CyGlass

Cyber Essentials 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

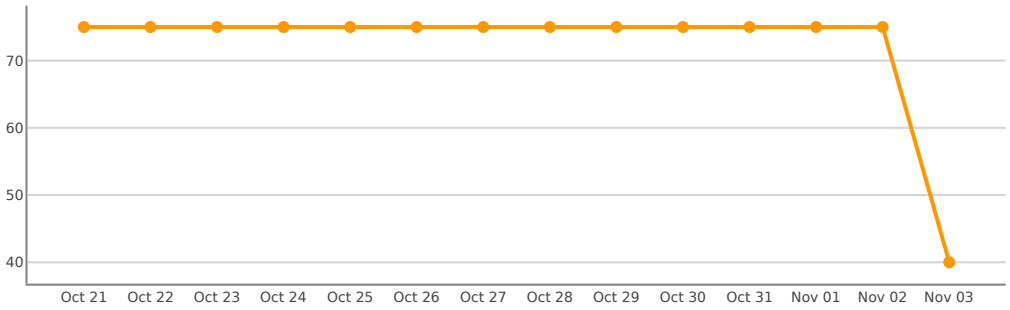
Legend

.....	Threshold
	No data available

75 Network Defense Overview

Threat Score

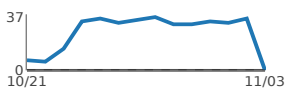
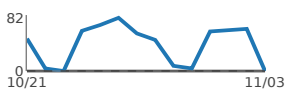
Threat Score History



3/4 Objectives are not compliant

24/59 Controls are not compliant

75 Top Network Threats

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	**1. Firewalls** **1.4 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
75	**5. User Access Control** **5.1 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.		0 Days
70	**1. Firewalls** **1.5 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

CyGlass

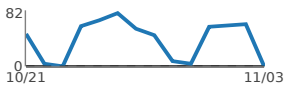
OBJECTIVE

1. Firewalls

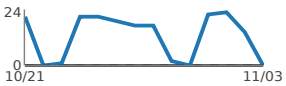
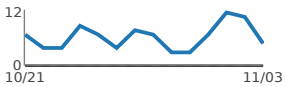
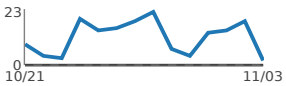
The Controls in this Objective address Cyber Essentials requirements for the Technical Control Theme Firewalls

75

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**1.1 Active Directory to External** Detect when Active Directory Servers are communicating improperly with the outside world on ports other than 53, 80, 123 or 443	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	**1.2 Activity Involving Blacklisted IPs** Detect traffic to or from Blacklisted IPs	Block all the malicious IP addresses at your perimeter firewall.		18 Days
0	**1.3 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	**1.4 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	**1.5 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	**1.6 Anomalous Activity from Blocked Countries** Detect when any anomalous events are detected due to communication from Blocked Countries	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	**1.7 Anomalous Activity to Blocked Countries** Detect when any anomalous events are detected communicating to Blocked Countries	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	**1.8 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	**1.9 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	**1.10 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	**1.11 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	**1.12 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
0	**1.13 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

0	**1.14 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
0	**1.15 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
0	**1.16 RDP Attempts from External to Internal** Detect when failed RDP sessions are attempted to be established into your network from an External IP	We recommend routing all legitimate external RDP connections through a VPN and blocking all incoming activity on port 3389.		18 Days
0	**1.17 RDP Connection from New External Host** Policy to monitor incoming connections from External Zone to Internal Zone where the external source IP connected over RDP to an internal IP for the first time.	We recommend routing all legitimate external RDP connections through a VPN and blocking all incoming activity on port 3389.		18 Days
0	**1.18 RDP from External to Internal** Detect when there are inbound RDP connections from an External IP	We suggest investigating this traffic and, if you suspect this may have been attack activity, block the external IP address on your perimeter security device.		18 Days
0	**1.19 SSH Attempts from External to Internal** Detect when failed SSH sessions are attempted to be established into your network from an External IP	We recommend routing all legitimate external SSH connections through a VPN and blocking all incoming activity on ports 3389 and 22.		18 Days
50	**1.20 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
30	**1.21 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
0	**1.22 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
0	**1.23 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
0	**1.24 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
23	**1.25 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
0	**1.26 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
0	**1.27 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

23	**1.28 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
28	**1.29 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
40	**1.30 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
40	**1.31 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
0	**1.32 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
23	**1.33 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
0	**1.34 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
0	**1.35 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
0	**1.36 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
0	**1.37 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

OBJECTIVE

2. Malware Protection

The Controls in this Objective address Cyber Essentials requirements for the Technical Control Theme Malware Protection

Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**2.1 AA21-356A - Detect potential Log4Shell Attacks to New Organizations via LDAP or RMI** As recommended in CISA Alert AA21-356A, this policy identifies LDAP and RMI activity to sites never before communicated with.	Upgrade the Java library of log4j to latest and stable version.		18 Days
0	**2.2 AA21-356A - Detect potential Log4Shell Attacks via LDAP or RMI** As recommended in CISA Alert AA21-356A, this policy identifies LDAP and RMI activity to known malicious IPs.	Upgrade the Java library of log4j to latest and stable version.		18 Days

0	**2.3 AA21-356A - Detecting unusual volume of DNS, LDAP or RMI activity due to potential Log4Shell Attacks** As recommended in CISA Alert AA21-356A, this policy identifies LDAP and RMI activity that is anomalous.	Upgrade the Java library of log4j to latest and stable version.		18 Days
0	**2.4 Beaconing Through Web API** 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.	We suggest quarantining any machines you suspect are running beaconing scripts as well as running anti-virus scans.		13 Days
0	**2.5 Communicate with Suspicious AA21-062AIPs** Volexity 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

-

OBJECTIVE

3. Secure Configuration

The Controls in this Objective address Cyber Essentials requirements for the Technical Control Theme Secure Configuration

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

4. Security Update Management

The Controls in this Objective address Cyber Essentials requirements for the Technical Control Theme Security Update Management

Not Compliant

There are no active controls in this objective.

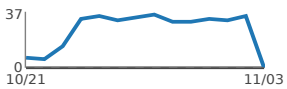
75

OBJECTIVE

5. User Access Control

The Controls in this Objective address Cyber Essentials requirements for the Technical Control Theme User Access Control

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	**5.1 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.		0 Days
70	**5.2 RDP Attempts from Internal to Internal** Detect when failed RDP sessions are attempted to be established within your network between two Internal IPs	We suggest investigating this traffic and, if you suspect this may have been attack activity, investigate the source device originating the ssh attempts.		0 Days
70	**5.3 SSH Attempts from Internal to Internal** Detect when failed SSH sessions are attempted to be established within your network between two Internal IPs	Identify the Internal IP address/source for SSH connection attempts.		0 Days
0	**5.4 Suspected Data Exfiltration through DNS** Unusually large volume of traffic is recorded from internal endpoints to external using the DNS protocol. This may be an indication of Data Exfiltration through DNS, one of ransomware related Command and Control activities.	We suggest ensuring all devices in your network are configured with your authorized DNS server and disabling DNS zone transfers to untrusted hosts. We also suggest investigating the volume of the DNS traffic that triggered these alerts to identify possible command and control or exfiltration activity.		18 Days
0	**5.5 Suspicious Access Location** A user has accessed resources on your network from a suspicious location. This could be a sign of internal malicious activity or account takeover	We recommend verifying that MFA and password complexity requirements are enabled for involved users and forcing a password reset.		18 Days
0	**5.6 Suspicious Access Time** A user has accessed resources on your network at a suspicious time. This could be a sign of internal malicious activity or account takeover	We recommend verifying that MFA and password complexity requirements are enabled for involved user accounts and forcing a password reset.		18 Days

0

5.7 Unusual Access Location For a VPN User

Alert when a VPN user is accessing the network from an unusual location. This may indicate that user's credentials have been compromised and were used for unauthorized VPN access.

We recommend contacting this user to validate their activity and forcing a password reset.

18 Days

0

5.8 Unusual Access Time For a VPN User

Alert when a VPN user is accessing the network at unusual times. This may indicate that user's credentials have been compromised and were used for unauthorized VPN access.

We recommend forcing a password reset for this account and contacting this user to validate their activity.

18 Days

5.9 Unusual Increase in Number of users logging in

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

5.10 Unusual Increase of User accounts whose password never expire

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

5.11 Unusual Increase of User accounts with Administrative Privileges

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

5.12 Unusual Increase of User accounts with password not required

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

CyGlass

Control Violation Detail and Remediation

1.4 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.

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

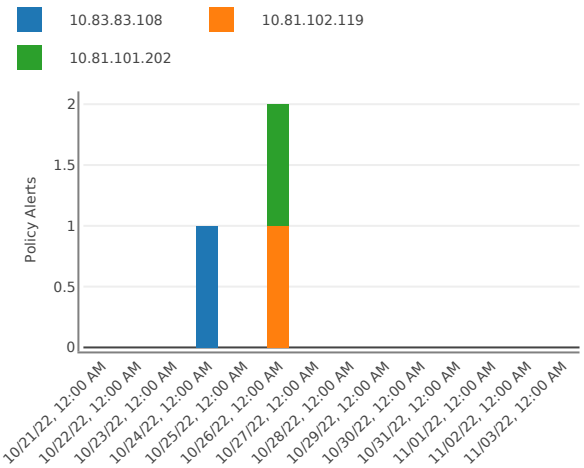
Number of unique destinations sources have raised violations for

Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

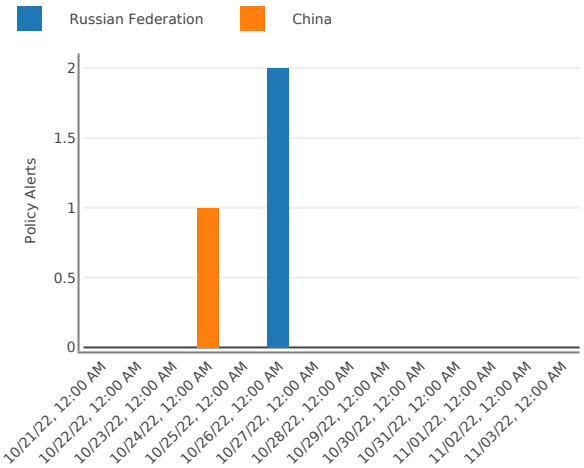
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.5 Activity to Social Media Sites

Control Detail

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

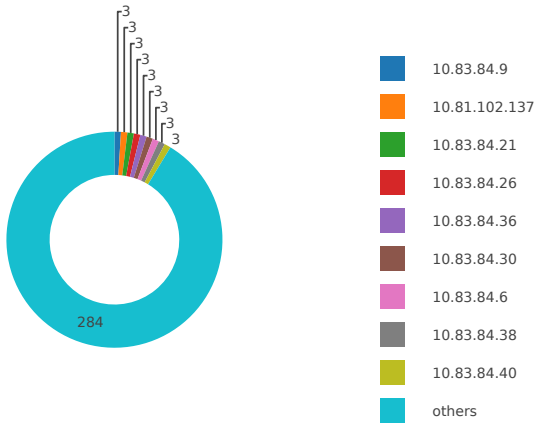
Remediation

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

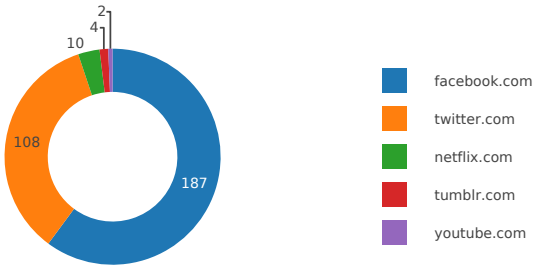
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



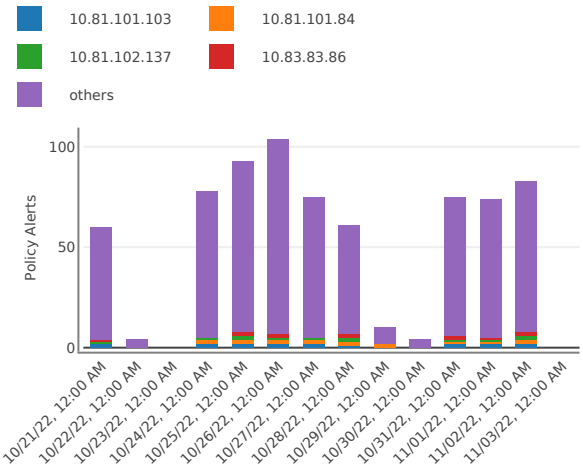
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



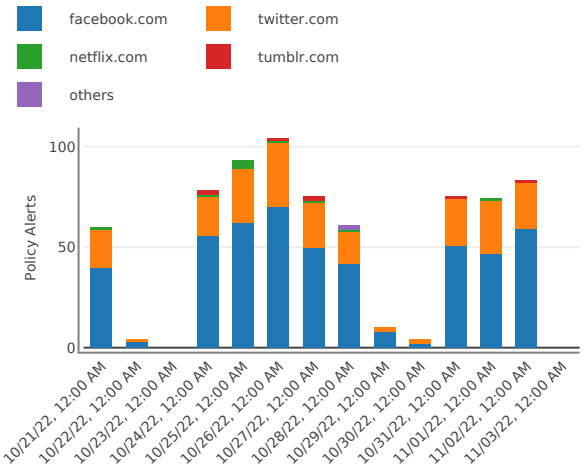
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.11 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.

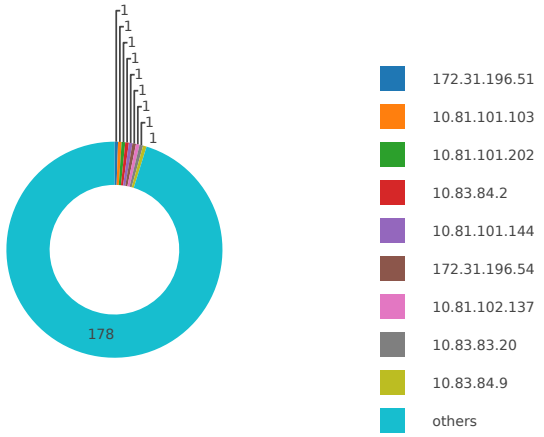
Remediation

Block accessing to Facebook to reduce the risk of data loss or increase productivity Ff 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

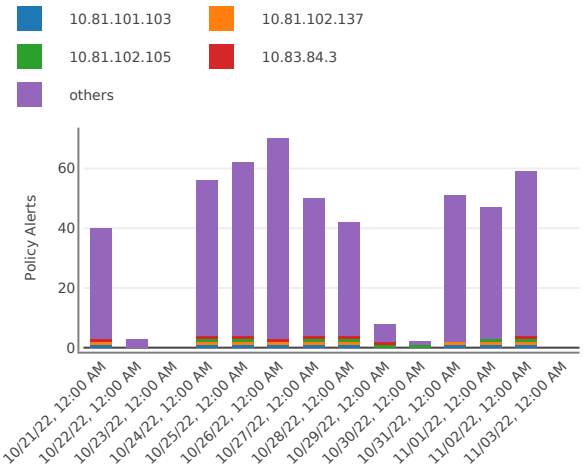


Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

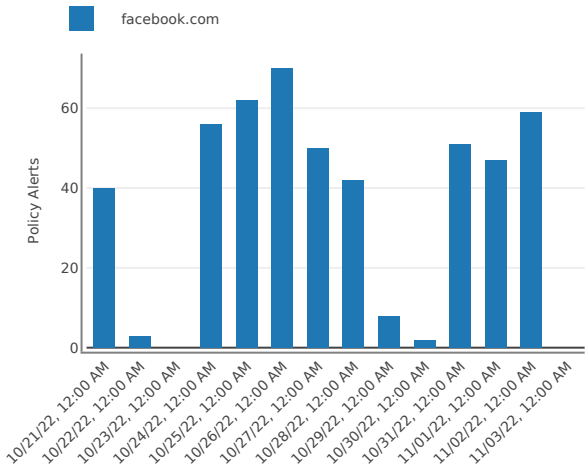
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.12 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.

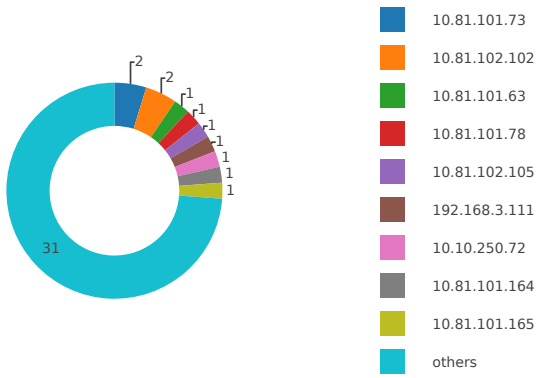
Remediation

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

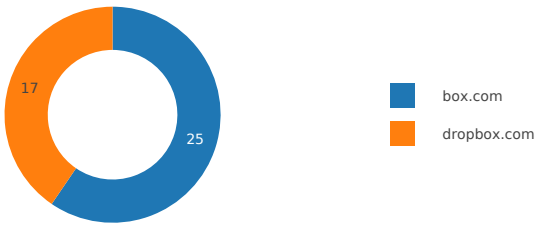
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



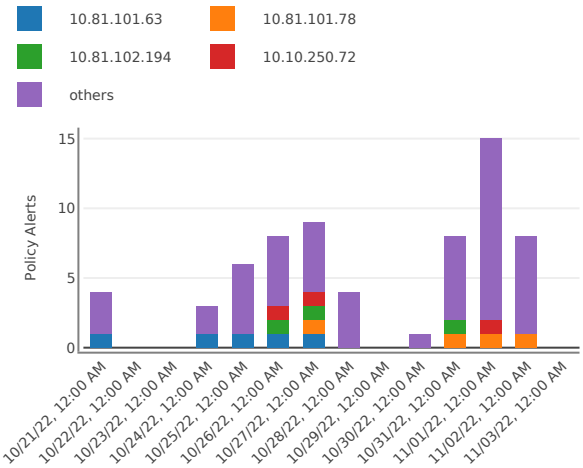
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



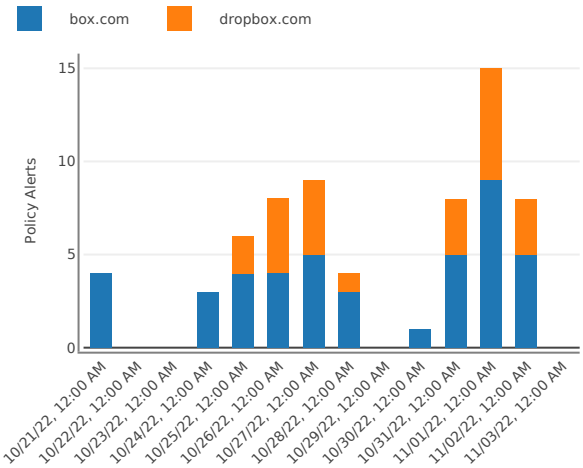
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



5.1 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.

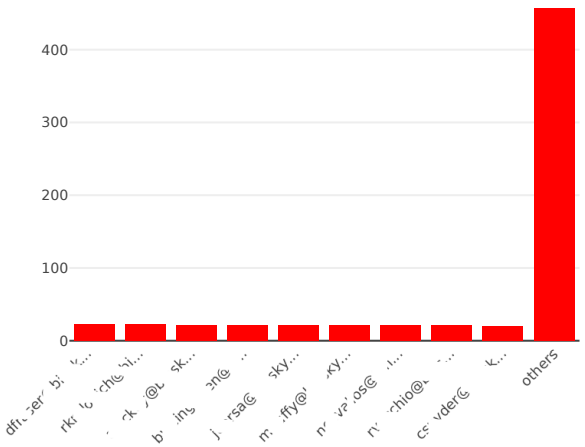
Remediation

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

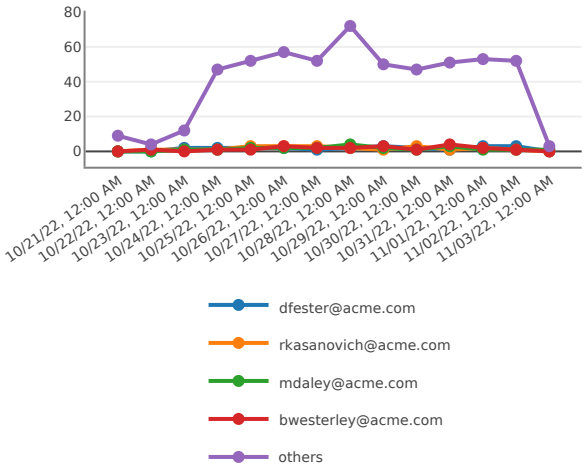
Distribution of Policy Alerts by User

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



5.2 RDP Attempts from Internal to Internal

Control Detail

An internal RDP failed connections attempts has been detected from an internal device within your network. This could indicate unauthorized an attempt to access your critical device that might be a threat.

Remediation

We suggest investigating this traffic and, if you suspect this may have been attack activity, investigate the source device originating the ssh attempts.

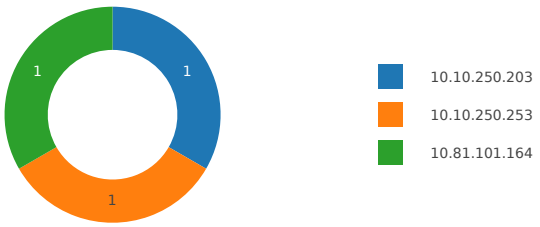
Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for

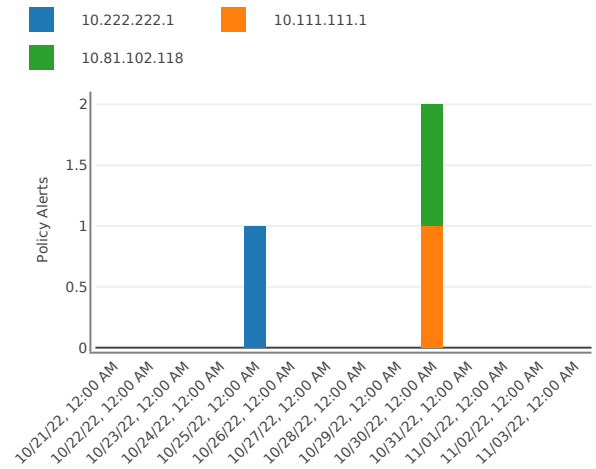
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



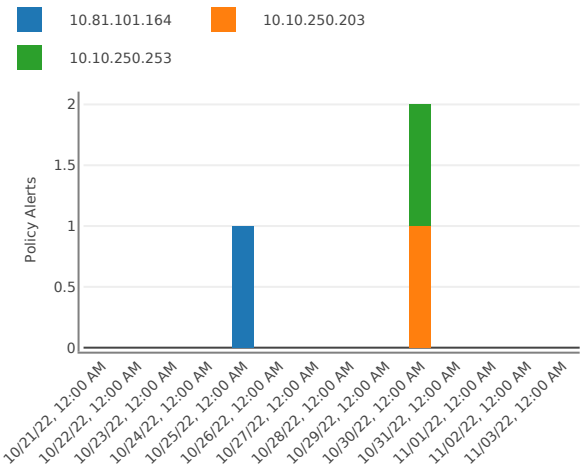
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



5.3 SSH Attempts from Internal to Internal

Control Detail

Detect when failed SSH sessions are attempted to be established within your network between two Internal IPs. Because SSH provides remote access into systems, it is critical that access be tracked and controlled. Since many organizations donâ€™t have centralized oversight and control of SSH, the risk of unauthorized access is increased.

Remediation

Identify the Internal IP address/source for SSH connection attempts , if you suspect this as malicious activity , isolate the PC from the network and run antivirus scan on it.

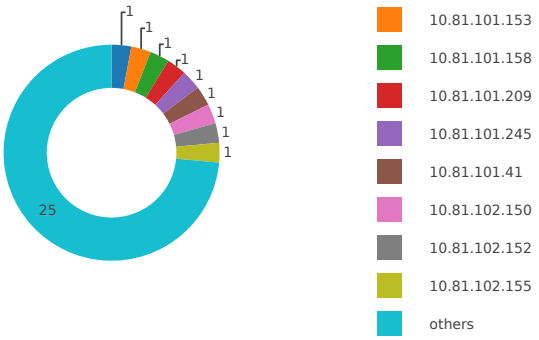
Alert Detail

Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for

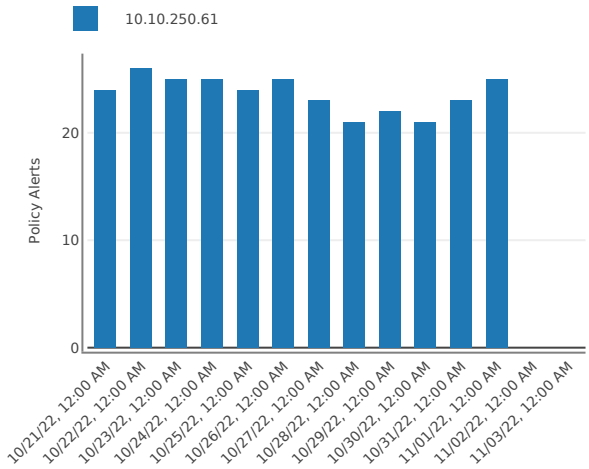
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



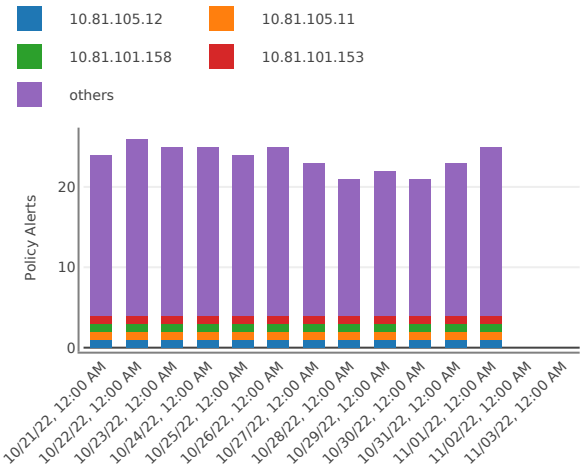
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.20 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.

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

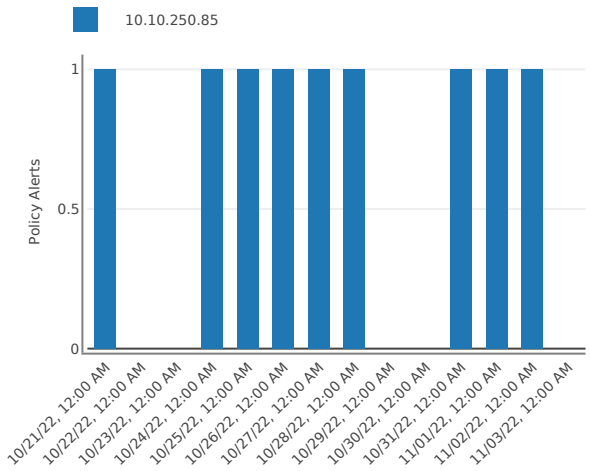
Number of unique destinations sources have raised violations for

Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

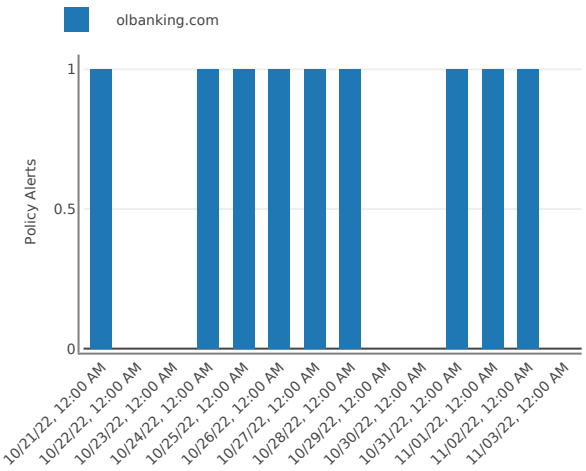
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.21 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.

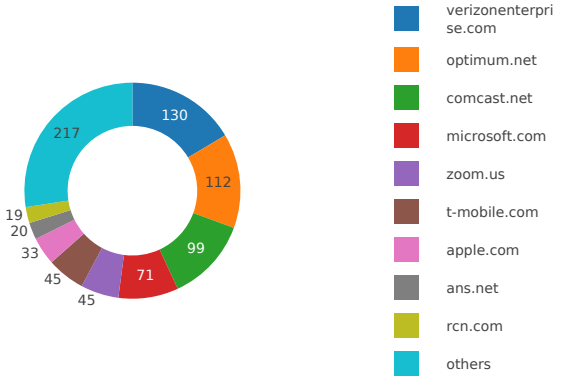
Remediation

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

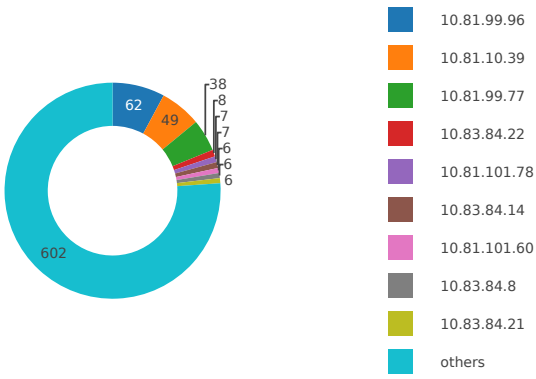
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



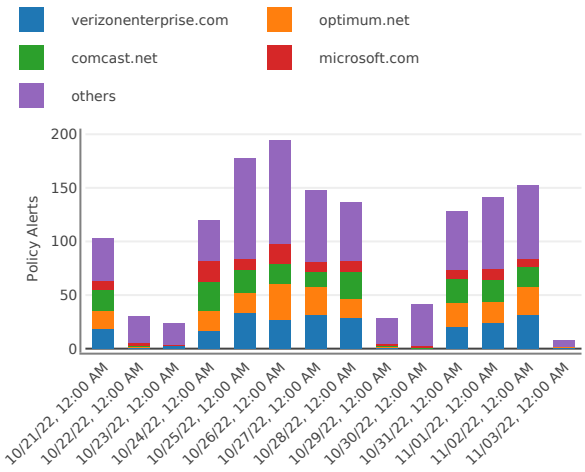
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



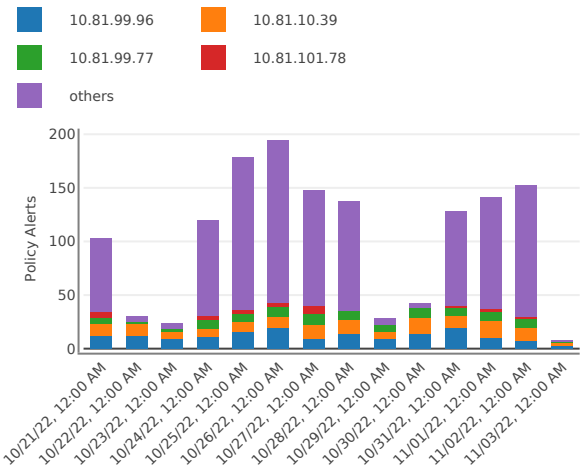
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.25 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.

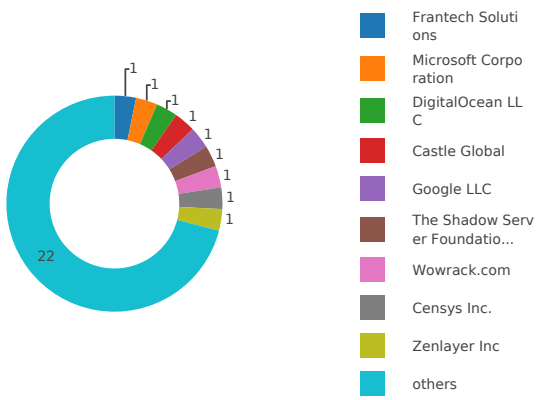
Remediation

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

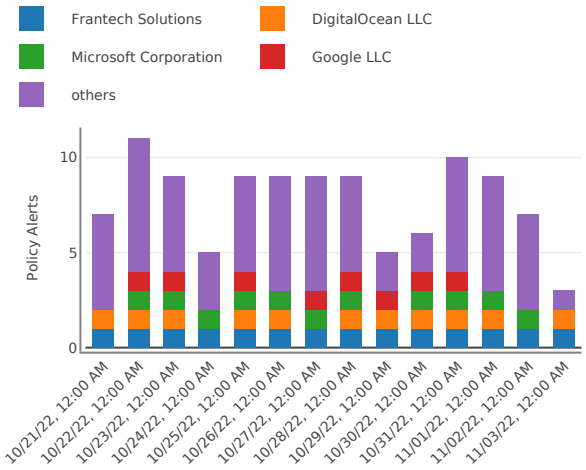


Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

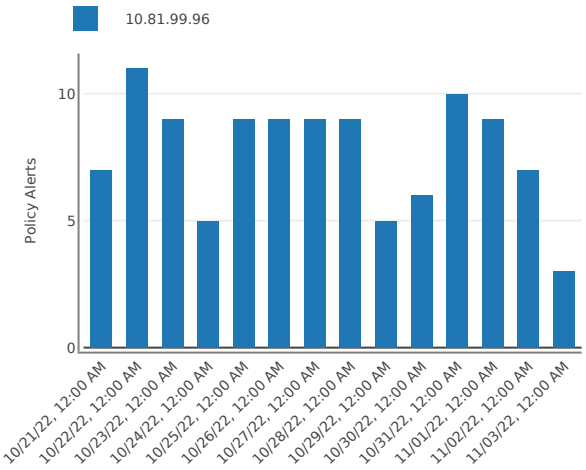
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.28 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.

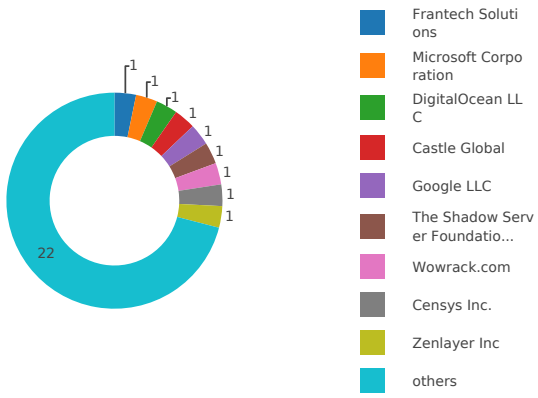
Remediation

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

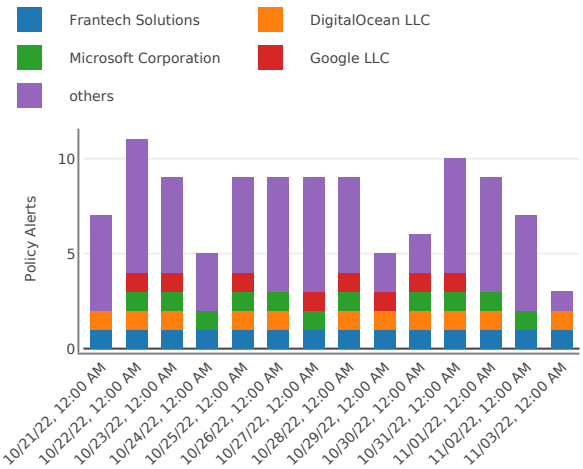


Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

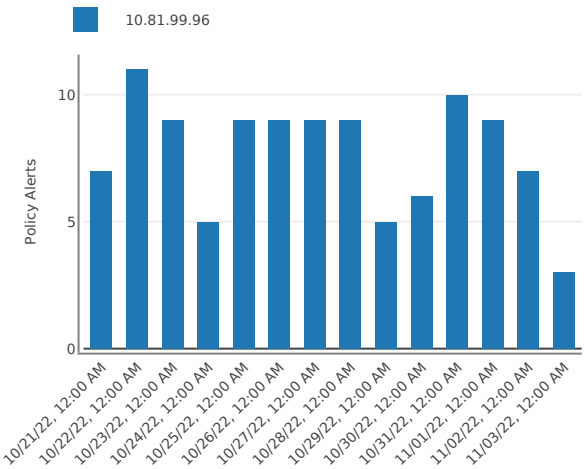
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.29 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.

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

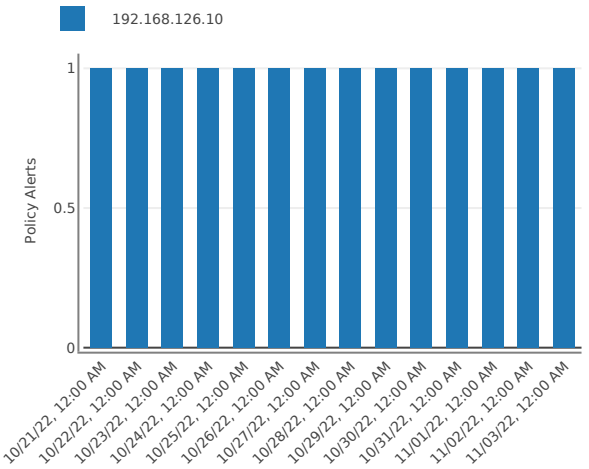
Number of unique destinations sources have raised violations for

Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

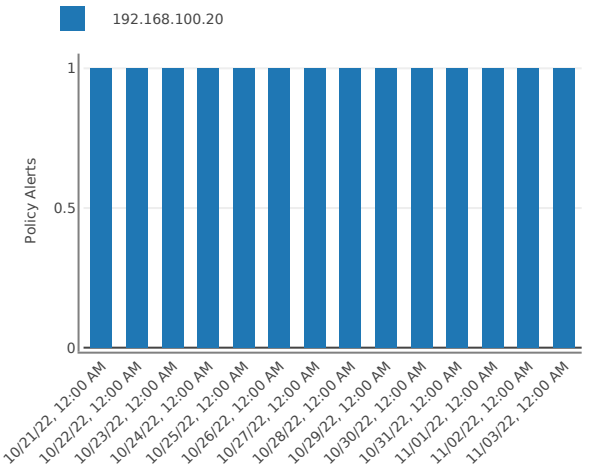
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.30 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.

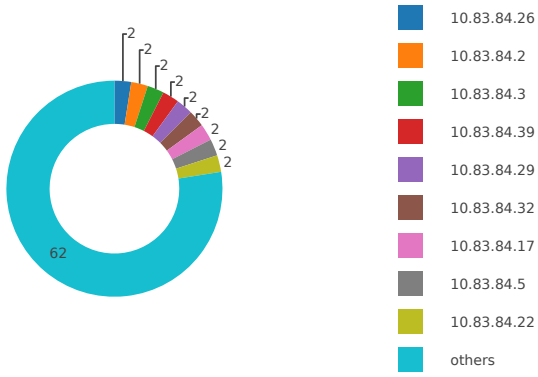
Remediation

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

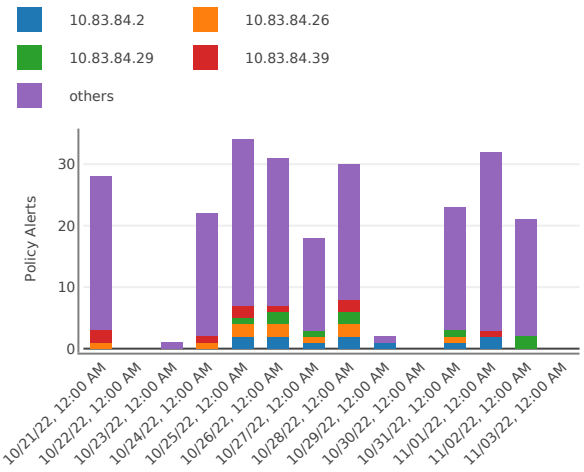


Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

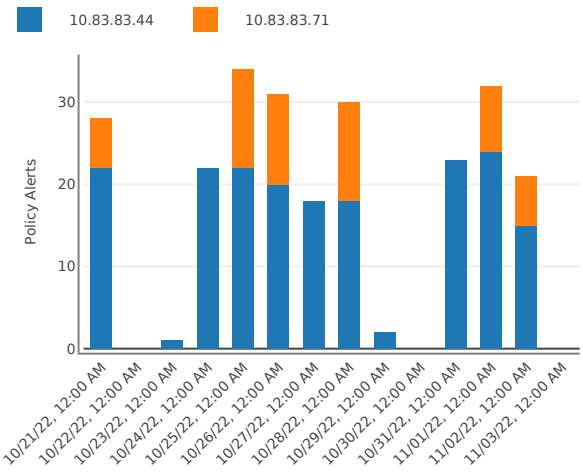
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.31 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.

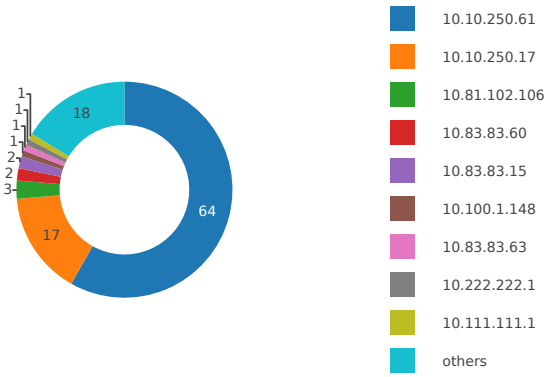
Remediation

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

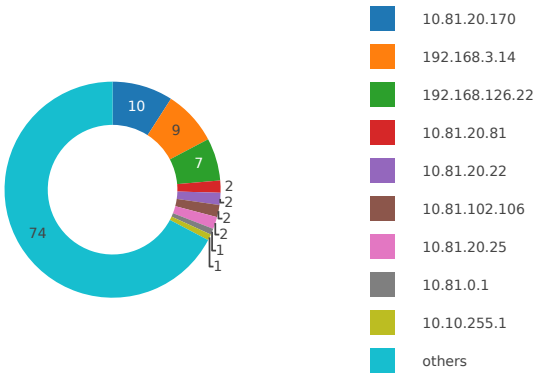
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



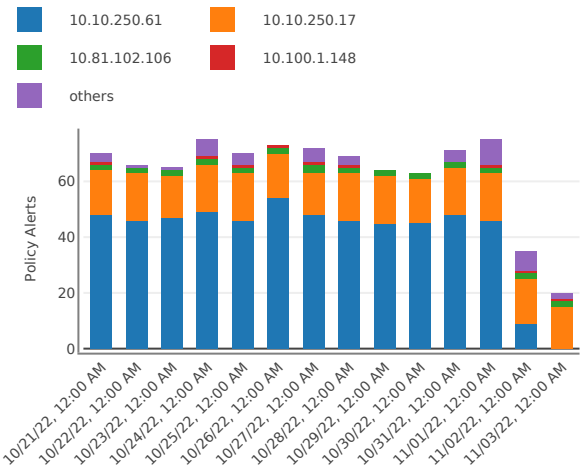
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



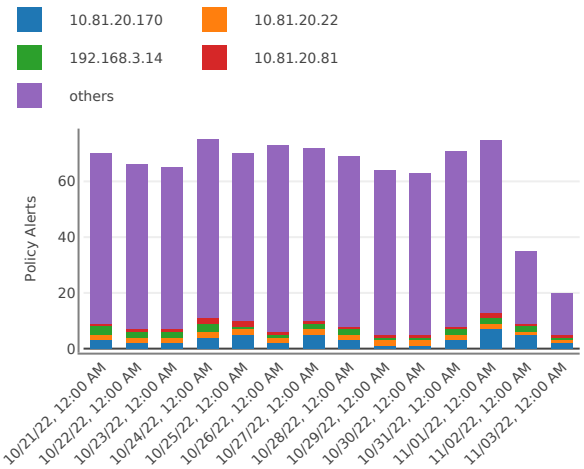
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



1.33 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.

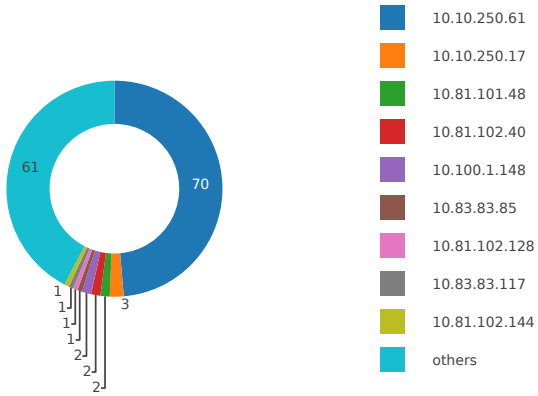
Remediation

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

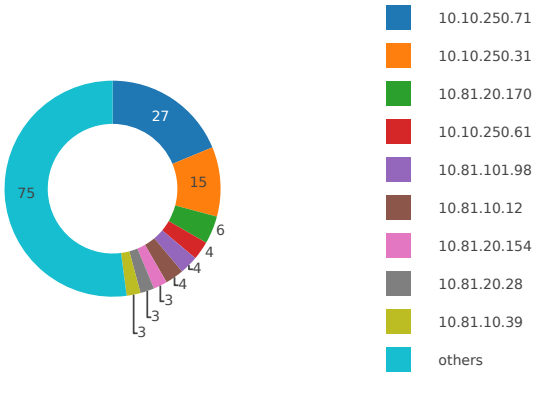
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



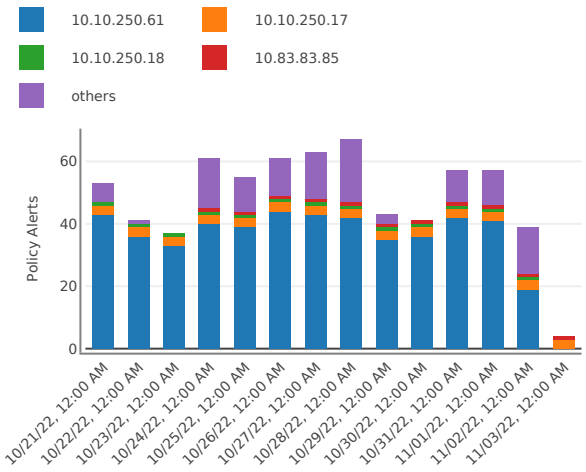
Distribution of Policy Alerts by Destination

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