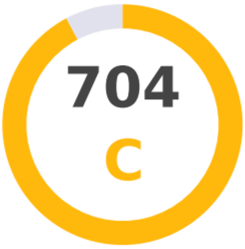
Executive Scorecard for Acme Corporation

Report generated on June 12, 2023

Read more about how to interpret this report ⇢

Cyber Score



A cyber score of 763 or higher is your target based on other CyGlass users.

Continued use of CyGlass is aimed at improving your CyberScore and securing your critical IT devices. CyGlass identifies, detects, and responds to threats to your network without requiring any additional hardware, software or people. The CyGlass 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.

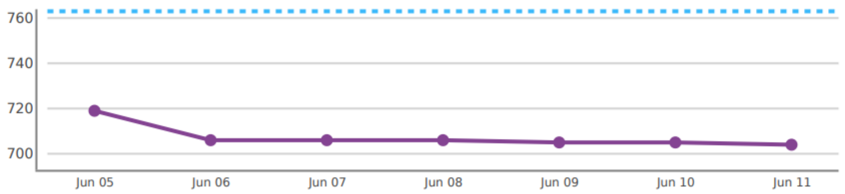
Time Period

From:	June 05, 2023
To:	June 11, 2023
Generated:	June 12, 2023
Period:	7 Days

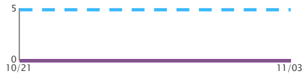
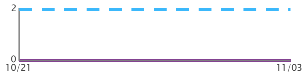
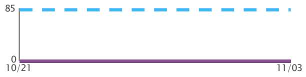
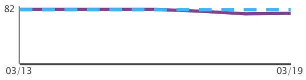
Legend

·········	Target Cyber Score
▬	No data available

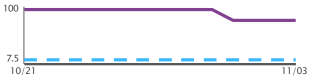
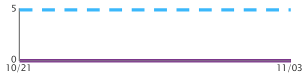
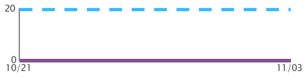
Cyber Score History



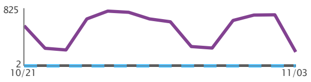
Threat Detection Summary

CYBER SCORE	SUMMARY	DESCRIPTION	14 DAY HISTORY
A	**Open Smart Alerts** 0 currently open	Smart Alerts are CyGlass' 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 CyGlass 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.	
B	**Log Collection Uptime** 96%	CyGlass 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 CyGlass. Labels and importance ratings help CyGlass highlight the threats that are most critical to you.	
A	**High Risk Devices** 0.0%	CyGlass 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 CyGlass. Labels help CyGlass 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.	

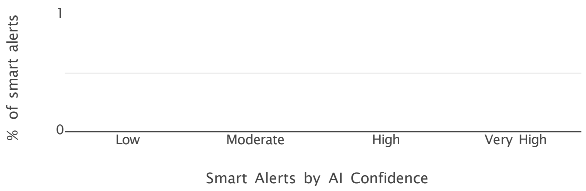
Threat Detection Detail

A

Open Smart Alerts

0 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.

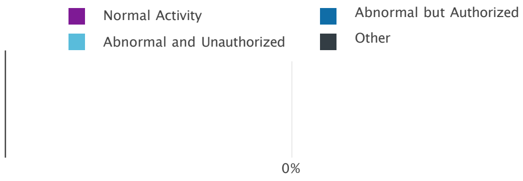


A

Average Time to Close Smart Alerts

0.0 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.



A

Detected Smart Alerts

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

SMART ALERT TYPE	COUNT	MAJOR ACTORS	TIME LAST TRIGGERED
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	
Probing or Reconnaissance Activity	0	No threats of this type detected in your network	
RDP Tunneling 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 Tunneling Plus Data Exfiltration	0	No threats of this type detected in your network	
Suspicious Tunneling Plus Port Scan	0	No threats of this type detected in your network	

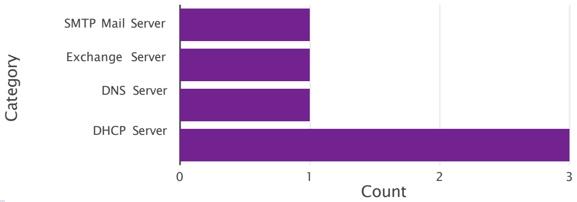
Network Visibility Detail

F

Unidentified Devices

75.0%

Unidentified devices are those that CyGlass sees that you have not labeled and rated. By applying labels and importance ratings, you provide important context for CyGlass 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, November 03, 2022.

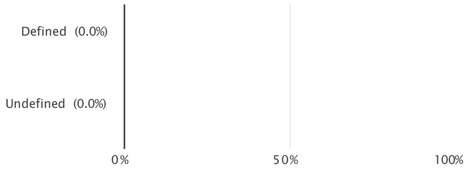


A

Unidentified Subnets or IP Ranges

0.0%

Unidentified subnets are those that have not been labeled in CyGlass. By applying labels, you provide important context to CyGlass in better understanding what threats are most critical to your organization. This chart reflects your network at the time of report generation, November 03, 2022.



IP START RANGE	ACTIVE IPs	LAST UPDATED
No Unidentified Subnets or IP ranges Available		

A

High Risk Devices

0 Devices with a Threat Score above 70

You know which devices are important to your business. CyGlass 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, November 03, 2022.

Very High Risk
High Risk
Medium Risk
Low Risk
Very Low Risk
0
1

HIGH RISK DEVICES	THREAT SCORE	ALERT COUNT	ROLE	IP ADDRESS
No High Risk Devices Available				

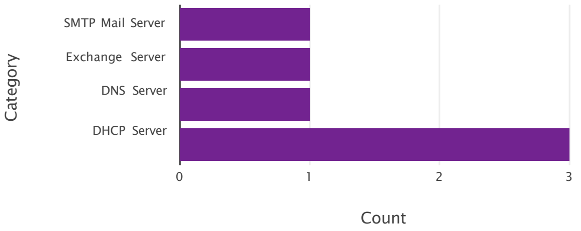
Network Visibility Detail

Unidentified Devices

F

75.0%

Unidentified devices are those that CyGlass sees that you have not labeled and rated. By applying labels and importance ratings, you provide important context for CyGlass 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, November 03, 2022.

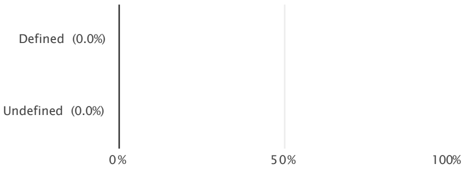


Unidentified Subnets or IP Ranges

A

0.0%

Unidentified subnets are those that have not been labeled in CyGlass. By applying labels, you provide important context to CyGlass in better understanding what threats are most critical to your organization. This chart reflects your network at the time of report generation, November 03, 2022.



IP START RANGE	ACTIVE IPs	LAST UPDATED
No Unidentified Subnets or IP ranges Available		

High Risk Devices

A

0 Devices with a Threat Score above 70

You know which devices are important to your business. CyGlass 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, November 03, 2022.

HIGH RISK DEVICES	THREAT SCORE	ALERT COUNT	ROLE	IP ADDRESS
No High Risk Devices Available				

Policy Assurance Detail

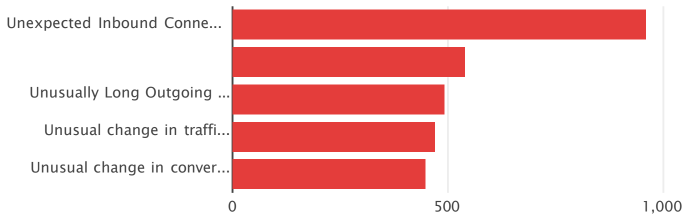
F

Policy Alerts

1152.1 Per day (Average of past 7 days)

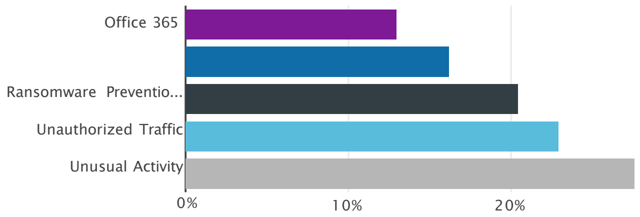
Most Common Policy Violations

CyGlass 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 21 Oct - 03 Nov.



Policy Alerts by Tags

This chart shows the most common tags of alerts generated during the period 21 Oct - 03 Nov.



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 21 Oct - 03 Nov.

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