



# CyGlass Network Defence Goals and Reports

## SET DEFENCE GOALS, SHOW SUCCESS REPORTS

- Defense goals activate prebuilt policies and AI driven controls
- Reports are generated automatically
- No extra overhead, no extra cost

### Add a Network Defence Goal

#### Network Operations

IT Asset Discovery  
IoT Security Risks

#### Security

Executive Summary  
Ransomware Threats  
M365 Monitoring and Defense

#### Compliance

CMMC  
NIST-CSF  
Cyber Essentials  
FFIEC

#### Users

AD Azure Risks

Add Goal

Cancel

[Learn more about Network Defence Goals](#) 

# Microsoft 365 Security Summary Report

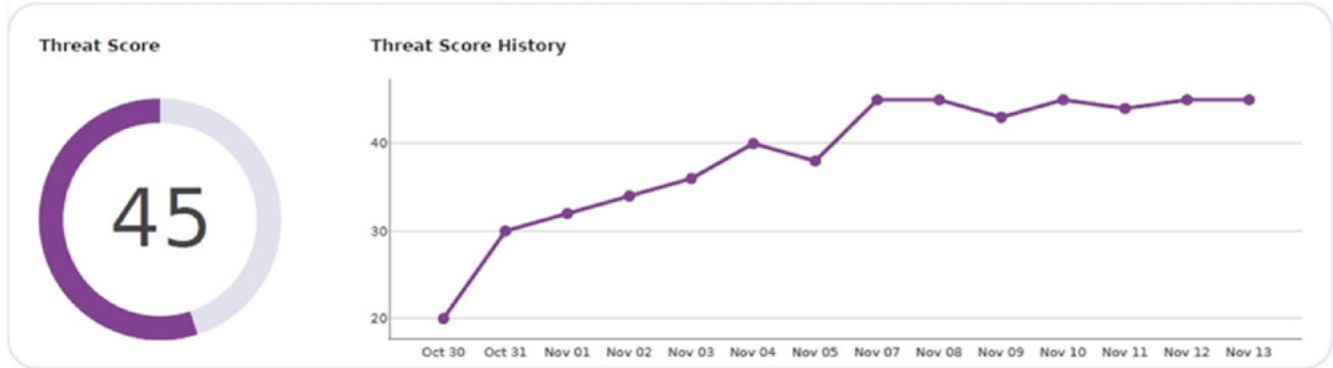
Report generated on March 09, 2021

Analysis based on 14 days of retained data from February 11, 2021 to February 24, 2021

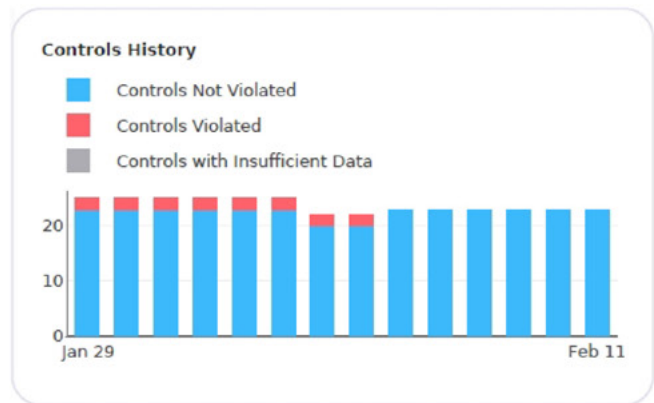
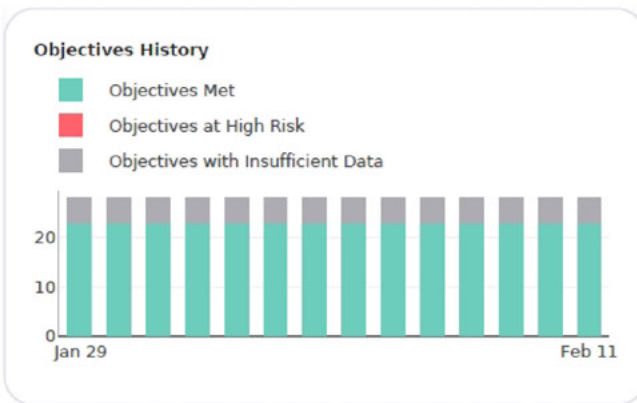
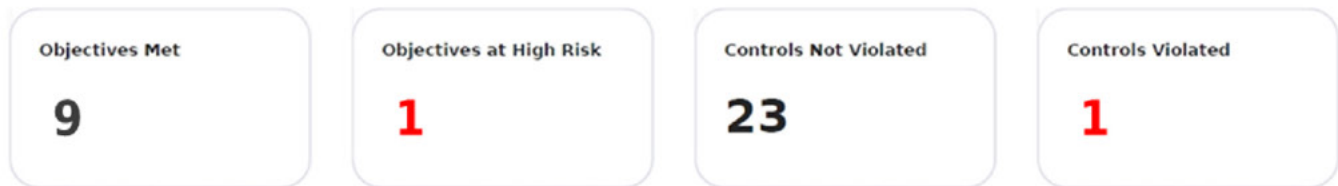
Network Defense Goal

## Microsoft 365 Security Summary

Compliant



## Objectives and Controls



This report has been prepared for devredteam1 site. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

Beta Release Version 2.

Copyright © 2021 Cyglass Inc. Confidential and Proprietary.

**45** OBJECTIVE **Unusual Login Activity** Compliant

| CONTROL DESCRIPTION  | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|--|------------------------|-----------------------|-------------------|
| <b>High Login Failure Rate</b><br>A user has attempted and failed to log into resources on your network multiple times. This could indicate an account takeover attempt.               | 45                     | 46                    | Compliant 6 Days  |
| <b>Simultaneous Login</b><br>A user has been active from two devices at the same time. This user's account may be compromised.   | 45                     | 45                    | Compliant 6 Days  |
| <b>Impossible Travel</b><br>A user has logged in from two locations, and the login times are too close together for plausible physical travel. This user's account may be compromised. | 45                     | 49                    | Compliant 6 Days  |
| <b>Login From Dormant Account</b><br>A user who has been inactive for more than 60 days recently logged in. Attackers often target unused accounts; this account may be compromised.   | 45                     | 49                    | Compliant 6 Days  |

**45** OBJECTIVE **Unusual Access Behavior** Compliant

| CONTROL DESCRIPTION   | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|---|------------------------|-----------------------|-------------------|
| <b>Unusual Access Time</b><br>A user has accessed resources on your network at an unusual time. This could be a sign of account takeover or malicious activity.                 | 45                     | 50                    | Compliant 6 Days  |
| <b>Unusual Access Location</b><br>A user has accessed resources on your network from a new or unusual location. This could be a sign of account takeover or malicious activity. | 45                     | 46                    | Compliant 6 Days  |
| <b>Unusual User Agent</b><br>A user has accessed web content using a new or unusual browser, tool, or device. This could be a sign of account takeover or malicious activity.   | 45                     | 49                    | Compliant 6 Days  |

**45** OBJECTIVE **Possible SAML Token Forgery** Compliant

| CONTROL DESCRIPTION  | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|--|------------------------|-----------------------|-------------------|
| <b>Unusual SAML Token</b><br>A Security Assertion Markup Language token with User Authentication Value of 16457 has been detected. This is a potential indicator of a forged SAML token. | 45                     | 47                    | Compliant 6 Days  |

This report has been prepared for devredteam1 site. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

Beta Release Version 2.

Copyright ©2021 Cyglass Inc. Confidential and Proprietary.

45

OBJECTIVE  
Active Directory Privilege Escalation

Compliant

| CONTROL DESCRIPTION   | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|---|------------------------|-----------------------|-------------------|
| <b>Batch Privilege Modification</b><br>An unusual volume of active directory privilege changes has been detected.                     |                        |                       | 6 Days            |
| <b>Suspicious Modification Of Group Privileges</b><br>An active directory group has been given unusual or risky credentials.          |                        |                       | 6 Days            |
| <b>Active Directory Admin Creation</b><br>An active directory account with domain, enterprise, or schema privileges has been created. |                        |                       | 6 Days            |

45

OBJECTIVE  
Active Directory Configuration Changes

Compliant

| CONTROL DESCRIPTION  | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|--|------------------------|-----------------------|-------------------|
| <b>Account Authentication Changes</b><br>Changes have been made to the protocol your active directory system uses to authenticate users. |                        |                       | 6 Days            |
| <b>New Domain Trust</b><br>A new trust relationship has been added between domain services in your network.                              |                        |                       | 6 Days            |
| <b>Adfs Trust Modification</b><br>A new trust relationship has been added to your ADFS.  |                        |                       | 6 Days            |

60

OBJECTIVE  
Unusual Active Directory Activity

Not Compliant

| CONTROL DESCRIPTION   | THREAT SCORE                                 | ALERT COUNT                                | COMPLIANCE |
|---|--|--|------------|
| <b>Active Directory to External</b><br>Detect when Active Directory Servers are communicating improperly with the outside world on ports other than 53, 80 or 443 | <p>Threat Score Compliance Threshold: 50</p> | <p>Alert Count Compliance Threshold: 0</p> | 0 Days     |

This report has been prepared for devredteam1 site. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

Beta Release Version 2.

Copyright ©2021 Cyglass Inc. Confidential and Proprietary.

45

OBJECTIVE  
Unusual Email Activity

Compliant

| CONTROL DESCRIPTION  | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|--|------------------------|-----------------------|-------------------|
| <b>Unusual Email Volume</b><br>A user sent an unusual volume of email. This may be a phishing attack from a compromised account.   | 45                     | 47                    | Compliant 6 Days  |
| <b>Unusual Email Activity Time</b><br>A user logged into their email account or sent mail at an unusual time. This account may be compromised.                                       | 45                     | 46                    | Compliant 6 Days  |
| <b>Suspicious Email Attachment Type</b><br>An email attachment with an suspicious file type has been detected. This may be attack behavior from a compromised account.               | 45                     | 50                    | Compliant 6 Days  |
| <b>Unusual Email Attachment Size</b><br>An email attachment with an unusual size has been detected. This may indicate attack behavior from a compromised account.                    | 45                     | 50                    | Compliant 6 Days  |
| <b>Suspicious Application Email Access</b><br>An application with email access credentials has executed suspicious searches, sent a high volume of email, or set up new inbox rules. | 45                     | 49                    | Compliant 6 Days  |
| <b>Possible Phishing</b><br>A user accessed their email immediately before attempting to resolve the address of a suspicious site. They may have clicked on a phishing link.         | 45                     | 46                    | Compliant 6 Days  |

45

OBJECTIVE  
Possible Exfiltration Over Email

Compliant

| CONTROL DESCRIPTION  | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|--|------------------------|-----------------------|-------------------|
| <b>Suspicious Email Forwarding Rules</b><br>Suspicious email forwarding rules have been detected. An attacker may be exfiltrating files over email.                    | 45                     | 50                    | Compliant 6 Days  |
| <b>High Email Volume To External Address</b><br>An unusual volume of email to an external address has been detected. An attacker may be exfiltrating files over email. | 45                     | 50                    | Compliant 6 Days  |
| <b>Suspicious Email Attachment Type</b><br>An email attachment with an suspicious file type has been detected. This may be attack behavior from a compromised account. | 45                     | 50                    | Compliant 6 Days  |

This report has been prepared for devredteam1 site. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

Beta Release Version 2.

Copyright ©2021 Cyglass Inc. Confidential and Proprietary.

45

OBJECTIVE  
Possible Exfiltration By Internal Actor

Compliant

| CONTROL DESCRIPTION   | THREAT SCORE & HISTORY | ALERT COUNT & HISTORY | COMPLIANCE & TIME |
|---|------------------------|-----------------------|-------------------|
| <b>Anonymous File Activity</b><br>An anonymous user is accessing or modifying files.  |                        |                       | <b>6 Days</b>     |
| <b>Unusual Rate Of File Activity</b><br>An unusual rate of file creation, deletion, or modification has been detected. This may indicate file encryption by ransomware or file exfiltration.                    |                        |                       | <b>6 Days</b>     |
| <b>Internal Files Made Public</b><br>Internal files have been made available to anyone on the internet.   |                        |                       | <b>6 Days</b>     |
| <b>Internal Files Shared Externally</b><br>Internal files have been shared with an external user.   |                        |                       | <b>6 Days</b>     |
| <b>Unusual File Permissions Modification</b><br>A user has modified the permissions on an unusual number of files and folders. This may be a compromised user account or file exfiltration by an internal user. |                        |                       | <b>6 Days</b>     |
| <b>Unusual File Download</b><br>A user has downloaded an unusual number of files. This may be a compromised account or file exfiltration by an internal user.   |                        |                       | <b>6 Days</b>     |

This report has been prepared for devredteam1 site. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

Beta Release Version 2.

Copyright ©2021 Cyglass Inc. Confidential and Proprietary.

Page 5