ISO 27001:2022 Compliance Report

Acme Inc.

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

Time Period

From:	May 03, 2024
To:	May 30, 2024
Generated:	May 31, 2024
Period:	28 Days

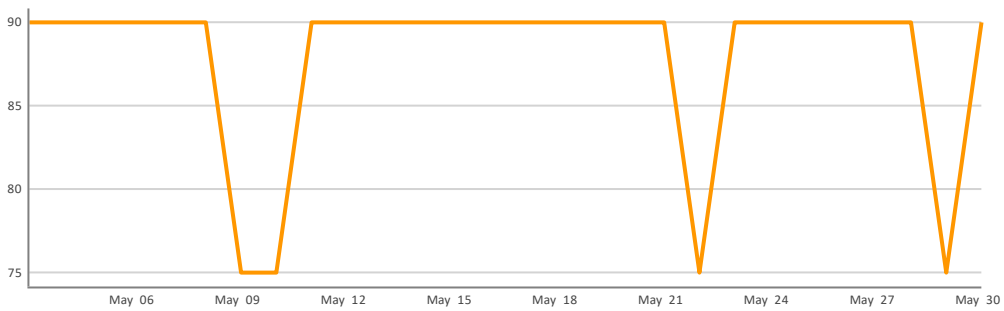
Legend

… … …	Threshold
	No data available

90 Network Defense Overview

Threat Score

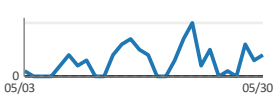
Threat Score History



7/8 Objectives are not compliant

31/58 Controls are not compliant

90 Top Network Threats

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
90	A.5.9: Inventory of information and other associated assets Internal Server Disruption An internal server witnessed a service disruption.	Identify the reason behind break of periodic activity and take action to mitigate the business risk.		0 Days
90	A.8.20 Networks security 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.		0 Days
75	A.5.15: Access Control 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

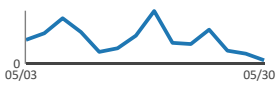
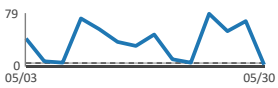
OBJECTIVE

A.5.9: Inventory of information and other associated assets

90

The Controls in this Objective address ISO 27001:2022 requirements for Section A.5.9: Inventory of information and other associated assets with the Objective: To identify organizational assets and define appropriate protection responsibilities.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
90	**Internal Server Disruption** An internal server witnessed a service disruption.	Identify the reason behind break of periodic activity and take action to mitigate the business risk.		0 Days
70	**Internal Server Discovery** An internal server was discovered.	This controls provide visibility within your network to identify any rogue devices and c&c communications.		0 Days
90	**External Server Disruption** An external server witnessed a service disruption.	Identify the reason behind break of periodic activity and take action to mitigate the business risk.		0 Days
70	**External Server Discovery** An external server was discovered.	This controls provide visibility within your network to identify any rogue devices and c&c communications.		0 Days

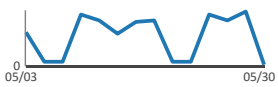
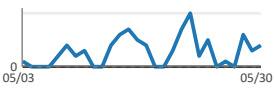
OBJECTIVE

A.5.15: Access Control

75

The Controls in this Objective address ISO 27001:2022 requirements for Section A.5.15: Access Control with the Objective: To limit access to information and information processing facilities.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
70	**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
70	**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
0	**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.		182 Days
0	**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.		182 Days
0	**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.		182 Days
70	**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
75	**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	**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
0	**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.		106 Days

OBJECTIVE

A.5.29 Information security during disruption

The Controls in this Objective address ISO 27001:2022 requirements for A.5.29 Information security during disruption with the Objective: Information security continuity shall be embedded in the organizationâ s business continuity management systems.

Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**Internal Backup Server Disruption** Regular backups to an internal server from internal devices was discontinued. Stopping or changing backups is a common part of ransomware attacks.	We recommend re-running any interrupted or stopped backup processes and investigating the cause of the disruption to your periodic backup.		106 Days
0	**External Backup Server Disruption** Regular backups to an external server from internal devices was discontinued. Stopping or changing backups is a common part of ransomware attacks.	We recommend re-running any interrupted or stopped backup processes and investigating the cause of the disruption to your periodic backup.		106 Days

OBJECTIVE

A.8.2 Privileged access rights

The Controls in this Objective address ISO 27001:2022 requirements for Section A.8.2 Privileged access rights with the Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

Not Compliant

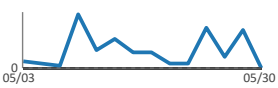
THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
70	**Unusual Increase of User accounts with Administrative Privileges** A significant increase in the number of users with administrative privileges has been detected.	We recommend reviewing any new accounts recently created with administrative privileges to assure they are authorized.		0 Days

OBJECTIVE

A.8.5 Secure authentication

The Controls in this Objective address ISO 27001:2022 requirements for Section A.8.5 Secure authentication with the Objective: To prevent unauthorized access to systems and applications.

Not Compliant

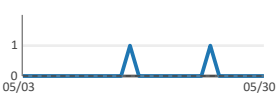
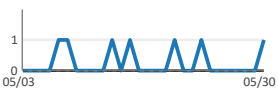
THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	**Possible Brute Force Account Access Attempt** Detect a user has attempted and failed to log into resources on your network multiple times	We recommend enabling multi-factor authentication and enforcing password complexity requirements.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

OBJECTIVE

A.8.15 Logging

The Controls in this Objective address ISO 27001:2022 requirements for A.8.15 Logging with the Objective: To record events and generate evidence.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
70	**Unusual Increase in Number of user accounts deleted** A significant increase in the number of user accounts deleted has been detected.	Validate deleted user accounts.		0 Days
70	**Unusual Increase in Number of user accounts created** A significant increase in the number of user accounts created has been detected.	Validate the newly created user accounts. Ensure users have limited access by default and provide privileges on a need basis only.		0 Days
70	**Unusual Increase in Number of computer accounts deleted** A significant increase in the number of computer accounts deleted has been detected.	Validate the reason for removing multiple computer accounts which were deleted.		0 Days
70	**Unusual Increase in Number of computer accounts created** A significant increase in the number of computer accounts created has been detected.	We recommend validating all new computer accounts created.		0 Days
70	**Unusual Increase in Number of Empty security groups** A significant increase in the number of empty security groups has been detected.	We recommend reviewing all empty security groups and identify the reason for users removed from security groups		0 Days

OBJECTIVE

A.8.19 Installation of software on operational systems

The Controls in this Objective address ISO 27001:2022 requirements for Section A.8.19 Installation of software on operational systems ewith the Objective: To ensure the integrity of operational systems.

Compliant

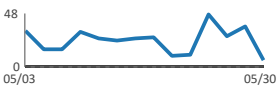
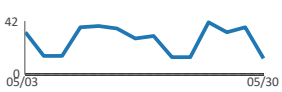
THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**WUDO Traffic Crossing Network Boundary** Detects Windows Update Delivery Optimization (WUDO) traffic between devices within your network and the public internet.	Identify the devices communicating on WUDO port 7680 and scan the machines with antivirus and investigate the destination domains are allowed in your network.		106 Days

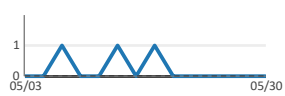
OBJECTIVE

A.8.20 Networks security

The Controls in this Objective address ISO 27001:2022 requirements for Section A.8.20 Networks security 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	**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.		106 Days
70	**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
0	**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.		106 Days
0	**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.		106 Days
0	**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.		76 Days
0	**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.		106 Days
0	**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		106 Days
23	**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	**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.		106 Days

40	**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	**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.		106 Days
0	**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.		106 Days
0	**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.		106 Days
0	**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.		76 Days
0	**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.		106 Days
23	**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	**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.		76 Days
0	**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.		106 Days
0	**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		106 Days
30	**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	**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.		106 Days
0	**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		106 Days
0	**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.		106 Days

0	**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.		106 Days
0	**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.		106 Days
0	**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.		84 Days
0	**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.		106 Days
0	**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.		27 Days
60	**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.		0 Days
0	**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.		89 Days
0	**Activity Involving Blacklisted IPs** Detect traffic to or from Blacklisted IPs	Block all the malicious IP addresses at your perimeter firewall.		106 Days
0	**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.		106 Days
0	**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.		106 Days
0	**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.		106 Days
0	**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.		106 Days

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.

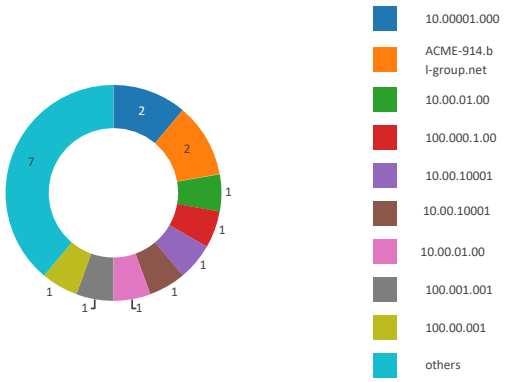
Remediation

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

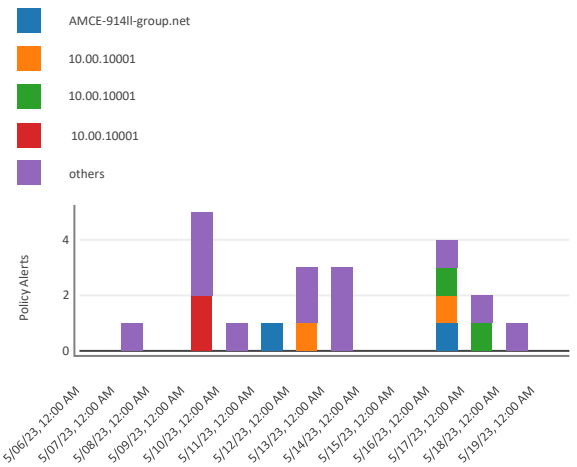
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



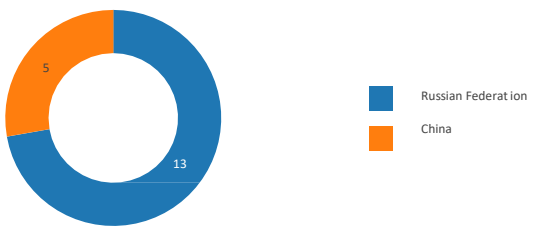
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



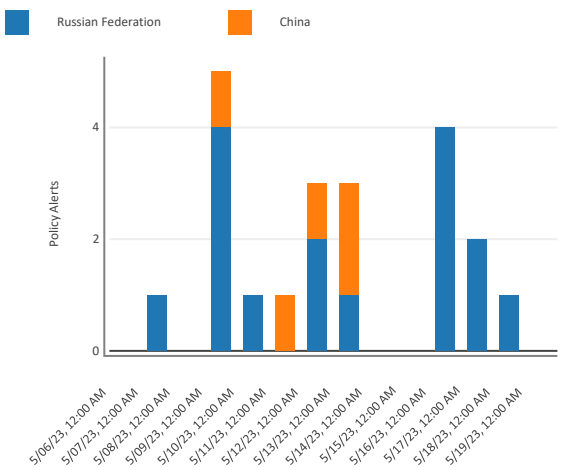
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations

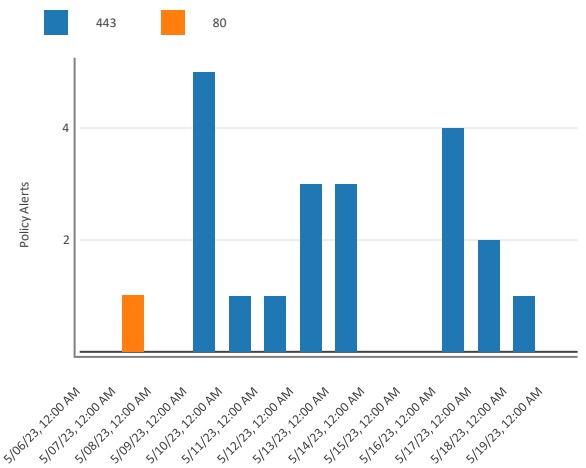


Distribution of Policy Alerts by Application Port

Number of Application Port raised violations for

Distribution of Policy Alerts over Time by Application Port

Timeline of alerts count involving affected Application Port



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.

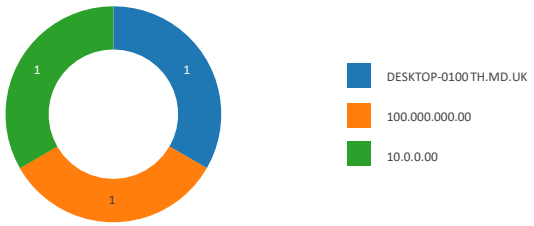
Remediation

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

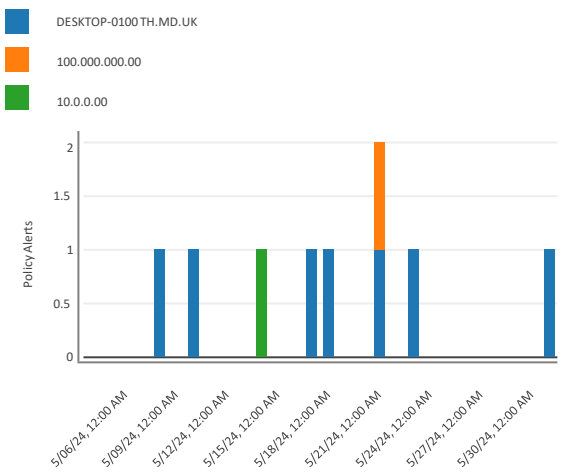
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources

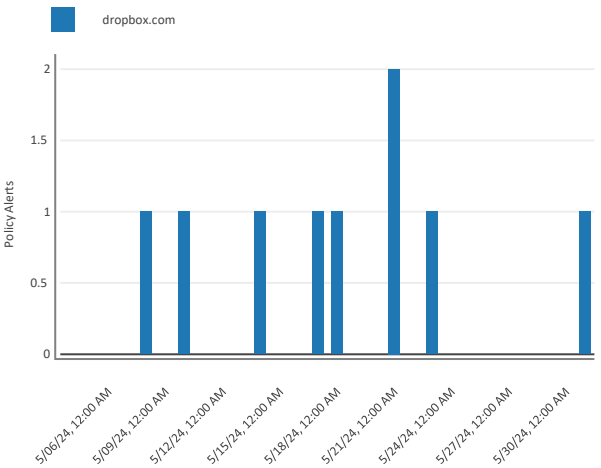


Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations

Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations

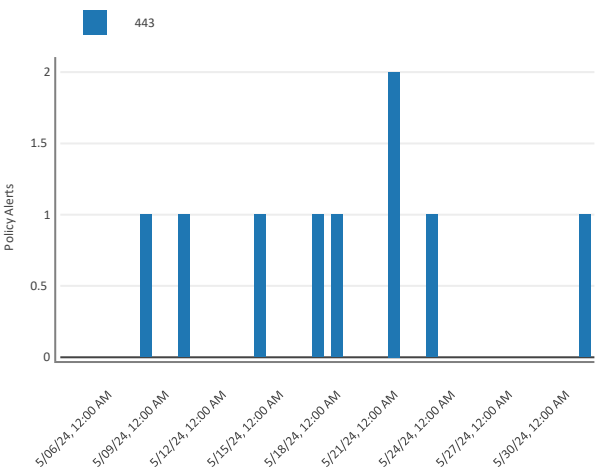


Distribution of Policy Alerts by Application Port

Number of Application Port raised violations for

Distribution of Policy Alerts over Time by Application Port

Timeline of alerts count involving affected Application Port



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.

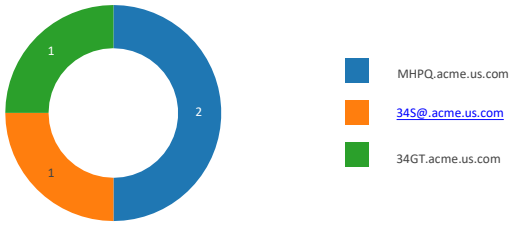
Remediation

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

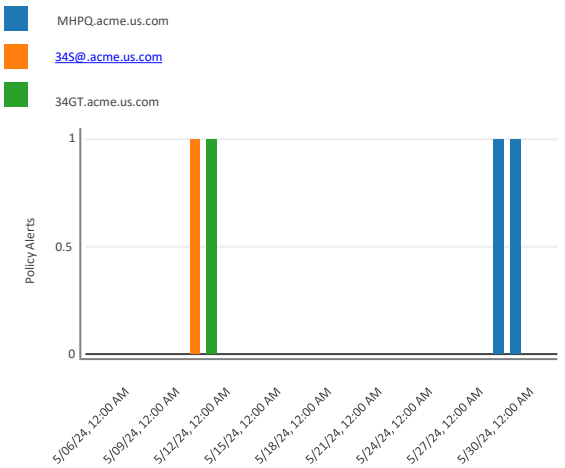
Distribution of Policy Alerts by Source

Number of unique destinations sources have raised violations for



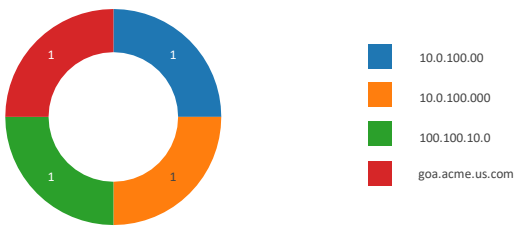
Distribution of Policy Alerts over Time by Source

Timeline of alerts count involving affected sources



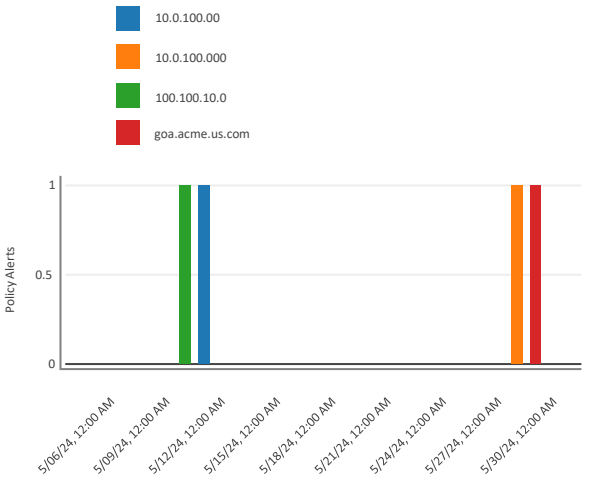
Distribution of Policy Alerts by Destination

Number of unique sources that have raised violations against destinations



Distribution of Policy Alerts over Time by Destination

Timeline of alerts count involving affected destinations



Distribution of Policy Alerts by Application Port

Number of Application Port raised violations for

Distribution of Policy Alerts over Time by Application Port

Timeline of alerts count involving affected Application Port