Electric bird

Threat Protection Performance Report for Contoso

Publication Date:

Nov 2020

Table of Contents

Executive Summary

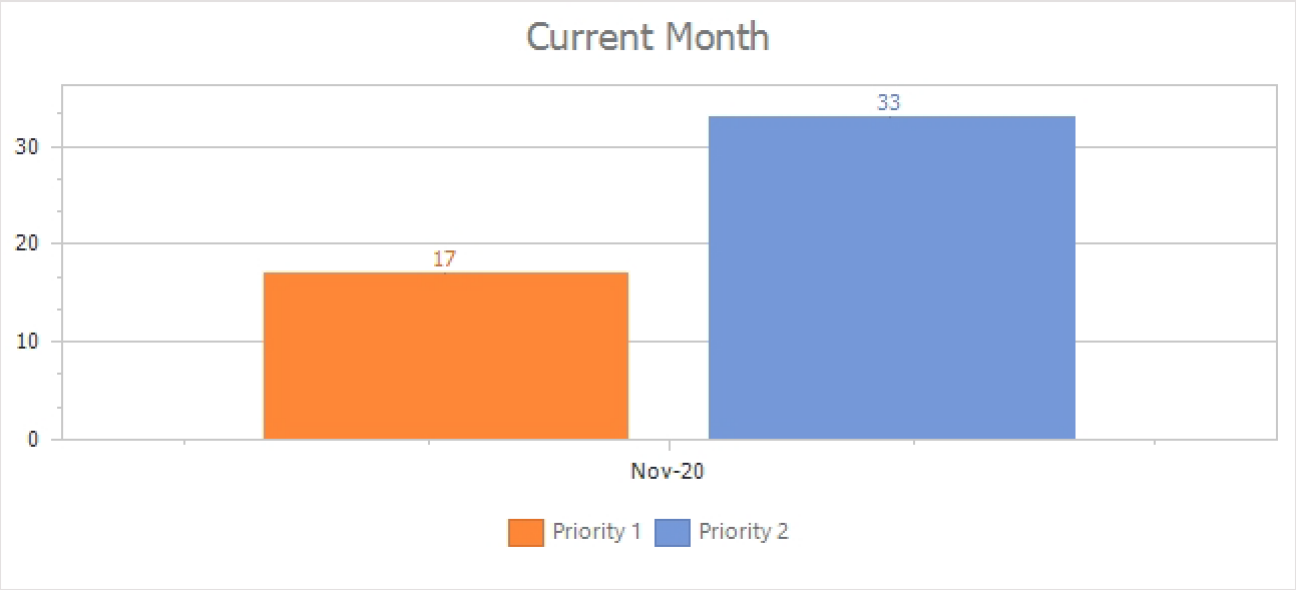
This report provides business summary and observations on the current security posture of the customer's environment. This includes trends, statistics, and metrics of security operations. Additional details can be found in the appendices.

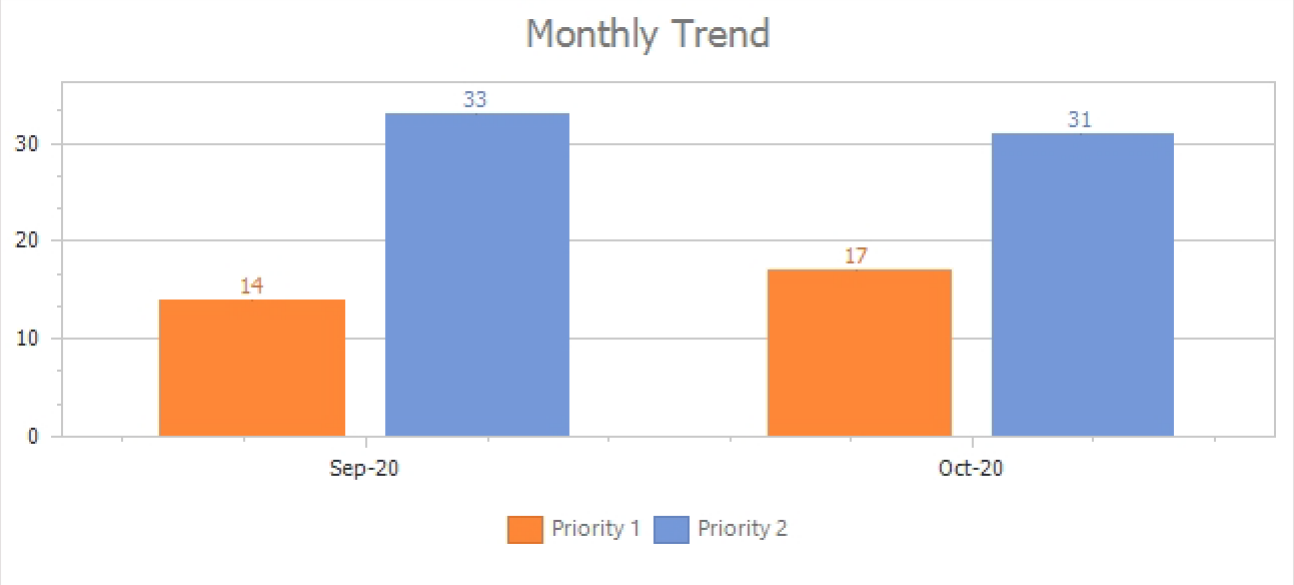
Report created on: 12/10/2020 5:56:24 PM From: 11/1/2020 12:00:00 AM

Interval: Previous 1 month To: 11/30/2020 11:59:59 PM

Monitoring Alert Statistics

Count as per the severity of alerts for the month of Nov 2020 and the last 2 months trend.

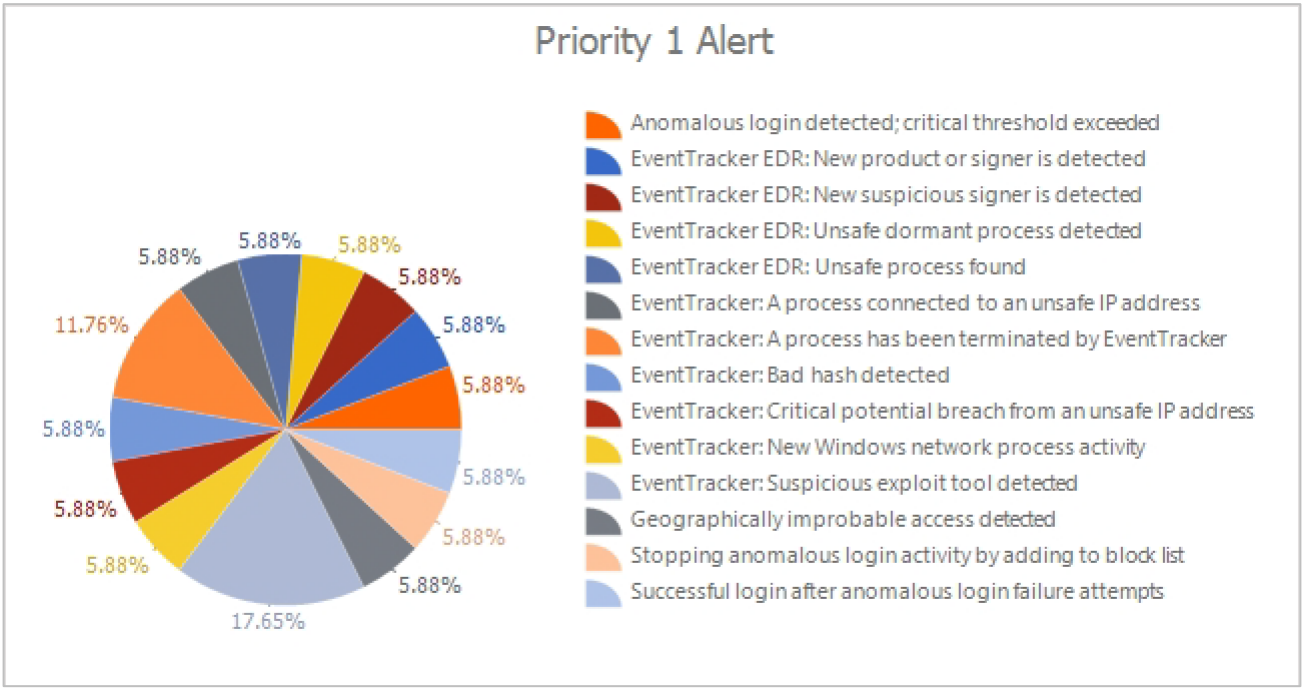




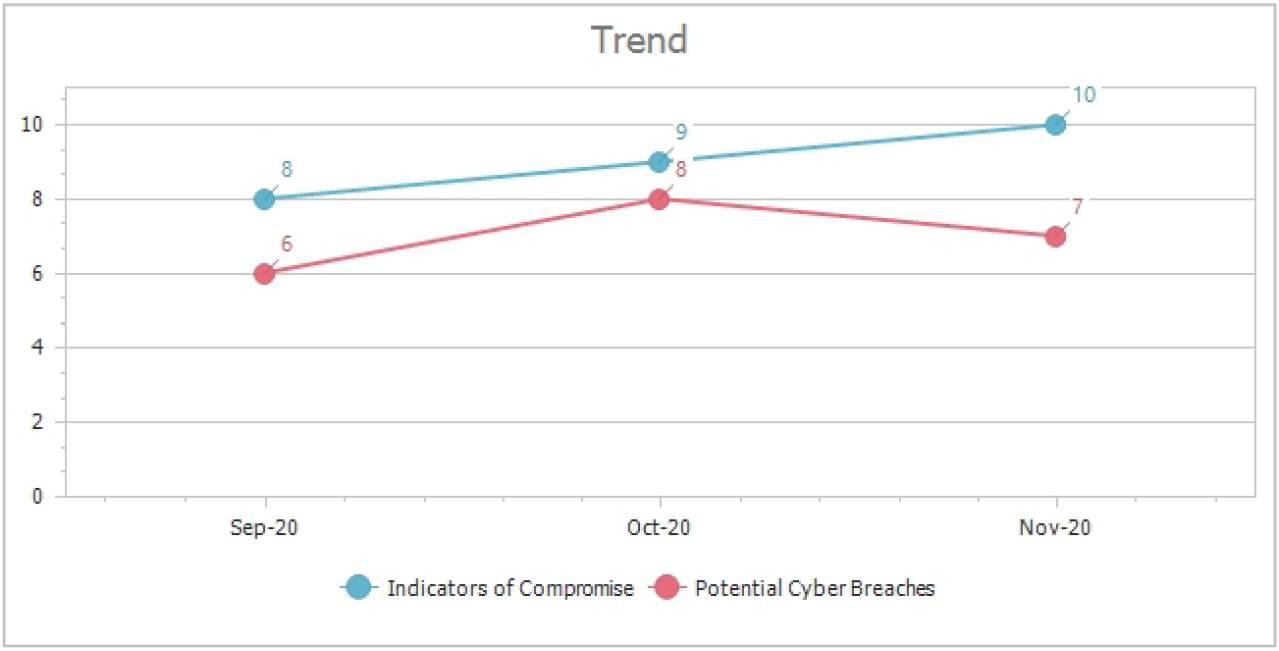
Appendix 1 Details of priority 1 and priority 2 alerts

Priority 1 Alerts Details

Details of priority 1 alerts observed and the last 2 months trend by category.



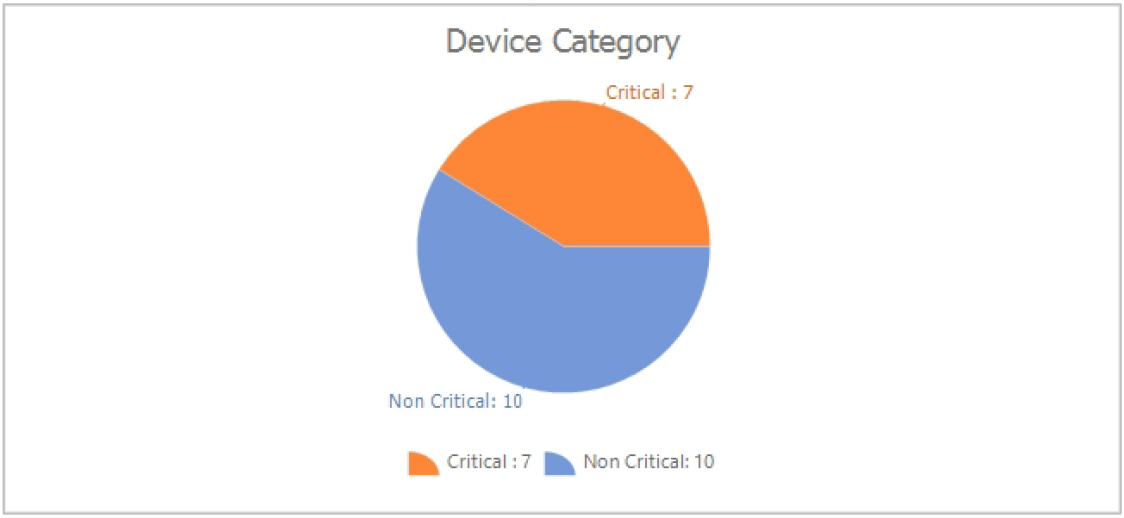
The trend shows the count of alerts based on the alert category in comparison to last 2 months.



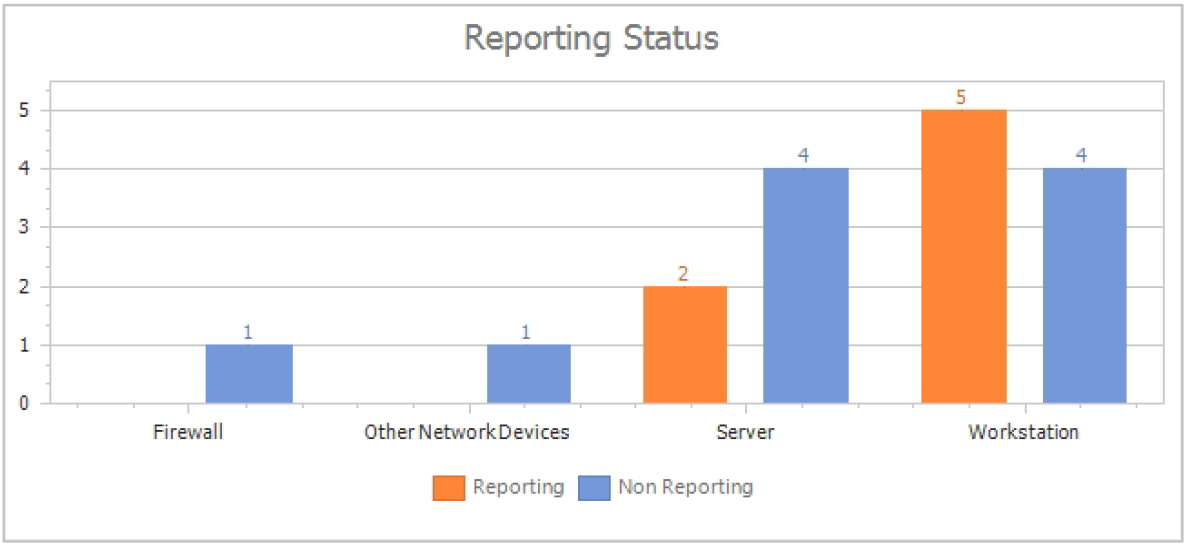
Category	Priority 1 Alert Name	Alert Count
Indicators of Compromise	EventTracker EDR: New product or signer is detected	1
Indicators of Compromise	EventTracker EDR: New suspicious signer is detected	1
Indicators of Compromise	EventTracker EDR: Unsafe dormant process detected	1
Indicators of Compromise	EventTracker EDR: Unsafe process found	1
Indicators of Compromise	EventTracker: Bad hash detected	1
Indicators of Compromise	EventTracker: New Windows network process activity	1
Indicators of Compromise	EventTracker: Suspicious exploit tool detected	3
Indicators of Compromise	Geographically improbable access detected	1
Potential Cyber Breaches	Anomalous login detected; critical threshold exceeded	1
Potential Cyber Breaches	EventTracker: A process connected to an unsafe IP address	1
Potential Cyber Breaches	EventTracker: A process has been terminated by EventTracker	2
Potential Cyber Breaches	EventTracker: Critical potential breach from an unsafe IP address	1
Potential Cyber Breaches	Stopping anomalous login activity by adding to block list	1
Potential Cyber Breaches	Successful login after anomalous login failure attempts	1
	Total	17

Security Monitoring Coverage

Total number of log sources being monitored by category and their log reporting status.



Critical category include firewalls and servers. Non-Critical category include workstations and other network devices.



Reporting status count calculation is based on the systems not reporting for last 10 days from report created date.

Appendix 1: Count of log sources monitored

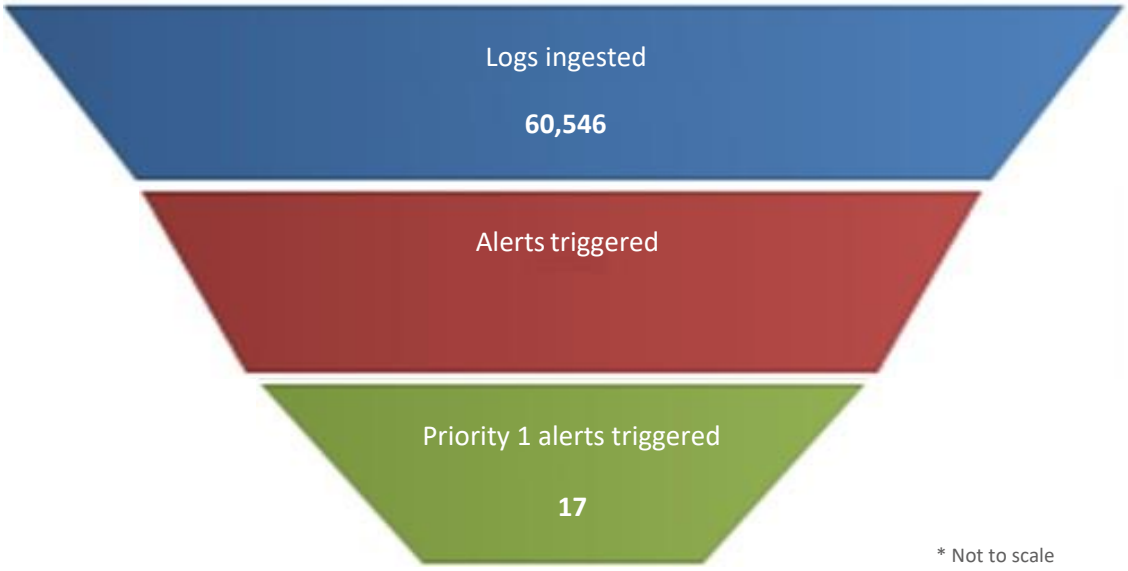
Appendix 2: Details of non-reporting systems

Metrics

Security monitoring:

The below graph depicts,

1. Total logs received from all the monitored log sources.
2. Total alerts triggered depicts the sum of all priority alerts.
3. Total number of priority 1 alerts triggered.



Log retention:

We have stored logs from May 2020 till date for your compliance and audit purposes.

Compliance summary:

Below table depicts the number of reports generated and reviewed with respect to below compliance standard(s) and are audit ready.

Standards	Controls Covered	No. of Reports
NIST 800-171	3.1, 3.1.1, 3.1.2, 3.1.5, 3.1.8, 3.3.2, 3.3.4, 3.5, 3.5.1, 3.5.2, 3.5.6, 3.13.1, 3.13.3, 3.13.6, 3.14.3	30
PCI-DSS	10.2.1, 10.2.2, 10.2.4, 10.2.5, 10.2.5.b, 10.2.5.c, 10.2.6, 10.2.7, 10.6.1	30

Appendix 4 Details of the controls and their description

References

Appendix 1 - Monitored priority 1 and priority 2 alerts

S. No.	Priority	Alert Category	Alert Name
1	Priority 1	Indicators of Compromise	EventTracker EDR: New product or signer is detected
2	Priority 1	Indicators of Compromise	EventTracker EDR: Unsafe dormant process detected
3	Priority 1	Indicators of Compromise	EventTracker EDR: Unsafe process found
4	Priority 1	Indicators of Compromise	EventTracker: New Windows network process activity
5	Priority 1	Indicators of Compromise	Geographically improbable access detected
6	Priority 1	Potential Cyber Breaches	Anomalous login detected; critical threshold exceeded
7	Priority 1	Potential Cyber Breaches	EventTracker: A process connected to an unsafe IP address
8	Priority 1	Potential Cyber Breaches	EventTracker: A process has been terminated by EventTracker
9	Priority 1	Potential Cyber Breaches	EventTracker: Critical potential breach from an unsafe IP address
10	Priority 1	Potential Cyber Breaches	Stopping anomalous login activity by adding to block list
11	Priority 1	Potential Cyber Breaches	Successful login after anomalous login failure attempts
12	Priority 2	Indicators of Compromise	EventTracker: Anomalous IP address activity
13	Priority 2	Indicators of Compromise	EventTracker: New Windows software install activity
14	Priority 2	Indicators of Compromise	EventTracker: Suspicious new process hash detected
15	Priority 2	Indicators of Compromise	Login activity from blacklisted location
16	Priority 2	Indicators of Compromise	New service installed
17	Priority 2	Indicators of Compromise	PowerShell running suspicious commands
18	Priority 2	Indicators of Compromise	Suspicious IP address connection by Microsoft Office application
19	Priority 2	Indicators of Compromise	Suspicious non browser application connecting to known webserver port
20	Priority 2	Indicators of Compromise	Suspicious process launch by Microsoft Office application
21	Priority 2	Indicators of Compromise	USB monitoring activity
22	Priority 2	Potential Cyber Breaches	Anomalous login detected; warning threshold exceeded

23	Priority 2	Potential Cyber Breaches	EventTracker: A new TCP port started listening
24	Priority 2	Potential Insider Threats	Active Directory: Group policy changed
25	Priority 2	Potential Insider Threats	EventTracker: Anomalous Windows interactive logon activity
26	Priority 2	Potential Insider Threats	EventTracker: New Windows audit policy and account management activity
27	Priority 2	Potential Insider Threats	EventTracker: New Windows user location affinity activity
28	Priority 2	Potential Insider Threats	Media insert alert
29	Priority 2	Potential Insider Threats	Security: User account disabled
30	Priority 2	Potential Insider Threats	Security: User added
31	Priority 2	Potential Insider Threats	Security: User added to domain admin or local admin group
32	Priority 2	Potential Insider Threats	Security: User deleted
33	Priority 2	Potential Insider Threats	Security: User password set to never expire
34	Priority 2	Potential Insider Threats	Windows: Audit log cleared
35	Priority 2	Undefined	Admin interactive/Remote interactive login success
36	Priority 2	Undefined	Email with pandemic or corona subject

Appendix 2 - Security monitoring coverage

Device Type	Current Month	Last Month
Firewall	1	1
Other Network Devices	1	1
Server	6	4
Workstation	9	4
Total Device Count	17	10

Appendix 3 - Details of non-reporting systems

S.No.	Device Type	Computer Name	IP Address	Last Event Received
1	Firewall	Sonic-syslog	172.28.127.6	10/29/2020 2:06:33 PM
2	Server	ETTVMBLR22019-2.Contoso.LOCAL	172.28.9.140	10/29/2020 5:53:21 AM
3	Server	ntpldtblr301	172.27.100.50	10/28/2020 7:47:27 PM
4	Server	R1S3VM2	172.28.9.155	10/29/2020 3:06:27 PM
5	Server	R1S3VM10~Contoso.DC	172.28.9.140	10/29/2020 12:06:06 PM
6	Workstation	R1S5-VM5~Contoso	172.28.9.146	10/29/2020 3:08:23 PM
7	Workstation	R1S4-VM1~Contoso	172.28.9.154	10/29/2020 3:07:23 PM
8	Other Network Devices	Barracuda-syslog	172.28.127.6	10/29/2020 2:07:07 PM
9	Workstation	R1S3VM1~Contoso.DC	172.28.9.134	10/29/2020 1:45:04 PM
10	Workstation	R1S3VM11~Contoso.DC	172.28.9.140	10/29/2020 12:21:07 PM

Appendix 4 - Details of compliance controls and their description

Compliance standard: PCI-DSS

Control	Description
10.2.1	Verify all individual access to cardholder data is logged.
10.2.2	All actions taken by any individual with root or administrative privileges.
10.2.4	Verify invalid logical access attempts are logged.
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
10.2.5.b	Use of elevation of privileges.
10.2.5.c	Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.
10.2.6	Verify the following are logged: Initialization of audit logs Stopping or pausing of audit logs.
10.2.7	Verify creation and deletion of system level objects are logged.
10.6.1	Review logs and security events of all servers and system components that perform security functions.

Compliance standard: NIST 800-171

Control	Description
3.1	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).
3.1.2	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.8	Limit unsuccessful logon attempts.
3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
3.13.3	Separate user functionality from information system management functionality.

3.13.6	Deny network communications traffic by default and allow network communications traffic by exception.
3.14.3	Monitor system security alerts and advisories and take action in response.
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
3.3.4	Alert in the event of an audit logging process failure.
3.5	Limit system access to the types of transactions and functions that authorized users are permitted to execute.
3.5.1	Identify information system users, processes acting on behalf of users, or devices
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
3.5.6	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.