed	Netflow

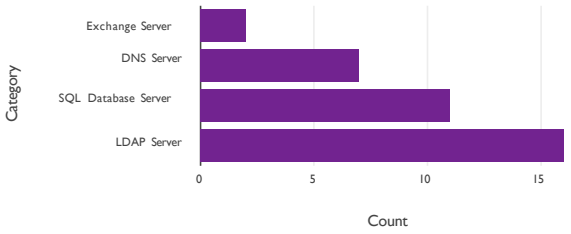
Network Visibility Detail

Unidentified Devices

0.0%

A

Unidentified devices are those that ThreatSync+ NDR sees that you have not labeled and rated. By applying labels and importance ratings, you provide important context for ThreatSync+ NDR in better understanding what threats are most critical. Optimally, there should be no unidentified devices on your network, however, when they are present, you should label them quickly or remediate any rogue ones. Don't let them accumulate. This chart reflects your network at the time of report generation, May 27, 2024.

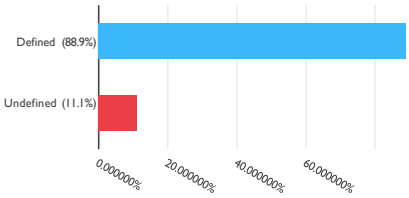


Unidentified Subnets or IP Ranges

11.1%

B

Unidentified subnets are those that have not been labeled in ThreatSync+ NDR. By applying labels, you provide important context to ThreatSync+ NDR in better understanding what threats are most critical to your organization. This chart reflects your network at the time of report generation, May 27, 2024.



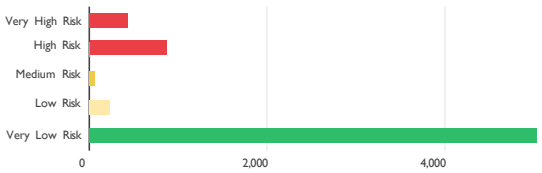
IP START RANGE	ACTIVE IPs	LAST UPDATED
10.100.10.0/0	152	05/06/2024 @ 23:00:00 UTC
10.10.100.0/0	131	05/06/2024 @ 23:00:00 UTC
10.100.100.0/0	123	05/06/2024 @ 23:00:00 UTC
10.100.100.0/0	103	05/06/2024 @ 23:00:00 UTC
10.100.100.0/0	73	05/06/2024 @ 23:00:00 UTC
10.100.100.0/0	67	05/06/2024 @ 23:00:00 UTC
10.100.100.0/0	44	05/06/2024 @ 23:00:00 UTC
10.100.100.0/0	43	05/06/2024 @ 23:00:00 UTC
10.100.100.0/0	41	05/06/2024 @ 23:00:00 UTC
10.10.100.0/0	39	05/06/2024 @ 23:00:00 UTC

High Risk Devices

0 Devices with a Threat Score above 70

A

You know which devices are important to your business. ThreatSync+ NDR knows which devices are most likely the target of threatening behavior. That's how we rate risk. Work to reduce the number of high risk devices to no more than a few by addressing Smart Alerts promptly and protecting your systems against attack. This chart reflects your network at the time of report generation, May 07, 2024.



HIGH RISK DEVICES	THREAT SCORE	ALERT COUNT	ROLE	P ADDRESS
PH.CAM.OT.acme.com	99	1		10.100.100.10C:58:B9:0B:C5:F5, PH.CAM.OT.acme.com
TRD-C40500F.acme.com	94	1		10.100.100.00, TRD-C40500F.acme.com
SRS-L140500.acme.com	92	1		10.100.100.00, SRS-L140500.acme.com,2C:58:0A:9E:0C
SYS-CL@405F.acme.com	88	1		SYS-CL@405F.acme.com 10.100.100.00,28::B0:BD:5F
PH-TD101000L.acme.com	85	1		10.100.100.00, PH-TD101000L.acme.com
TRD-C22000F.acme.com	85	1		10.100.100.00, TRD-C22000F.acme.com

Policy Assurance Detail

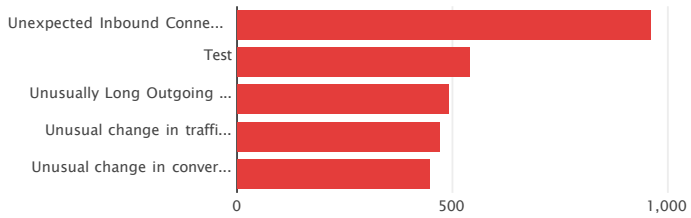
F

Policy Alerts

1152.1 Per day (Average of past 7 days)

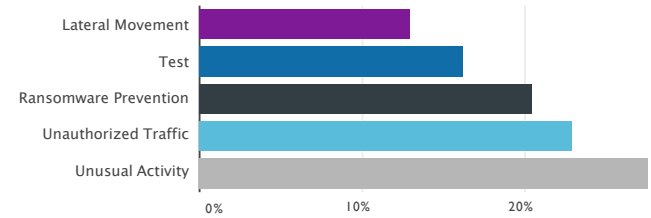
Most Common Policy Violations

ThreatSync+ NDR monitors your network for violations of activity policies that are important to you . This chart shows the number of alerts generated for these policies that were active during the period 01 May – 14 May.



Policy Alerts by Tags

This chart shows the most common tags of alerts generated during the period 01 May – 14 May.



Policy Alerts by Device or IP

These are the devices in your network that were most frequently involved in policy violations .This chart shows the number of alerts generated for these devices during the period 01 May – 14 May.

DEVICE	THREAT SCORE	ALERTS
10.83.83.63	67	12
10.81.101.6	66	10
10.81.101.60	64	10
10.81.101.39	64	10
10.81.101.9	63	10
10.81.101.78	61	10
10.81.101.73	60	10
10.81.101.75	59	11
10.81.101.147	55	10
10.81.101.12	54	10

How to Use this Report

Continued use of ThreatSync+ NDR is aimed at improving your CyberScore and securing your critical IT devices. ThreatSync+ NDR identifies, detects, and responds to threats to your network without requiring any additional hardware, software or people. The ThreatSync+ NDR Cloud continuously analyzes the billions of conversations happening on your network, learns what is normal, and alerts when suspicious behaviors that users risk the security of your critical IT devices are detected.

Whether you are evaluating ThreatSync+ NDR for use or actively protecting your network with it, this report provides you with a quick and easy assessment of your network, enabling you to see where key threats and vulnerabilities are.

CyberScore

Your CyberScore provides you an overall measure of network health measured by the threats and vulnerabilities that ThreatSync+ NDR detects.

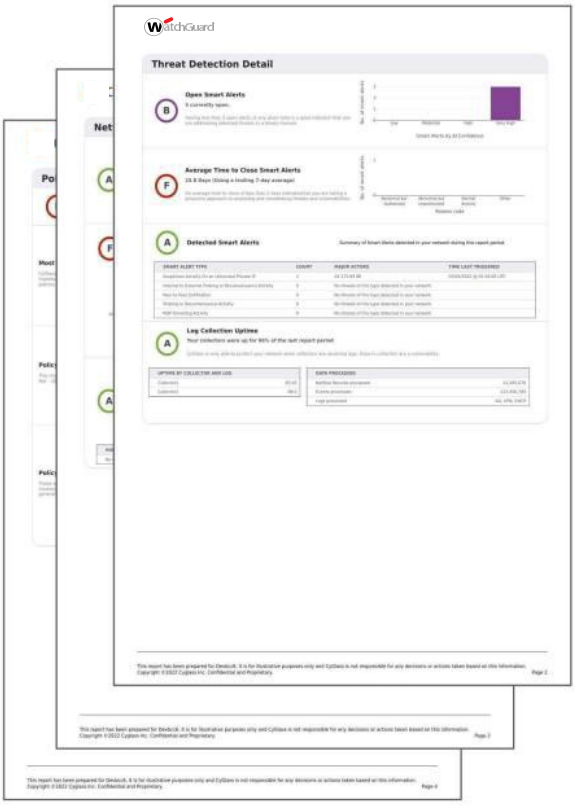
The score enables you to track your progress over time and compare your network to that of other ThreatSync+ NDR customers. The score is calculated like a credit score, on a scale of 300 to 850. Your health grade reflects your performance compared to others. Most get a B. But we all strive for an A.

Metrics

ThreatSync+ NDR tracks a set of key metrics across 3 areas: Network Visibility, Policy Assurance and Threat Detection. These metrics allow you to see your progress in each area so you can work on increasing your score.

You can configure which metrics are displayed in the report from within the ThreatSync+ NDR website.You can also customize how your CyberScore is weighted across the 3 areas.

The additional pages of the report provide more detail about each one of these three areas.



Metric Details

Pages two, three and four provide more details into the key metrics displayed on page one. Each metric includes a multi-day trend chart showing how the metrics has varied over the preceding report period.

Each page also contain additional charts that show specific information about the metrics.

The Unidentified Devices metric is Not Applicable when there are no devices defined in the system nor any detected undefined devices.

The High Risk Devices metric is Not Applicable when there are no devices defined in the system

The Unidentified Subnets or IP Ranges metric is Not Applicable when there are no subnet defined in the system nor any detected undefined subnets.

The Policy Alerts metric is Not Applicable when there are no active policies