

ISO 27001 Network Defense Goal Report

Acme Corporation

Continued use of CyGlass is aimed at improving your threat score 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.

[Read more about how to interpret this report ->](#)

Time Period

From: October 21, 2022
 To: November 03, 2022
 Generated: November 03, 2022
 Period: 14 Days

Legend

..... Threshold
 — No data available

75

Network Defense Overview

Threat Score

75

Threat Score History

Date	Threat Score
Oct 21	75
Oct 22	75
Oct 23	75
Oct 24	75
Oct 25	75
Oct 26	75
Oct 27	75
Oct 28	75
Oct 29	75
Oct 30	75
Oct 31	75
Nov 01	75
Nov 02	75
Nov 03	70

7/8 Objectives are not compliant

26/58 Controls are not compliant

75

Top Network Threats

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	<p>6. A.9.1: Business requirements of access control 6.3 Activity to Blocked Countries</p> <p>Detect traffic to countries blocked by your firewall</p>	<p>We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.</p>		✘ 0 Days
75	<p>8. A.9.4: System and application access control 8.1 Possible Brute Force Account Access Attempt</p> <p>Detect a user has attempted and failed to log into resources on your network multiple times</p>	<p>We recommend enabling multi-factor authentication and enforcing password complexity requirements. We also suggest forcing a password reset on involved user accounts.</p>		✘ 0 Days
70	<p>3. A.13.1: Network security management 3.34 Unusual connection count from Internal to External</p> <p>The connection count from an internal IP address to an external domain is varying considerably from the usual activity. This could indicate unauthorized activity to an unusual destination.</p>	<p>We suggest investigating this traffic and if you suspect this may have been attack activity, running antivirus on the involved critical devices will help identify the security risk and mitigate it.</p>		✘ 0 Days

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

Copyright ©2022 Cyglass Inc. Confidential and Proprietary.

Page 1



OBJECTIVE

1. A.12.4: Logging and monitoring

The Controls in this Objective address ISO 27001 requirements for Section A.12.4: Logging and monitoring with the Objective: To record events and generate evidence.

Insufficient Data

CyGlass has not received enough data to assess this network defense objective. Please confirm that CyGlass has received relevant data for the report evaluation period or email support@cyglass.com.



OBJECTIVE

2. A.12.5: Control of operational software

The Controls in this Objective address ISO 27001 requirements for Section A.12.5: Control of operational software with the Objective: To ensure the integrity of operational systems.

Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	<p>2.1 WUDO Traffic Crossing Network Boundary</p> <p>Detects Windows Update Delivery Optimization (WUDO) traffic between devices within your network and the public internet.</p>	Identify the devices communicating on WUDO port 7680 and scan the machines with antivirus and investigate the destination domains are allowed in your network.		18 Days



OBJECTIVE

3. A.13.1: Network security management

The Controls in this Objective address ISO 27001 requirements for Section A.13.1: Network security management with the Objective: To ensure the protection of information in networks and its supporting information processing facilities.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	<p>3.1 AA21-356A - Detect potential Log4Shell Attacks to New Organizations via LDAP or RMI</p> <p>As recommended in CISA Alert AA21-356A, this policy identifies LDAP and RMI activity to sites never before communicated with.</p>	Upgrade the Java library of log4j to latest and stable version.		18 Days
0	<p>3.2 AA21-356A - Detect potential Log4Shell Attacks via LDAP or RMI</p> <p>As recommended in CISA Alert AA21-356A, this policy identifies LDAP and RMI activity to known malicious IPs.</p>	Upgrade the Java library of log4j to latest and stable version.		18 Days
0	<p>3.3 AA21-356A - Detecting unusual volume of DNS, LDAP or RMI activity due to potential Log4Shell Attacks</p> <p>As recommended in CISA Alert AA21-356A, this policy identifies LDAP and RMI activity that is anomalous.</p>	Upgrade the Java library of log4j to latest and stable version.		18 Days
0	<p>3.4 Active Directory to External</p> <p>Detect when Active Directory Servers are communicating improperly with the outside world on ports other than 53, 80, 123 or 443</p>	We recommend closing all unused ports on your AD server. This usually means closing all ports but 53, 80, 123, and 443.		18 Days
0	<p>3.5 Activity Involving Blacklisted IPs</p> <p>Detect traffic to or from Blacklisted IPs</p>	Block all the malicious IP addresses at your perimeter firewall.		18 Days
0	<p>3.6 Anomalous Activity from Blocked Countries</p> <p>Detect when any anomalous events are detected due to communication from Blocked Countries</p>	Identify the destinations domains and determine if they pose a risk to your organization. If so, isolate the internal devices that are connecting to these unauthorized countries.		18 Days
0	<p>3.7 Anomalous Activity to Blocked Countries</p> <p>Detect when any anomalous events are detected communicating to Blocked Countries</p>	We recommend configuring your firewall to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		18 Days
0	<p>3.8 Beaconing Through Web API</p> <p>Possible automated beaconing activity through a 3rd party web service has been detected between an IP in your network and a remote location. This could indicate unauthorized Command and Control activity.</p>	We suggest quarantining any machines you suspect are running beaconing scripts as well as running anti-virus scans.		13 Days

3.9 Communicate with Suspicious AA21-062AIPs

Volatility has seen attackers leverage the following IP addresses. Although these are tied to virtual private servers (VPSs) servers and virtual private networks (VPNs), responders should investigate these IP addresses on their networks and act accordingly

Investigate the malicious IP Addresses define in CISA alert <https://www.cisa.gov/uscert/ncas/alerts/aa21-062a>.



✓ 18 Days

3.10 Incoming Web Server Traffic from the Internet

Incoming connections have been detected on ports commonly used by web servers. It is unusual that a web server should be operating in the configured internal organizations/subnets.

Identify the root cause for setting up webserver on internal organization subnet as this could be attacker exfiltrating the data from an internal source to external command and control server.



✓ 18 Days

3.11 LLMNR Traffic Crossing Network Boundary

Link-Local Multicast Name Resolution (LLMNR) traffic - port 5355 UDP - is detected across network boundary. This is Unnecessary or Unexpected Port Activity, and blocking it is part of preventing ransomware attacks.

We suggest blocking ports UDP/137, UDP/138, and TCP/139 at the perimeter firewall in both directions and disabling LLMNR on all of your Windows devices.



✓ 18 Days

3.12 NetBIOS-NS Traffic Crossing Network Boundary

NetBIOS-NS traffic - port 137 UDP - is detected across network boundary. This is Unnecessary or Unexpected Port Activity, and blocking it is part of preventing ransomware attacks.

We suggest blocking ports UDP 137, UDP 138, and TCP 139 at the perimeter firewall in both directions and disabling NetBIOS-NS on all of your Windows devices.



✓ 18 Days

3.13 Outbound NetBIOS Traffic

NetBIOS traffic from internal endpoints to public IPs is detected. This is an indicator of possible SMB Leakage, and blocking such activity is part of preventing ransomware attacks.

We suggest blocking ports UDP/137, UDP/138, and TCP/139 at the perimeter firewall in both directions and disabling NetBIOS-NS on all of your Windows devices.



✓ 18 Days

3.14 Outbound SMB Traffic

Server Message Block (SMB) traffic - port 445 TCP - from internal endpoints to public IPs is detected. This is an indicator of possible SMB Leakage, and blocking such activity is part of preventing ransomware attacks.

We recommend disabling SMB protocol on Web and DNS Servers, disabling SMB protocol on Internet facing servers, disabling ports TCP 139 and TCP 445 used by the SMB protocol, restricting anonymous access through "RestrictNullSessAccess" parameter from the Windows Registry



✓ 18 Days

3.15 Unauthorized Outbound SSH

An unauthorized SSH connection has been detected from an internal device to an external domain.

We recommend routing all legitimate external SSH connections through a VPN and blocking all incoming activity on ports 3389 and 22.



✗ 0 Days

3.16 Unexpected Inbound Connection

An unexpected connection from external to an internal endpoint is detected. This is Unnecessary or Unexpected Port Activity, an indicator of ransomware attacks.

We recommend configuring this control to alert only on traffic with high-value devices and investigating the traffic associated with these alerts to determine if it is legitimate. Start by identifying the external IP, looking at the volume of data exchanged, and finding what protocols are associated with the observed ports.



✗ 0 Days

3.17 Unsecured Inbound FTP/TFTP Traffic

FTP/TFTP Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports Indicates vulnerabilities against ransomware attacks.

We suggest using SFTP in place of FTP/TFTP to ensure that your data is secured during transfer and blocking ports UDP/137, UDP/138, and TCP/139 at perimeter firewall in both directions



✓ 18 Days

3.18 Unsecured Inbound IRC Traffic

IRC Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest closing TCP ports 194 and 6667 on all your high-value devices and blocking traffic on these ports from your perimeter firewalls.



✓ 18 Days

3.19 Unsecured Inbound SNMP Traffic

SNMP Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports Indicates vulnerabilities against ransomware attacks.

We suggest disabling SNMP on all high-value devices in your network and blocking ports 161 and 162 on your perimeter firewalls. If you require SNMP, we suggest upgrading to SNMP3, which is encrypted.



✓ 18 Days

3.20 Unsecured Inbound TCP Traffic

TCP Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports Indicates vulnerabilities against ransomware attacks.

We suggest configuring your firewall to block all externally initiated TCP traffic destined for machines you don't expect to serve content to the public internet.



✗ 0 Days

3.21 Unsecured Inbound Telnet Traffic

Telnet Traffic - port 23 TCP - is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest disabling telnet on all your high-value devices and blocking port 23 on your perimeter firewalls.



✓ 18 Days



3.22 Unsecured Inbound UDP Traffic

UDP Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest configuring your firewall to block all externally initiated UDP traffic destined for machines you don't expect to serve content to the public internet.



✓ 18 Days



3.23 Unsecured Inbound Web Server Activity

Unsecure web server traffic - port 80 TCP - is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest using HTTPS to serve any publicly-facing content. If this alert was generated for a high-value device, we suggest investigating the source, destination, and traffic volume.



✗ 0 Days



3.24 Unsecured Internal FTP/TFTP Traffic

FTP/TFTP Traffic is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest using SFTP in place of FTP/TFTP to ensure that your data is secured during transfer.



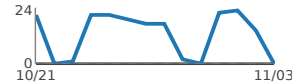
✗ 0 Days



3.25 Unsecured Internal IRC Traffic

IRC Traffic is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest closing TCP ports 194 and 6667 on all your high-value devices and blocking traffic on these ports from your perimeter firewalls.



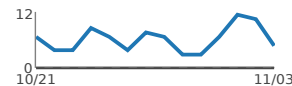
✗ 0 Days



3.26 Unsecured Internal SNMP Traffic

SNMP Traffic is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest disabling SNMP on all high-value devices in your network. Where you require SNMP, we suggest upgrading to SNMP3, which is encrypted.



✗ 0 Days



3.27 Unsecured Internal Telnet Traffic

Telnet Traffic - port 23 TCP - is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest disabling telnet on all your high-value devices and blocking port 23 on your perimeter firewalls.



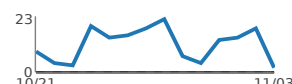
✓ 18 Days



3.28 Unsecured Internal Web Server Activity

Unsecure web server traffic - port 80 TCP - is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest using HTTPS to serve any publicly-facing content. If this alert was generated for a high-value device, we suggest investigating the source, destination, and traffic volume.



✗ 0 Days



3.29 Unsecured Outbound FTP/TFTP Traffic

FTP/TFTP Traffic is detected from internal to external endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest using SFTP in place of FTP/TFTP to ensure that your data is secured during transfer and blocking ports UDP/137, UDP/138, and TCP/139 at perimeter firewall in both directions



✓ 18 Days



3.30 Unsecured Outbound IRC Traffic

IRC Traffic is detected from internal to external endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest closing TCP ports 194 and 6667 on all your high-value devices and blocking traffic on these ports from your perimeter firewalls.



✓ 18 Days



3.31 Unsecured Outbound SNMP Traffic

SNMP Traffic is detected from internal to external endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest disabling SNMP on all high-value devices in your network and blocking ports 161 and 162 on your perimeter firewalls. If you require SNMP, we suggest upgrading to SNMP3, which is encrypted.



✓ 18 Days



3.32 Unsecured Outbound Telnet Traffic

Telnet Traffic - port 23 TCP - is detected from internal to external endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.

We suggest disabling telnet on all your high-value devices and blocking port 23 on your perimeter firewalls.



✓ 18 Days



3.33 Unusual connection count from Critical Devices to External

The connection count from a Critical Device to an external domain is unusual. This could indicate unauthorized activity to an unusual destination.

We suggest investigating this traffic and, if you suspect this may have been attack activity, running antivirus on the involved critical devices.



✓ 18 Days



3.34 Unusual connection count from Internal to External

The connection count from an internal IP address to an external domain is varying considerably from the usual activity. This could indicate unauthorized activity to an unusual destination.

We suggest investigating this traffic and if you suspect this may have been attack activity, running antivirus on the involved critical devices will help identify the security risk and mitigate it.



✗ 0 Days



3.35 Unusually High Activity from Critical Devices to External

An unusual volume of activity has been detected between a critical device and an external domain.

We suggest investigating this traffic and, if you suspect this may have been attack activity, running antivirus on the involved critical devices.



✓ 18 Days



OBJECTIVE

4. A.17.1: Information security continuity

The Controls in this Objective address ISO 27001 requirements for Section A.17.1: Information security continuity with the Objective: Information security continuity shall be embedded in the organization's business continuity management systems.

! Insufficient Data

CyGlass has not received enough data to assess this network defense objective. Please confirm that CyGlass has received relevant data for the report evaluation period or email support@cyglass.com.



OBJECTIVE

5. A.8.1: Responsibility for assets

The Controls in this Objective address ISO 27001 requirements for Section A.8.1: Responsibility for assets with the Objective: To identify organizational assets and define appropriate protection responsibilities.

! Insufficient Data

CyGlass has not received enough data to assess this network defense objective. Please confirm that CyGlass has received relevant data for the report evaluation period or email support@cyglass.com.



OBJECTIVE

6. A.9.1: Business requirements of access control

The Controls in this Objective address ISO 27001 requirements for Section A.9.1: Business requirements of access control with the Objective: To limit access to information and information processing facilities.

✗ Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDATION	ALERT HISTORY	COMPLIANCE
0	6.1 Activity between Development and Production Detect when unauthorized development systems are communicating with Production systems	We suggest investigating this traffic and, if you suspect this may have been attack activity, running antivirus on the involved machines.		✓ 18 Days
0	6.2 Activity from Blocked Countries Detect traffic from countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		✓ 18 Days
75	6.3 Activity to Blocked Countries Detect traffic to countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		✗ 0 Days
70	6.4 Activity to Social Media Sites Detect when anyone communicates with a prohibited social media site	Block social media access to protect from data loss or phishing attacks, as well as to increase productivity. Use exclusions to not alert on sites that are authorized or groups of users that may access social media for their jobs.		✗ 0 Days
0	6.5 Connection From New External Domain to Internal A remote Domain has connected to a device in your network for the first time. It may be unusual for connections to be initiated from external domain, especially those that have not connected in the past.	We recommend investigating the traffic that triggered this alert and either blocking the involved external IPs at the firewall or updating the zones associated with this policy to prevent future alerts.		✓ 18 Days
0	6.6 Connection To New Domain from Critical Device A Critical Device in your network has connected to a domain for the first time. It may be unusual for a critical device to interact with an external domain that it has never communicated with before.	We suggest investigating this traffic and, if you suspect this may have been attack activity, running anti-virus on your critical device.		✓ 18 Days
0	6.7 Critical Device to or from Facebook Detect when a critical device is communicating with Facebook	We suggest blocking traffic between high-value devices and Facebook.		✓ 18 Days
70	6.8 Detect Internal traffic to or from Facebook Detect when anyone is communicating with Facebook	Block access to Facebook to reduce the risk of data loss or to increase productivity.		✗ 0 Days
70	6.9 Detect Large Volume to File Sharing sites Detect when sending more than 40K bytes to a public file sharing site	Identify the User sending more than 40K bytes. Consider that this could be an indicator of account take-over.		✗ 0 Days



OBJECTIVE

7. A.9.2: User access management

The Controls in this Objective address ISO 27001 requirements for Section A.9.2: User access management with the Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

! Insufficient Data

CyGlass has not received enough data to assess this network defense objective. Please confirm that CyGlass has received relevant data for the report evaluation period or email support@cyglass.com.

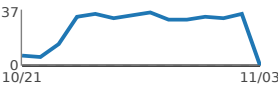
75

OBJECTIVE

8. A.9.4: System and application access control

The Controls in this Objective address ISO 27001 requirements for Section A.9.4: System and application access control with the Objective: To prevent unauthorized access to systems and applications.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	8.1 Possible Brute Force Account Access Attempt Detect a user has attempted and failed to log into resources on your network multiple times	We recommend enabling multi-factor authentication and enforcing password complexity requirements. We also suggest forcing a password reset on involved user accounts.	 <p>37 0 10/21 11/03</p>	0 Days

Control Violation Detail and Remediation

6.3 Activity to Blocked Countries

Control Detail

This control alerts on traffic coming from a country that is blocked by most firewalls. According to a report published by the United Nations, upwards of 80% of cybercrime is committed by criminal organizations with a centralized physical presence. Several countries in Eastern Europe, Eastern Asia, and West Africa show high levels of cybercrime, and several governments have divisions dedicated to cyberattacks. Unless you have a business use case that requires communication with a high-risk country, blocking or alerting on traffic with high-risk countries can significantly lower your exposure to Ransomware and other network attacks. [A.9.1.2 Access to networks and network services]

Remediation

We recommend configuring your firewall to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan. Most firewalls support geographically-based block rules. We also suggest investigating the traffic that generated this alert. If you believe it may be command and control traffic, we suggest quarantining the affected devices, running AV scans, and trying to identify the process generating command and control traffic. Review logs to identify any other devices that have communicated with the same domain and run AV scans on those devices as well. If you are unable to identify the process generating command and control traffic, we suggest reimaging all affected machines.

Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



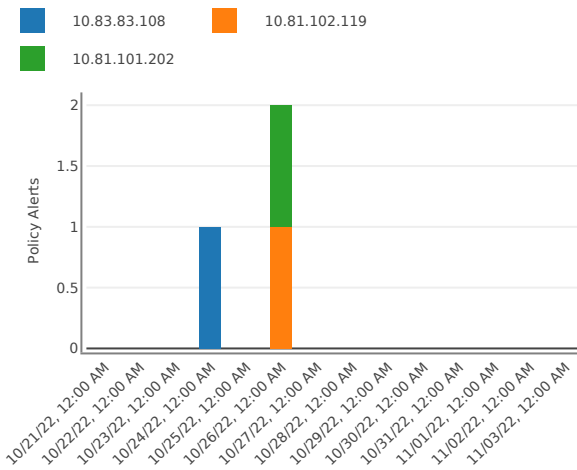
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



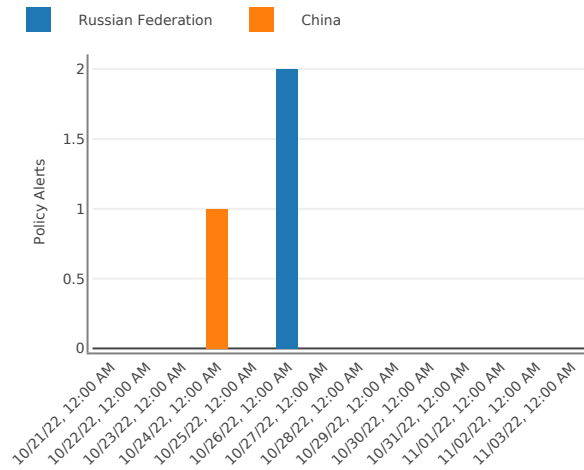
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



6.4 Activity to Social Media Sites

Control Detail

This control gives you visibility within your network to users accessing social networking platforms.

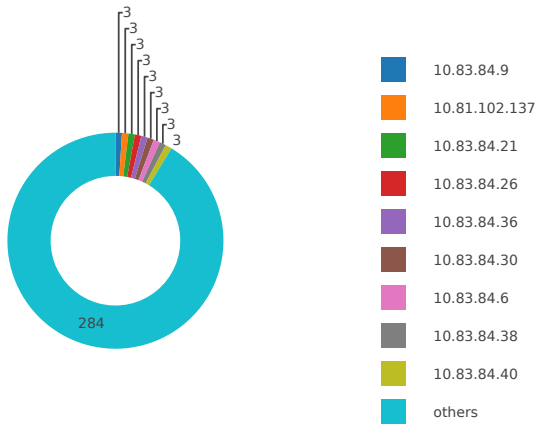
Remediation

Block social media access to protect from data loss or phishing attacks, as well as to increase productivity. Adjust firewall rules to block sites that are not authorized. Use CyGlass policy exclusions to not alert on sites that are authorized or groups of users that may access social media for their jobs.

Alert Detail

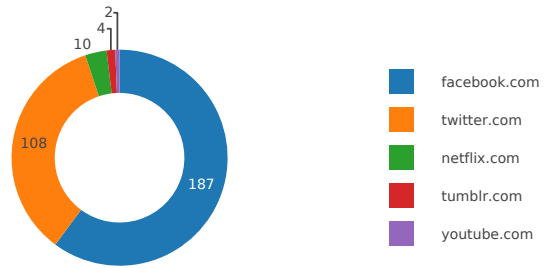
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



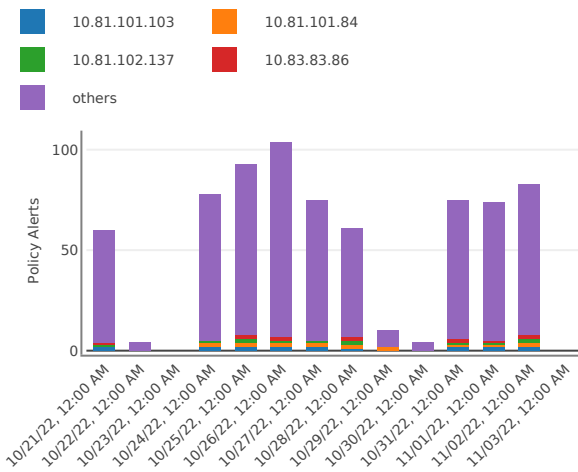
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



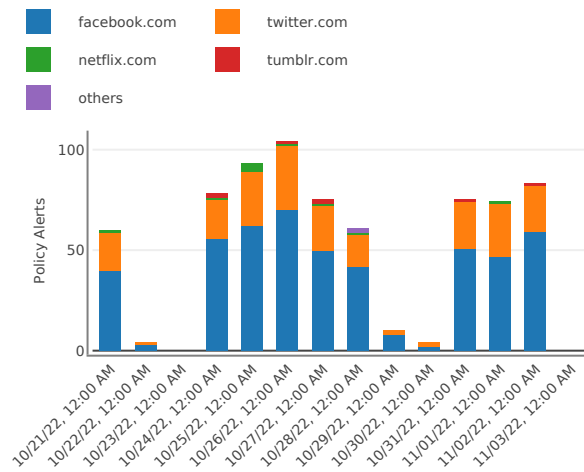
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



6.8 Detect Internal traffic to or from Facebook

Control Detail

This control gives you visibility within your network to users accessing the social networking platform Facebook.

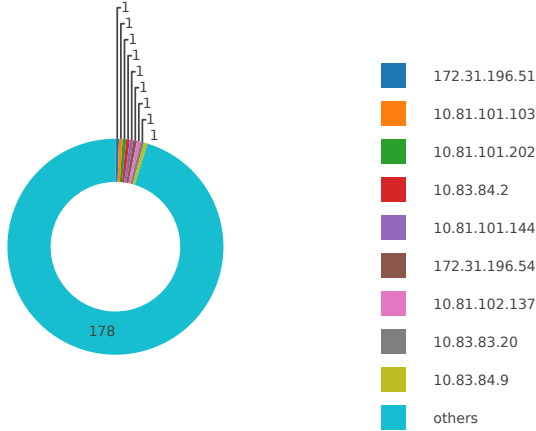
Remediation

Block accessing to Facebook to reduce the risk of data loss or increase productivity. If this is allowed in your network, consider deactivating this policy. If a limited set of users in your network are using Facebook for their work responsibilities, exclude the allowed subnets to enhance the policy.

Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



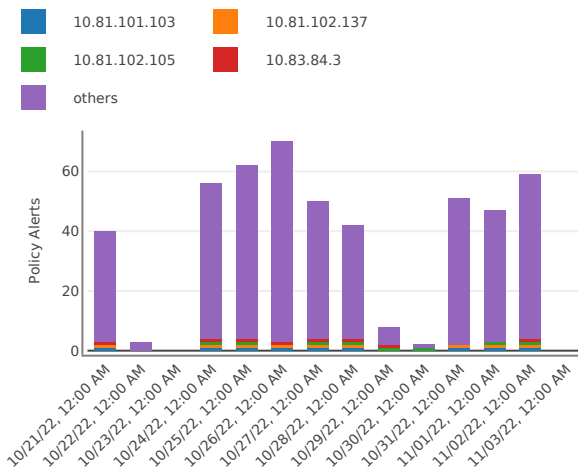
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



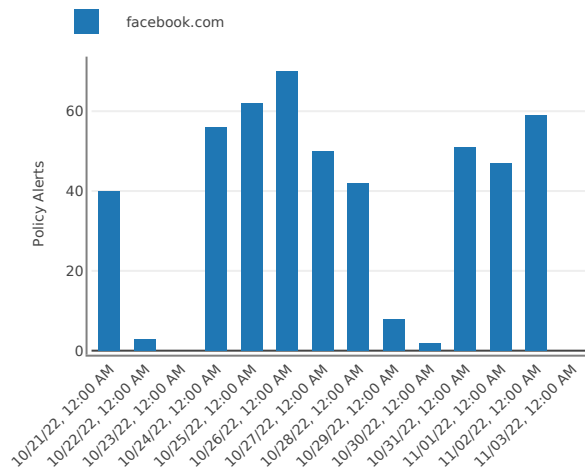
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



6.9 Detect Large Volume to File Sharing sites

Control Detail

This control provide visibility to protect your data getting into the hands of attackers from the exfiltrating the data to unauthorized file servers or C&C servers.

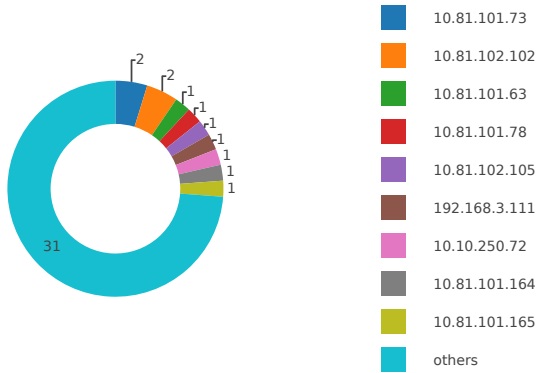
Remediation

Identify the user account exfiltrating the data to a public file share or C&C server. Investigate the content or the file and determine if it is sensitive business data that should not be placed in this public location.

Alert Detail

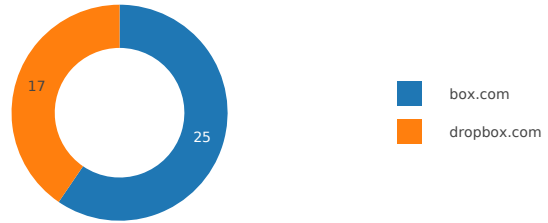
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



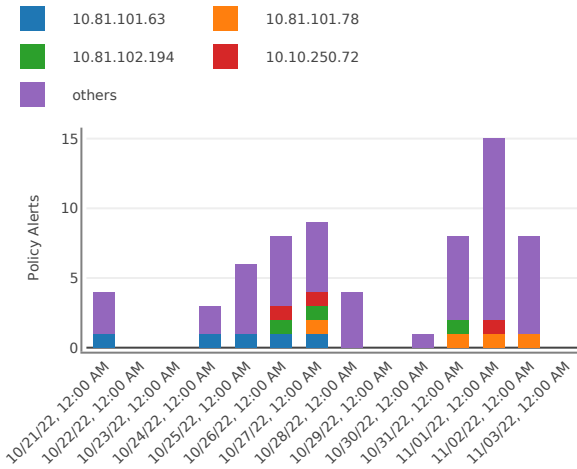
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



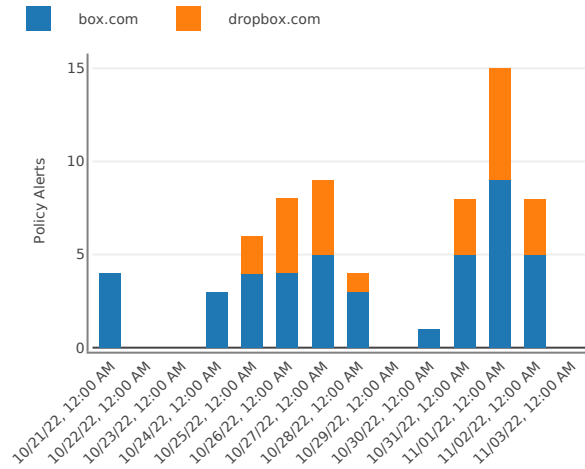
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



8.1 Possible Brute Force Account Access Attempt

Control Detail

An unusual number of failed logins can indicate that an attacker is trying to gain access to your network by iteratively trying common or published passwords. [A.9.4.2 Secure log-on procedures]

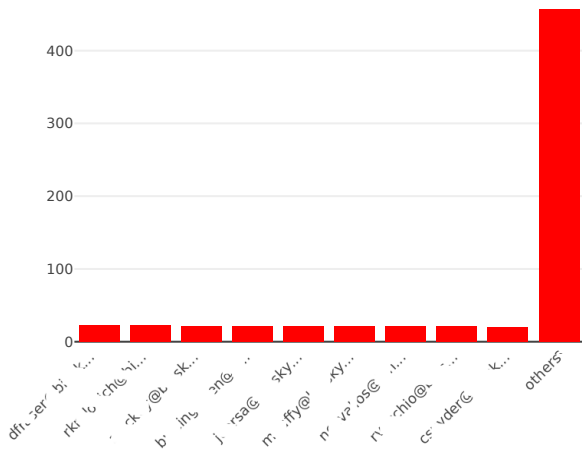
Remediation

We recommend enabling multi-factor authentication and enforcing a password complexity policy. We also suggest investigating these access attempts for unusual login time or location. If you are concerned this access is not legitimate, we recommend contacting this user and forcing a password reset.

Alert Detail

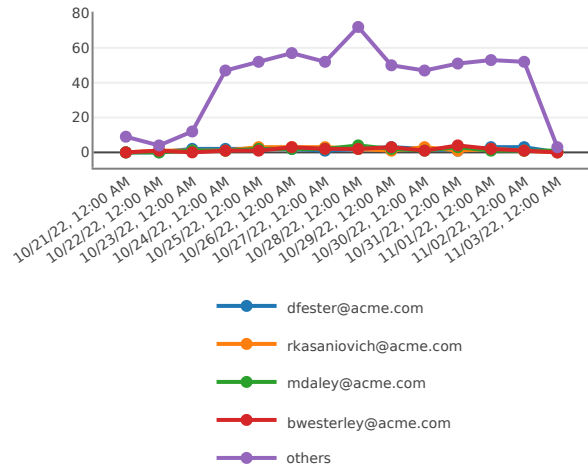
Distribution of Policy Alerts by User

Number of Possible Brute Force Account Access Attempt Policy Alerts, broken down by user



Distribution of Policy Alerts Associated with User Over Time

Number of Possible Brute Force Account Access Attempt Policy Alerts over time



3.15 Unauthorized Outbound SSH

Control Detail

An SSH session destined to an external ip can be a sign that an internal resource is compromised and reaching out to an attacker's public IP to receive further instructions. You can add exceptions to this control for devices you expect to have SSH traffic with external resources. [A.13.1.1 Network controls]

Remediation

Accessing resources on the public internet via SSH is very rarely a legitimate use case, and we suggest you disable SSH on resources that don't require it. If you have legitimate external administration activity, you might want to consider only allowing it through a VPN or similar secure channel. That will allow you to block all incoming activity on these ports (3389 and 22) at your firewall and ensure that this type of access is never allowed.

Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



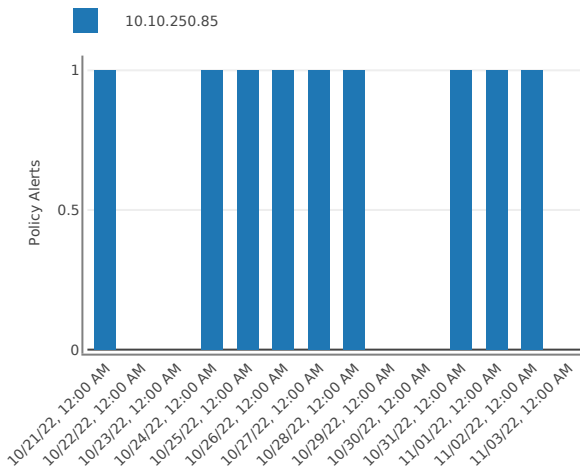
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



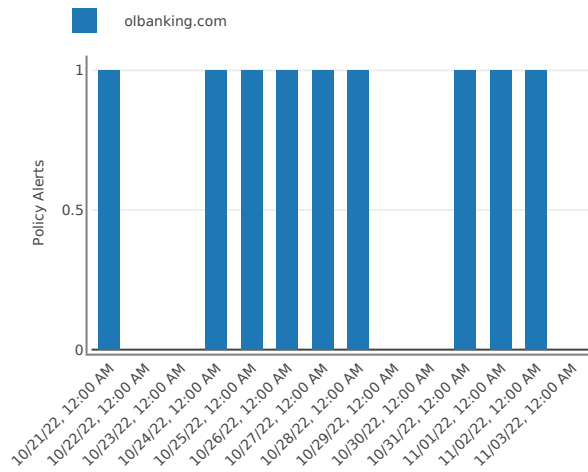
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.16 Unexpected Inbound Connection

Control Detail

We flag any unexpected connection that is initiated outside your network. If a flow was initiated by an outside actor, it may be an attacker trying to gain access to resources on your network. Almost all legitimate north-south traffic will be initiated by users within your network. [A.13.1.1 Network controls]

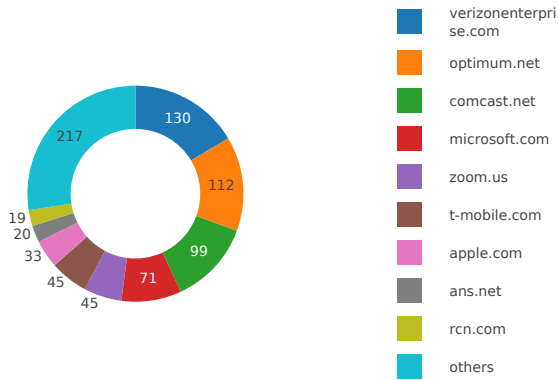
Remediation

We recommend investigating the traffic associated with these alerts to determine if it is legitimate. Start by looking at the volume of data exchanged and on what ports. This is a sensitive control; it's best used on high-value devices. If you have resources that you expect to respond to external connection requests, you can create exceptions to this policy.

Alert Detail

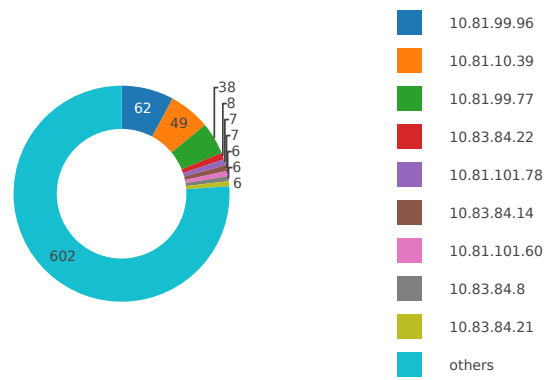
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



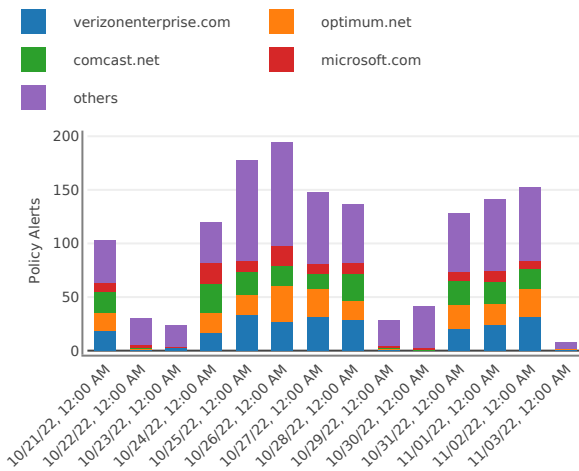
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



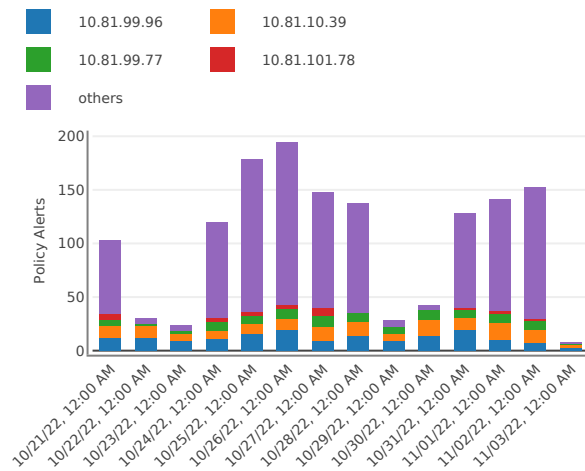
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.20 Unsecured Inbound TCP Traffic

Control Detail

This control alerts on TCP flows originating in the public internet destined for devices in your network. There are a wide variety of known attacks that use web traffic. Because TCP and other common protocols are so critical, attackers know associated ports are likely to be open. We recommend creating a zone for the devices in your network that you expect to have two-way web traffic with the external internet and applying this control to the rest of your network. [A.13.1.1 Network controls]

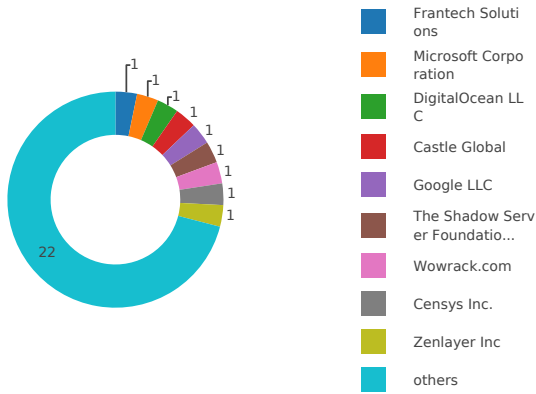
Remediation

When this control is triggered for a device you don't expect to serve content to the public internet, we suggest checking a firewall rule is in place to block all TCP communication with this device. We also suggest investigating the source of these flows and the volume of data transferred. If you believe this may have been attack traffic, we suggest running antivirus on the affected machines.

Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



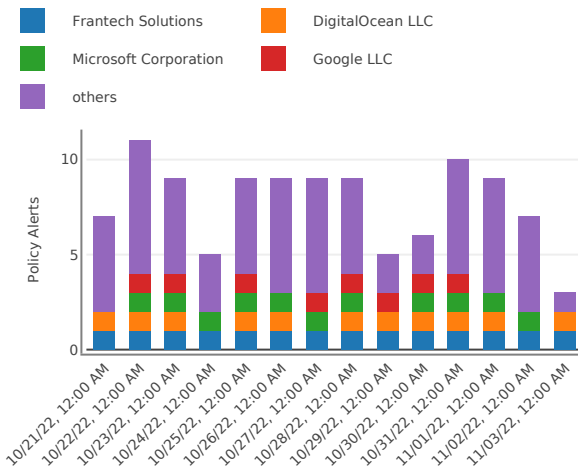
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



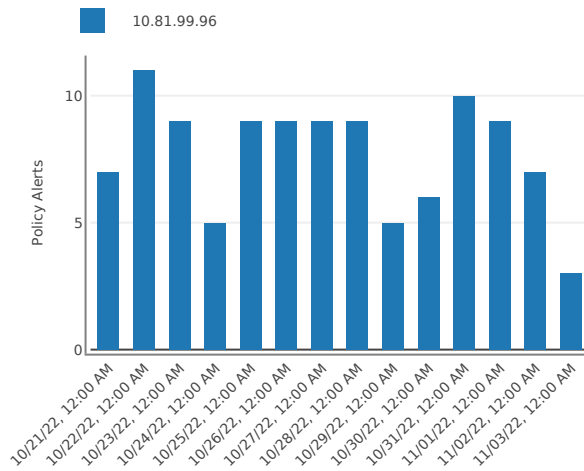
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.23 Unsecured Inbound Web Server Activity

Control Detail

This control alerts on flows from the public internet communicating with devices in your network over port 80. There are a wide variety of known attacks that target web servers on port 80. Because HTTP is a common unencrypted protocol, attackers know that port 80 is likely to be open. We recommend creating a zone for the devices in your network that you expect to have two-way web traffic with the external internet and applying this control to the rest of your network. [A.13.1.1 Network controls]

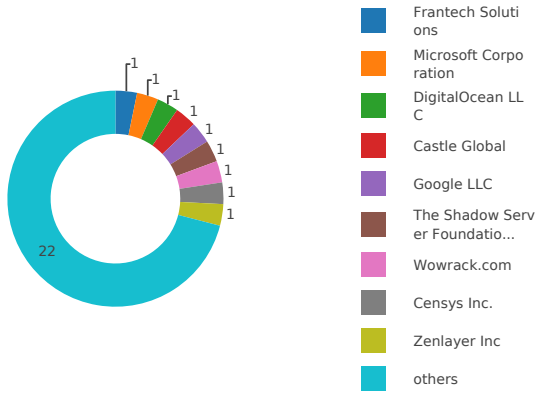
Remediation

We suggest using HTTPS to serve any publicly-facing content and closing port 80 whenever possible. If this alert was generated for a high-value device, we suggest investigating the source, destination, and traffic volume.

Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



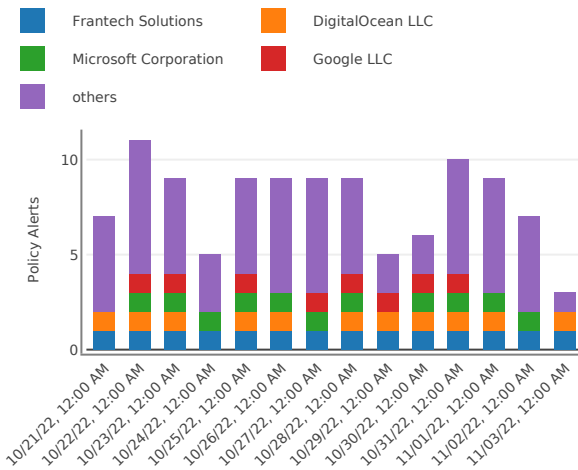
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



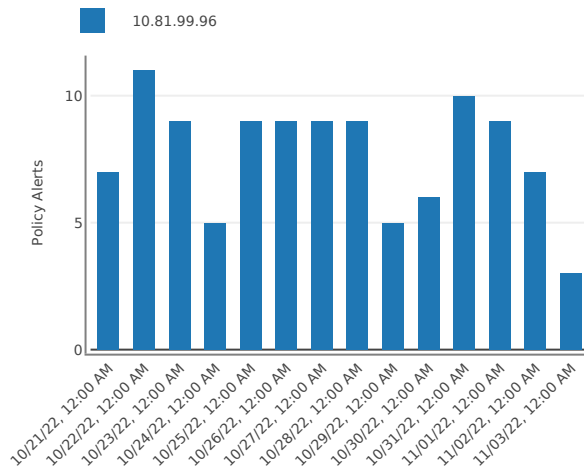
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.24 Unsecured Internal FTP/TFTP Traffic

Control Detail

FTP and TFTP are not encrypted file transfer protocols, and they are used by attackers to access and exfiltrate files. FTP and TFTP can also be used to load scripted attacks. There are more than 1200 recorded attacks that rely on FTP and TFTP. Using SFTP in place of these protocols significantly reduces your network's vulnerability. [A.13.1.1 Network controls]

Remediation

We suggest using SFTP in place of FTP/TFTP to ensure that your data is secured during transfer.

Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



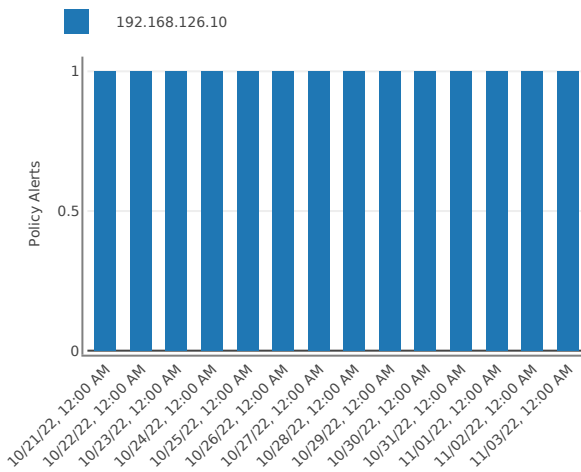
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



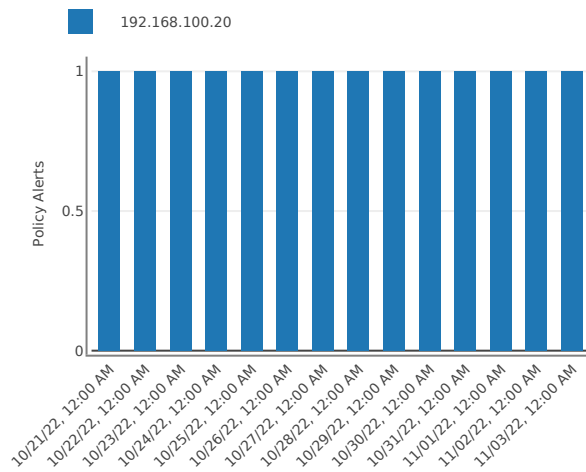
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.25 Unsecured Internal IRC Traffic

Control Detail

This control alerts on Internet Relay Chat (IRC) traffic from an address in the public internet to a device in your network. IRC is a plaintext protocol, meaning that anyone can read the contents of the packets. This can be used for device discovery. IRC is often used by botnets because it supports broadcast communication. It's unlikely that IRC has a valid business use case in your network, and we suggest closing the ports that it runs on - 194 and 6667. [A.13.1.1 Network controls]

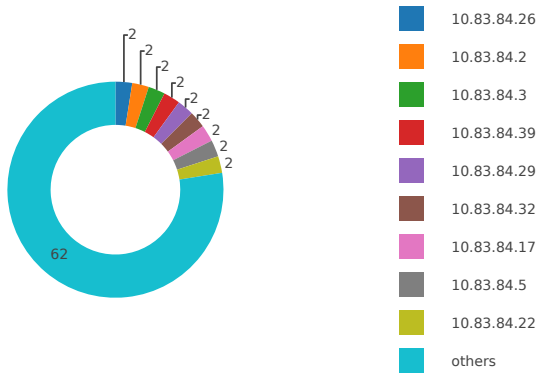
Remediation

We suggest disabling IRC on all your high-value devices and blocking traffic on ports 194 and 6667 from your perimeter firewalls.

Alert Detail

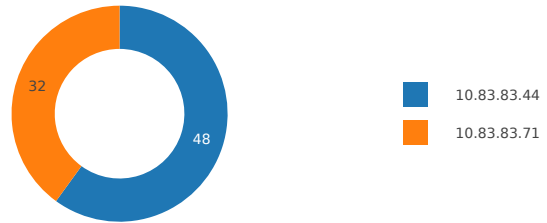
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



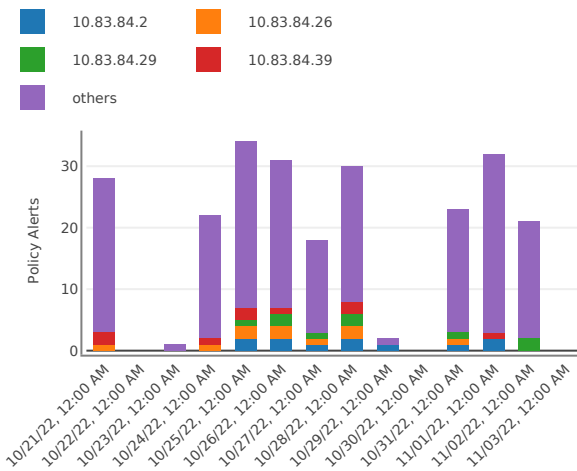
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



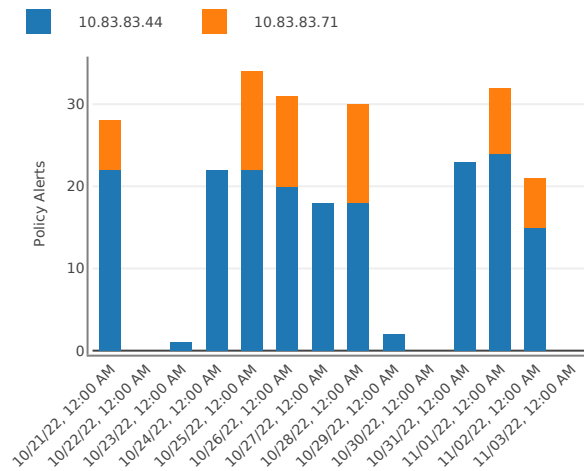
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.26 Unsecured Internal SNMP Traffic

Control Detail

Simple Network Management Protocol (SNMP) is a plaintext protocol used for network device management and discovery. It was designed with strong trust assumptions before the public internet was widespread, and it offers a convenient opportunity for hackers to obtain information about your network and the devices it contains. [A.13.1.1 Network controls]

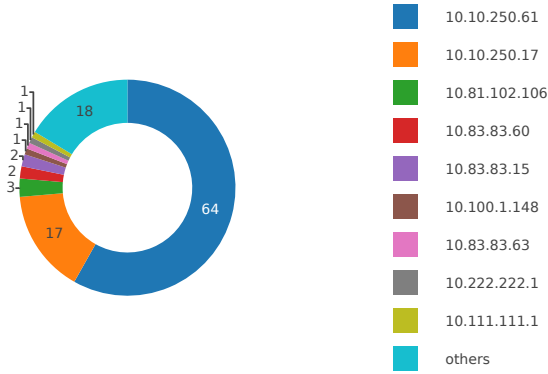
Remediation

We suggest blocking ports 161 and 162 on your perimeter firewalls. We also suggest disabling SNMP on all high-value devices in your network. How to disable SNMP: 1. Remove the SNMP agent or turn off the SNMP service 2. If shutting off SNMP is not an option, upgrade to SNMPV3, which encrypts passwords and messages 4. On Windows machines, implement the Group Policy security option called "Additional restrictions for anonymous connections" 5. Ensure that access to null session pipes, null session shares, and IPSec filtering is restricted.

Alert Detail

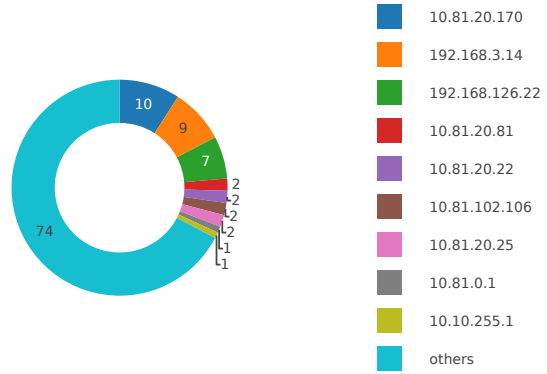
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



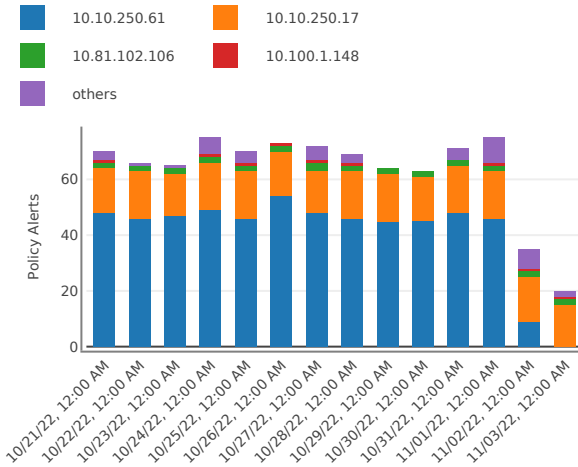
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



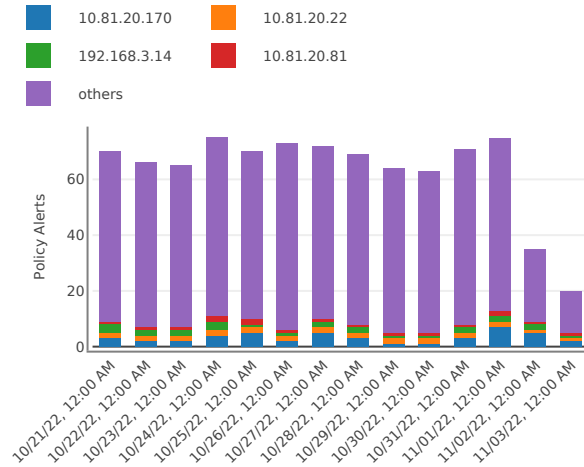
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.28 Unsecured Internal Web Server Activity

Control Detail

This control alerts on traffic within your network on TCP port 80. There are a wide variety of known attacks that target web servers on port 80. Because HTTP is a common unencrypted protocol, attackers know that port 80 is likely to be open and it is commonly used in attacks. [A.13.1.1 Network controls]

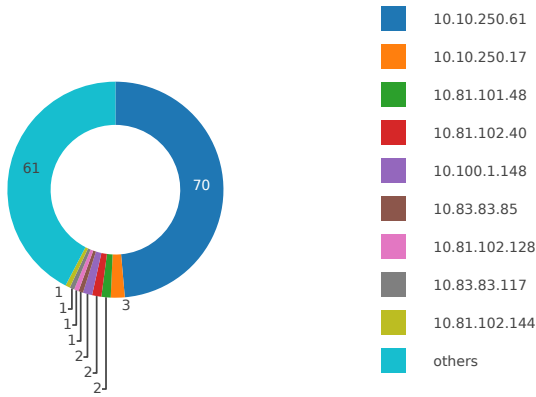
Remediation

We suggest using HTTPS to serve any publicly-facing content and closing port 80 whenever possible. If this alert was generated for a high-value device, we suggest investigating the source, destination, and traffic volume.

Alert Detail

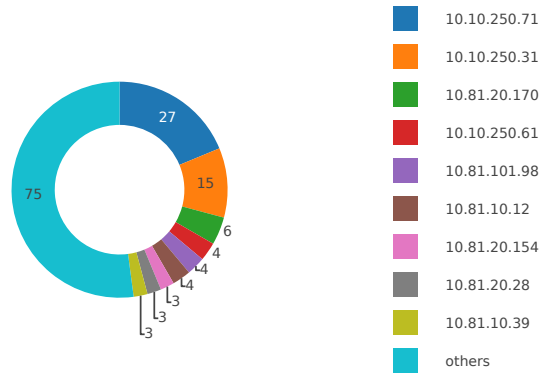
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



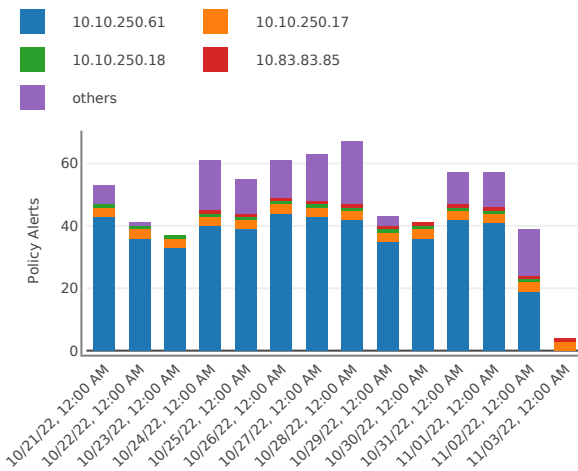
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



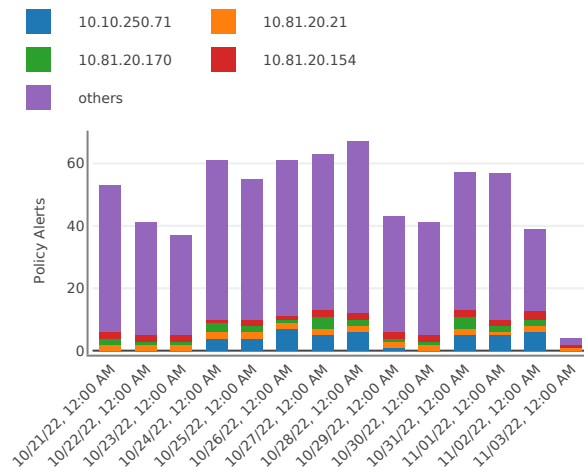
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



3.34 Unusual connection count from Internal to External

Control Detail

An unusual connection count between an internal IP address to an external domain is varying from its unusual baseline and this could indicate attack activity, system take-over, security breach, data exfiltration or C&C communication. This is a sensitive control, but it allows you to monitor your high-value devices closely.

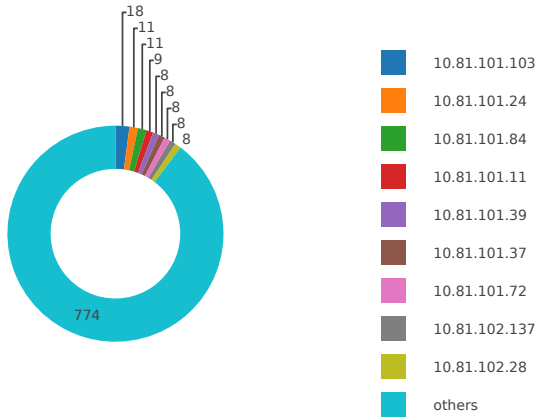
Remediation

We suggest investigating the following:\n1. Are the external domains IPs associated with a domain you expect to see traffic with?\n2. How much data was transferred? \n3. On which port did this activity occur? \n If you suspect this may have been attack activity, we suggest running an antivirus scan on the involved critical devices

Alert Detail

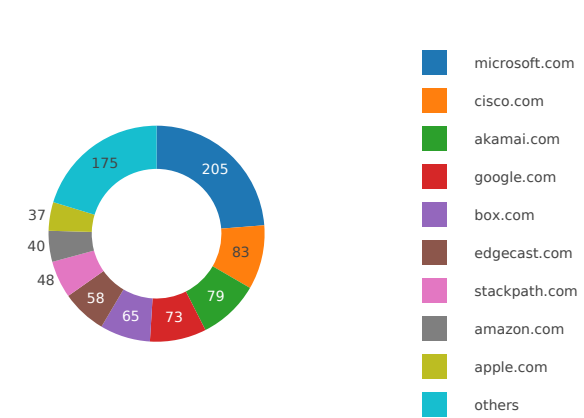
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



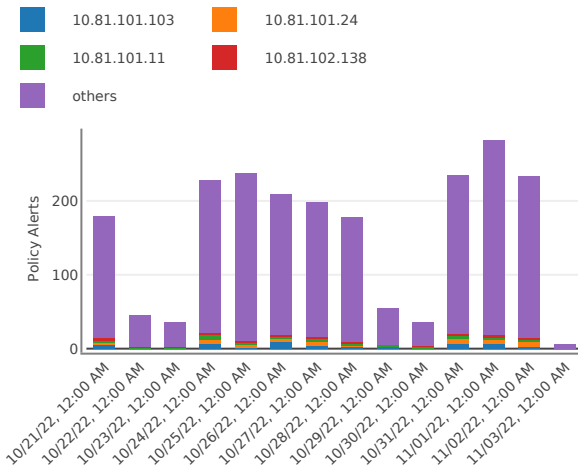
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations

