CYBOT™

Automated Investigation & Hunting Platform

Datasheet

CYBOT™ Compliance

activebytes innovations

www.active-bytes.com

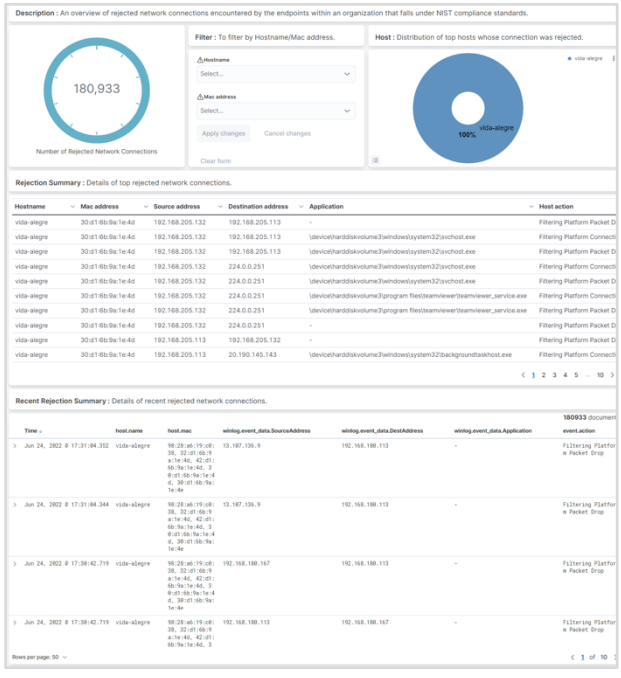
CYBOT™ Compliance

We have designed a compliance module in CYBOT solution, with an aim to aid organizations and security teams to meet regulatory standards such as ISO 27001, PCI DSS & NIST. The alerts and dashboards in the module are based on controls requirement. The enterprise data from data lake relevant to compliance controls is visually displayed in an accessible, user-friendly interface that provides actionable insights, and allows administrators to prioritize and respond to the most serious threats first. A compliant company culture establishes an organization's trustworthiness, integrity, and maturity in the industry landscape

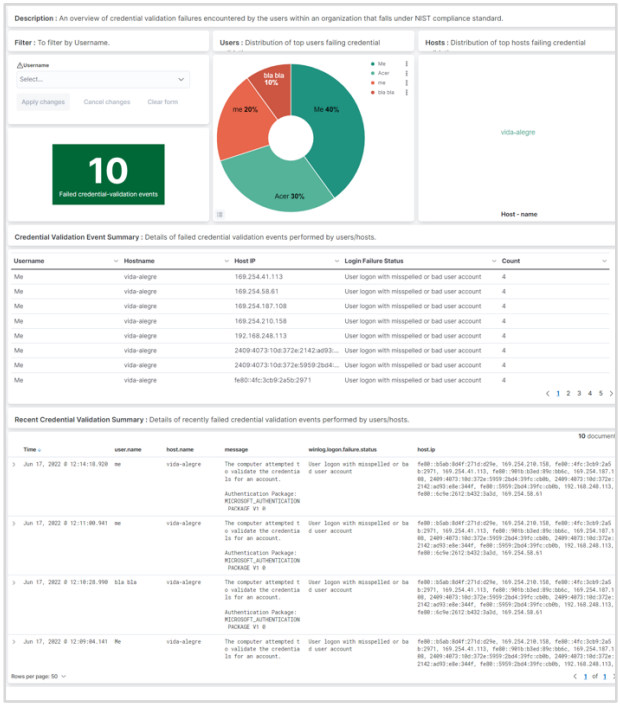
CYBOT compliance package consists of **compliance Dashboards** and **Active monitoring**

Dashboard for compliance

There are more than hundreds of dashboards designed based on compliance standards PCI DSS, NIST & ISO 27001

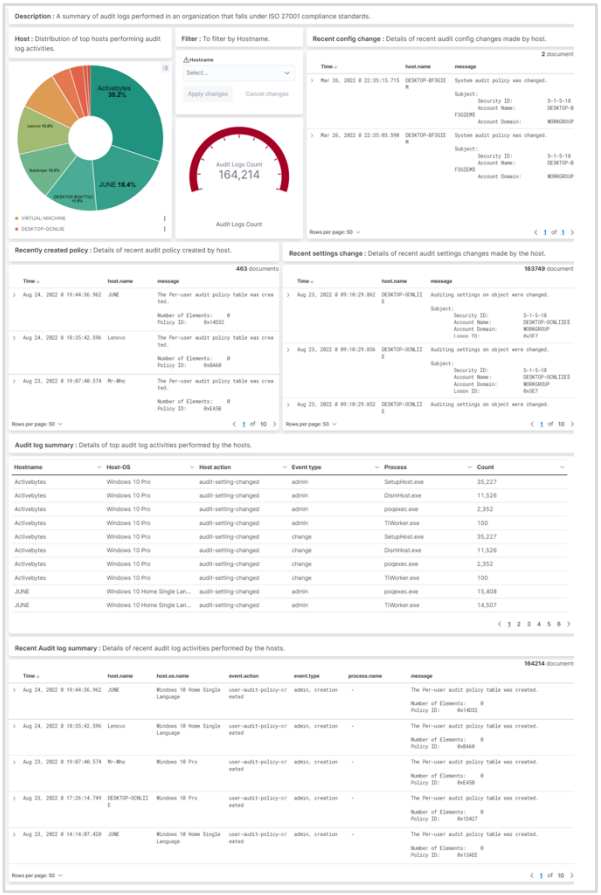


This dashboard shows an overview of rejected network connections encountered by the endpoints within an organization that falls under NIST compliance standards.

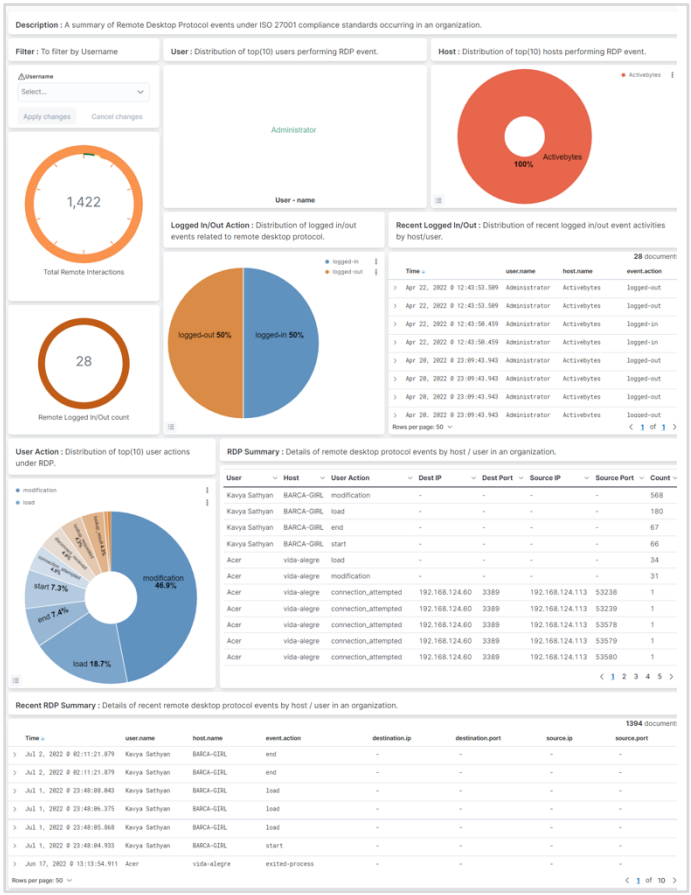


This dashboard gives an overview of credential validation failures encountered by the users within an organization that falls under NIST compliance standard.

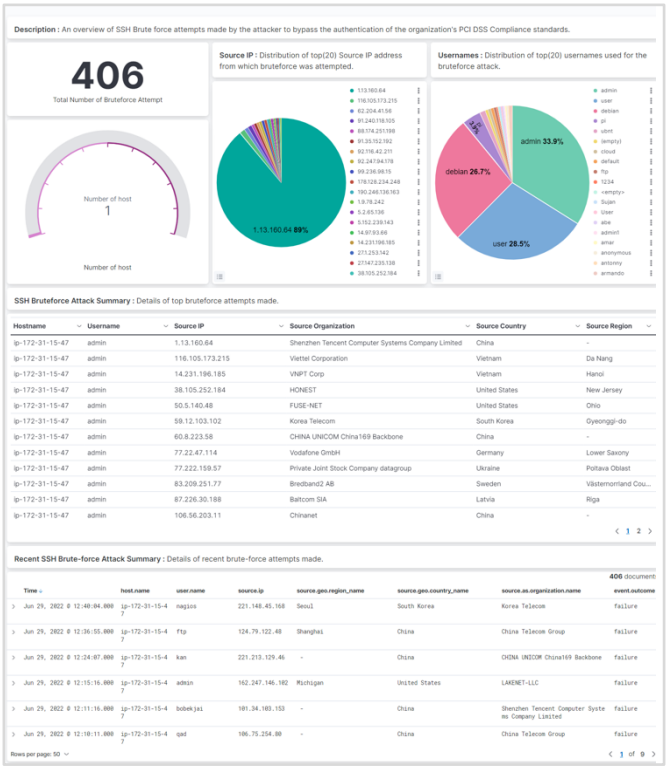
activebytes innovations



This dashboard gives a summary of audit logs performed in an organization that falls under ISO 27001 compliance standards.



This dashboard gives a summary of Remote Desktop Protocol events under ISO 27001 compliance standards occurring in an organization.



This dashboard shows an overview of SSH Brute force attempts made by the attacker to bypass the authentication of the organization's PCI DSS Compliance standards.

activebytes innovations

Dashboard Compliance (ISO 27001 Standard)

NO:	Dashboard Name	ISO 27001 Standard Control Number	Description
1	ISO-27001 -01- Account Management Summary	A.9.2.1	**User registration and de-registration:** A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
		A.9.2.2	**User access provisioning:** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services
2	ISO-27001 -02- Authentication Failure Summary	A.12.4.1	**Event logging:**Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.11.1.2	**Physical entry controls:** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
3	ISO 27001 -03- Configuration or Policy Change Summary	A.14.2.2	**System change control procedures:** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
4	ISO-27001 -04- Disabled & Locked account summary	A.9.2.6	**Removal or adjustment of access rights:**The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
5	ISO 27001 -05- Enabled & Unlocked Account Summary	A.9.2.6	**Removal or adjustment of access rights:**The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
6	ISO27001 -06- File Integrity Monitor Log Summary	A.12.4.1	**Event logging:**Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.12.4.2	**Protection of log information:** Logging facilities and log information shall be protected against tampering and unauthorized access
		A.10.1	**Cryptographic controls:**To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

7	ISO 27001 -07- Accounts Modification Summary	A.6.1.2	**Segregation of duties:** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
8	ISO 27001 -08- Traffic to Internet Summary	A.13.2.1	**Information transfer policies and procedures:** Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities
		A.13.2.3	**Electronic messaging:** Information involved in electronic messaging shall be appropriately protected.
		A.14.1.2	**Securing application services on public networks:** Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification
		A.14.1.3	**Protecting application services transactions:** Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
9	ISO 27001 -09- Traffic to Uncommon Ports Summary	A.14.1.3	**Protecting application services transactions:** Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
10	ISO 27001 -10- Windows Firewall Change Summary	A.13.2.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
11	ISO 27001 -11- Applications Accessed By User Summary	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy
		A.9.4.4	**Use of privileged utility programs:** The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
		A.11.2.7	**Secure disposal or reuse of equipment:** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use
12	ISO 27001 -12- Uncommon softwares usage summary	A.12.6.2	**Restrictions on software installation:**Rules governing the installation of software by users shall be established and implemented.
		A.12.5.1	**Installation of software on operational systems:** Procedures shall be implemented to control the installation of software on operational systems.
13	ISO 27001 -13- File Monitoring Event-File Changes	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

14	ISO 27001 -14- Use Of Non-Encrypted Protocols Summary	A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
15	ISO 27001 -15- Windows Host Configuration Change Summary	A.14.2.2	**System change control procedures:** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
16	ISO 27001 -16- User Priv Escalation (SU & SUDO)	A.9.2.3	**Management of privileged access rights:** The allocation and use of privileged access rights shall be restricted and controlled.
		A.9.2.2	**User access provisioning:** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services
17	ISO 27001 - 17 - Host Configuration Change Summary	A.14.2.2	**System change control procedures:** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
18	ISO 27001 - 18 - Data Transfer Summary	A.13.2.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
		A.13.2.2	**Security of network services:** Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced
		A.13.2.3	**Segregation in networks:** Groups of information services, users and information systems shall be segregated on networks
19	ISO 27001 - 19 - User Priv Escalation (Windows) Summary	A.9.2.3	**Management of privileged access rights:** The allocation and use of privileged access rights shall be restricted and controlled.
20	ISO 27001 - 20 - Software Installed Summary	A.12.5.1	**Installation of software on operational systems:** Procedures shall be implemented to control the installation of software on operational systems.
		A.12.6.2	**Restrictions on software installation:** Rules governing the installation of software by users shall be established and implemented
21	ISO 27001 - 21 - Software Uninstalled Summary	A.14.2.4	**Restrictions on changes to software packages:** Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
		A.12.5	**Logging and monitoring:** To record events and generate evidence.
22	ISO 27001 - 22 - Remote Desktop Protocol Summary	A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
23	ISO 27001 - 23 - Monitoring Linux Processes	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
24	ISO 27001 - 24 - Failed File System Access (Windows)	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.

25	ISO 27001 - 25 - Audit Log Summary	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
26	ISO 27001 - 26 - Detailed File Share Summary	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.
27	ISO 27001 - 27 - Suspected Wireless Connection Attempt Summary	A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
		A.13.1.2	**Security of network services:**Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
28	ISO 27001 - 28 - Critical Environment Error Summary	A.11.2.2	**Supporting utilities:** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities
		A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.14.2.6	**Secure development environment:** Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
29	ISO 27001 - 29 - Failure Credential-validated Summary	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.9.2.4	**Management of secret authentication information of users:**The allocation of secret authentication information shall be controlled through a formal management process.
30	ISO 27001 - 30 - Social Media Summary	A.5.1.1	**Policies for information security:** A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties
31	ISO 27001 - 31 - Failed File System Access (Linux)	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.
32	ISO 27001 - 32 - Rejected Connection to Network	A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
		A.9.1.2	**Access to networks and network services:** Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
33	ISO 27001 - 33 - Detected Virus/Spyware Summary	A.12.2.1	**Controls against malware:** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
34	ISO 27001 - 34 - System File Permission Change (Linux)	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.
35	ISO 27001 - 35 - Monitoring External Device Access	A.8.3.1	**Management of removable media:** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization

		A.6.2.1	**Mobile device policy:** A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices
36	ISO 27001 - 36 - Detecting SSH Brute Force Attack Summary	A.11.1.4	**Protecting against external and environmental threats:** Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
		A.9.4.3	**Password management system:** Password management systems shall be interactive and shall ensure quality passwords.
37	ISO 27001 - 37 - Physical Security Summary	A.11.1.2	**Physical entry controls:** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access
38	ISO 27001 - 38 - Unknown User Account Detail	A.9.2.5	**Review of user access rights:** Asset owners shall review users' access rights at regular intervals.
39	ISO 27001 - 39 - Time Sync Error Summary(Windows)	A.12.4.4	**Clock synchronisation:** The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source
40	ISO 27001- 40 -System Log File Deletion Summary (Linux)	A.12.4.2	**Protection of log information:** Logging facilities and log information shall be protected against tampering and unauthorized access.
		A.18.1.3	**Protection of records:** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements
41	ISO 27001 - 41 - WebServer Access Logs Deleted Summary	A.12.4.2	**Protection of log information:** Logging facilities and log information shall be protected against tampering and unauthorized access.
		A.18.1.3	**Protection of records:** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements

Dashboard Compliance (PCI DSS Standard)

NO:	Dashboard Name	PCI DSS Standard Control Number	Description
1	Compliance- PCI DSS- Host Configuration Change Summary	1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and theCDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users ofthe computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.
		6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		2.2.6	System security parameters are configured to prevent misuse.

		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
2	Compliance- PCI DSS - Data Transfer Summary	1.2.4	An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment
		6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
3	Compliance- PCI DSS - User Priv Escalation (Windows) Summary	6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
4	Compliance- PCI DSS - Software Installed Summary	6.3.2.a	Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.

		6.3.2.b	Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
5	Compliance- PCI DSS - Software Uninstalled Summary	6.3.2.a	Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.
		6.3.2.b	Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.
		6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
6	Compliance- PCI DSS - Remote Desktop Protocol Summary	1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained
		1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need
		1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated
		1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.

		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
7	Compliance- PCI DSS - Monitoring Linux Processes	2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
		10.2.2	Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol)
8	Compliance- PCI DSS - Failed File System Access (Windows)	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.
9	Compliance- PCI DSS - Audit Log Summary	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

		10.2.2	Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol)
10	Compliance- PCI DSS - Detailed File Share Summary	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
11	Compliance- PCI DSS - Suspected Wireless Connection Attempt Summary	1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.
		1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.
		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
12	Compliance- PCI DSS - Critical Environment Error Summary	6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
13	Compliance- PCI DSS - Failure Credential-validated Summary	6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.

		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
14	Compliance- PCI DSS - Social Media Summary	1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties
		1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.
15	Compliance- PCI DSS - Failed File System Access (Linux)	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.
16	Compliance- PCI DSS - Rejected Connection to Network	1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.
		1.4.1	NSCs are implemented between trusted and untrusted networks.
		1.4.4	System components that store cardholder data are not directly accessible from untrusted networks
		1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied

		1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied
17	Compliance- PCI DSS - Detected Virus/Spyware Summary	5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware
		5.2.2	5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.
		5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection
		5.3.1	The anti-malware solution(s) is kept current via automatic updates
		6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		5.2.3.1.a	Examine the entity's targeted risk analysis for the frequency of periodic evaluations of system components identified as not at risk for malware to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1
		5.2.3.1.b	Examine documented results of periodic evaluations of system components identified as not at risk for malware and interview personnel to verify that evaluations are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement
		5.3.2.a	Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution(s) is configured to perform at least one of the elements specified in this requirement.
		5.3.2.b	Examine system components, including all operating system types identified as at risk for malware, to verify the solution(s) is enabled in accordance with at least one of the elements specified in this requirement
		5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1
		10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis
18	Compliance- PCI DSS - System File Permission Change (Linux)	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

		6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
19	Compliance- PCI DSS - Monitoring External Device Access	2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components
20	Compliance- PCI DSS - Detecting Brute Force Attack Summary	6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections
		6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs.

			• Configured to either block web-based attacks or generate an alert that is immediately investigated.
21	Compliance- PCI-DSS - Physical Security Summary	7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.
22	Compliance- PCI-DSS - Unknown User Account Detail	7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.
23	Compliance- PCI-DSS - Time Sync Error Summary	6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections
		6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.
24	Compliance- PCI-DSS - System Log File Deletion Summary (Linux)	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

25	Compliance- PCI-DSS - WebServer Access Logs Deleted Summary	6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections
		6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.

Dashboard Compliance (NIST Standard)

NO:	Dashboard Name	NIST Standard Control Number	Description
1	NIST -01- User Priv Escalation (SU & SUDO)	AC-6	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
		AC -2(7)	• Establish and administer privileged user accounts in accordance with [Selection: a rolebased access scheme; an attribute-based access scheme]; • Monitor privileged role or attribute assignments; • Monitor changes to roles or attributes; and • Revoke access when privileged role or attribute assignments are no longer appropriate.
		AC-2(4)	Automatically audit account creation, modification, enabling, disabling, and removal actions.
		AU-2(8)	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.
		AC-2(11)	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].
2	NIST -02- Applications Accessed By User Summary	AC-3(12)	Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions]; (b) Provide an enforcement mechanism to prevent unauthorized access; and

			(c) Approve access changes after initial installation of the application.
		CM-7	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].
3	NIST -03- Account Management Summary	AC-2	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.

		IA-4	a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual, group, role, service, or device; and d. Preventing reuse of identifiers for [Assignment: organization-defined time period].
4	NIST -04- Authentication Failure Summary	IA-5	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.
		AU-2	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organizationdefined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support atier-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
		AC-7	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

5	NIST -05- Configuration or Policy Change Summary	CM-3	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organizationdefined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].
		CM-1	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and c. Review and update the current configuration management: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
		CM-6(2)	Take the following actions in response to unauthorized changes to [Assignment: organizationdefined configuration setings]: [Assignment: organization-defined actions].
6	NIST -06- Disabled & Locked account summary	AC-2(3)	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
		AC-2(13)	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].
		AC-2 (2)	Automatically [Selection: remove; disable] temporary and emergency accounts a□er

			[Assignment: organization-defined time period for each type of account].
		AC-7(1)	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.
		AC-7(4)	(a) Allow the use of [Assignment: organization-defined authentication factors] that are different from the primary authentication factors a□er the number of organizationdefined consecutive invalid logon attempts have been exceeded; and (b) Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the alternative factors by a user during a [Assignment: organization-defined time period].
		AC-2(1)	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].
7	NIST -07- Enabled & Unlocked Account Summary	AC-2 (1)	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].
		AC-7	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.
8	NIST -08- File Integrity Monitor Log Summary	SC-16 (1)	Verify the integrity of transmitted security and privacy attributes.

		SI-4	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].
		SC-28(1)	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].
		AU -2	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organizationdefined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
		SC-13	a. Determine the [Assignment: organization-defined cryptographic uses]; and b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].
		RA-10	a. Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls; and b. Employ the threat hunting capability [Assignment: organization-defined frequency].

		SC-8	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
9	NIST -09- Accounts Modification Summary	AC-2(1)	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].
		AC-2(4)	Automatically audit account creation, modification, enabling, disabling, and removal actions.
		AC-9(3)	Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time period].
10	NIST -10- Traffic to Internet Summary	AC-4	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
		AC-17	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.
		SI-4(4)	(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [Assignment: organizationdefined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].
		CA-3	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements [Assignment: organization-defined frequency].
		SC-7(3)	Limit the number of external network connections to the system.
11	NIST -11- Traffic to uncommon ports Summary	SA-4(9)	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.
		CM-7(1)	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].
		SA-9(2)	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organizationdefined external system services].

12	NIST -12- Windows Firewall Change Summary	IR-4(2)	Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organizationdefined types of dynamic reconfiguration].
		SC-7(11)	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].
13	NIST -13- Uncommon Software's Usage Summary	CM-10	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
		CM-7(4)	(a) Identify [Assignment: organization-defined software programs not authorized to execute on the system]; (b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and (c) Review and update the list of unauthorized so□ware programs [Assignment: organization-defined frequency].
		CM-11	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organizationdefined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].
		CM-7(5)	(a) Identify [Assignment: organization-defined software programs authorized to execute on the system]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized so□ware programs [Assignment: organizationdefined frequency].
14	NIST -14- Use of Non-Encrypted Protocols	AC-4 (4)	Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].

		AC-16	a. Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission; b. Ensure that the attribute associations are made and retained with the information; c. Establish the following permitted security and privacy attributes from the attributes defined in AC-16a for [Assignment: organization-defined systems]: [Assignment: organization-defined security and privacy attributes]; d. Determine the following permitted attribute values or ranges for each of the established attributes: [Assignment: organization-defined attribute values or ranges for established attributes]; e. Audit changes to attributes; and f. Review [Assignment: organization-defined security and privacy attributes] for applicability [Assignment: organization-defined frequency].
		AC-10	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].
		AC-6	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
		AC-17	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.
15	NIST -15- File Monitoring Event-File Changes	SI-4(11)	(a) Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; and (b) Take the following actions upon detection: [Assignment: organization-defined leastdisrup tive actions to terminate suspicious events].
		CM-6	a. Establish and document configuration se□ngs for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration se□ngs; c. Identify, document, and approve any deviations from established configuration se□ngs for [Assignment: organization-defined system components] based on [Assignment: organizationdefined operational requirements]; and d. Monitor and control changes to the configuration se□ngs in accordance with organizational policies and procedures.

		AU-6	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
16	NIST -16- Windows Host Configuration Change Summary	CM-3	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organizationdefined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].
		AC-4	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
17	NIST - 17 - Host Configuration Change Summary	CM-3	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organizationdefined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].

		IA-3(3)	(a) Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; and (b) Audit lease information when assigned to a device.
		CA-7(3)	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.
18	NIST - 18 - Data Transfer Summary	AC-4	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
		CA-3	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements [Assignment: organization-defined frequency].
		AU-10	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation
		CM-12	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.
19	NIST - 19 - User Privilege Escalation (Windows) Summary	AC-6(7)	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.
		AC-6(10)	Prevent non-privileged users from executing privileged functions.
20	NIST - 20 - Software Installed Summary	CM-11	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organizationdefined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].
		SA-7	

		SI -7 (12)	Require that the integrity of the following user-installed so□ware be verified prior to execution: [Assignment: organization-defined user-installed software].
		CM-7(6)	Require that the following user-installed so□ware execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].
		CM-8	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and b. Review and update the system component inventory [Assignment: organization-defined frequency].
		CM-14	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
21	NIST - 21 - Software Uninstalled Summary	CM-8(1)	Update the inventory of system components as part of component installations, removals, and system updates.
		CM-8(3)	(a) Detect the presence of unauthorized hardware, so□ware, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].
		SA-22	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].
		SI-2 (6)	Remove previous versions of [Assignment: organization-defined software and firmware components] a□er updated versions have been installed.
		SI-7	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

22	NIST - 22 - Remote Desktop Protocol Summary	AC -17(1)	Employ automated mechanisms to monitor and control remote access methods.
		AC-17(2)	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
		AC-17(3)	Route remote accesses through authorized and managed network access control points.
		AC-17(4)	(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; and (b) Document the rationale for remote access in the security plan for the system.
		AC-17(5)	
		AC-17(6)	Protect information about remote access mechanisms from unauthorized use and disclosure.
		AC-17(7)	
		AC-17(8)	
		AC-17(9)	Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].
		AC-17(10)	Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].
23	NIST - 23 - Monitoring Linux Processes	AU-3	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.
		AU-2	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organizationdefined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
24	NIST - 24 - Failed File System Access Summary	AC-2(4)	Automatically audit account creation, modification, enabling, disabling, and removal actions.

		AC-3(3)	Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy: (a) Is uniformly enforced across the covered subjects and objects within the system; (b) Specifies that a subject that has been granted access to information is constrained from doing any of the following; (1) Passing the information to unauthorized subjects or objects; (2) Granting its privileges to other subjects; (3) Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components; (4) Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and (5) Changing the rules governing access control; and (c) Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints.
		AC-3(13)	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].
25	NIST - 25 - Audit Log Summary	AU-2	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organizationdefined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
		AU-9	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.
		AU-9(6)	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].

26	NIST - 26 - Detailed File Share Summary	CA-3	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements [Assignment: organization-defined frequency].
		AU-13(3)	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.
		CA-3(6)	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.
		CA-3(7)	(a) Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-3a; and (b) Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.
27	NIST - 27 - Suspected Wireless Connection Attempt Summary	AC-18	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
		AC-18(2)	MONITORING UNAUTHORIZED CONNECTIONS
		SI-4(15)	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.
28	NIST - 28 - Critical Environment Error Summary	SI-11	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and b. Reveal error messages only to [Assignment: organization-defined personnel or roles].
		AU-5	a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organizationdefined time period] in the event of an audit logging process failure; and b. Take the following additional actions: [Assignment: organization-defined additional actions].
29	NIST- 29 -Failure Credential-validated Summary	AC-7	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

		AU-2	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organizationdefined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
		AU-6	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
30	NIST- 30 -Social Media Summary	PL-4(1)	Include in the rules of behavior, restrictions on: (a) Use of social media, social networking sites, and external sites/applications; (b) Posting organizational information on public websites; and (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.
		PM-20	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are publicly available; and c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.
		AU-13	a. Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; and b. If an information disclosure is discovered: 1. Notify [Assignment: organization-defined personnel or roles]; and 2. Take the following additional actions: [Assignment: organization-defined additional actions].

		AC-22	a. Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.
31	NIST- 31 - Failed File System Access (Linux)	AC-2(4)	Automatically audit account creation, modification, enabling, disabling, and removal actions.
		AC-3(3)	Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy: (a) Is uniformly enforced across the covered subjects and objects within the system; (b) Specifies that a subject that has been granted access to information is constrained from doing any of the following; (1) Passing the information to unauthorized subjects or objects; (2) Granting its privileges to other subjects; (3) Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components; (4) Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and (5) Changing the rules governing access control; and (c) Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints.
		AC-3(13)	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].
32	NIST- 32 -Rejected Connection to Network	SC-7(5)	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organizationdefined systems]]
		AC-12	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].
		SC-10	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity

33	NIST- 33 -Detected Virus/Spyware Summary	SI-3	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.
		CM-7(6)	Require that the following user-installed so□ware execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].
		AT-2(4)	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].
34	NIST- 34 -System File Permission Change (Linux)	CM-6	a. Establish and document configuration se□ngs for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration se□ngs; c. Identify, document, and approve any deviations from established configuration se□ngs for [Assignment: organization-defined system components] based on [Assignment: organizationdefined operational requirements]; and d. Monitor and control changes to the configuration se□ngs in accordance with organizational policies and procedures.
35	NIST- 35 -Monitoring External Device Access	AC-20	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organizationally-defined types of external systems].

		SC-41	a. Prohibit [Selection (one or more): the use of devices possessing [Assignment: organizationdefined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems]; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]]; and b. Provide an explicit indication of sensor use to [Assignment: organization-defined group of users].
		CM-8(3)	(a) Detect the presence of unauthorized hardware, so□ware, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].
		SC-43	a. Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]; and b. Authorize, monitor, and control the use of such components within the system.
		SI-4(5)	Alert [Assignment: organization-defined personnel or roles] when the following systemgenerated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].
36	NIST- 36 -Detecting SSH Brute Force Attack Summary	AC-7	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.
		SC-23 (3)	Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.
37	NIST- 37 -Physical Security Summary	PE-6	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinate results of reviews and investigations with the organizational incident response capability.

		PE-2	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Remove individuals from the facility access list when access is no longer required.
		PE-8	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period]; b. Review visitor access records [Assignment: organization-defined frequency]; and c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].
		PE-3	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards]; b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]; c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls]; d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity]; e. Secure keys, combinations, and other physical access devices; f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
		PE-4	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].
		PE-5	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.
		PE-7	Visitor Control
38	NIST- 38 -Unknown User Account Detail	AC-2(1)	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].
		AC-2(3)	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
		AC-2 (11)	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts]

		AU-6(5)	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
		AC-2(12)	(a) Monitor system accounts for [Assignment: organization-defined atypical usage]; and (b) Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].
		AC-2(13)	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].
39	NIST- 39 -Time Sync Error Summary(Windows)	SC-45	Synchronize system clocks within and between systems and system components
		AU-8	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.
		AU-12(1)	Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].
		AU-14	a. Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; and b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
40	NIST- 40 -System Log File Deletion Summary (Linux)	AU-9	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.
		AU-9(4)	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].
		AU-9(6)	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].
		IR-2	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter; and b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
		SI-12 (3)	Use the following techniques to dispose of, destroy, or erase information following the

			retention period: [Assignment: organization-defined techniques].
41	NIST- 41 -WebServer Access Logs Deleted Summary	AU-9	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.
		AU-9(4)	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].
		AU-9(6)	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].

Active Monitoring

Active monitoring are alerts designed to trigger in an organisation based on the compliance regulatory standards like NIST, PCI DSS & ISO 27001

- ✓ When active monitoring is triggered the security team will see (Fig 1), showing the details of an alert triggered, along with its compliance mapping control number.

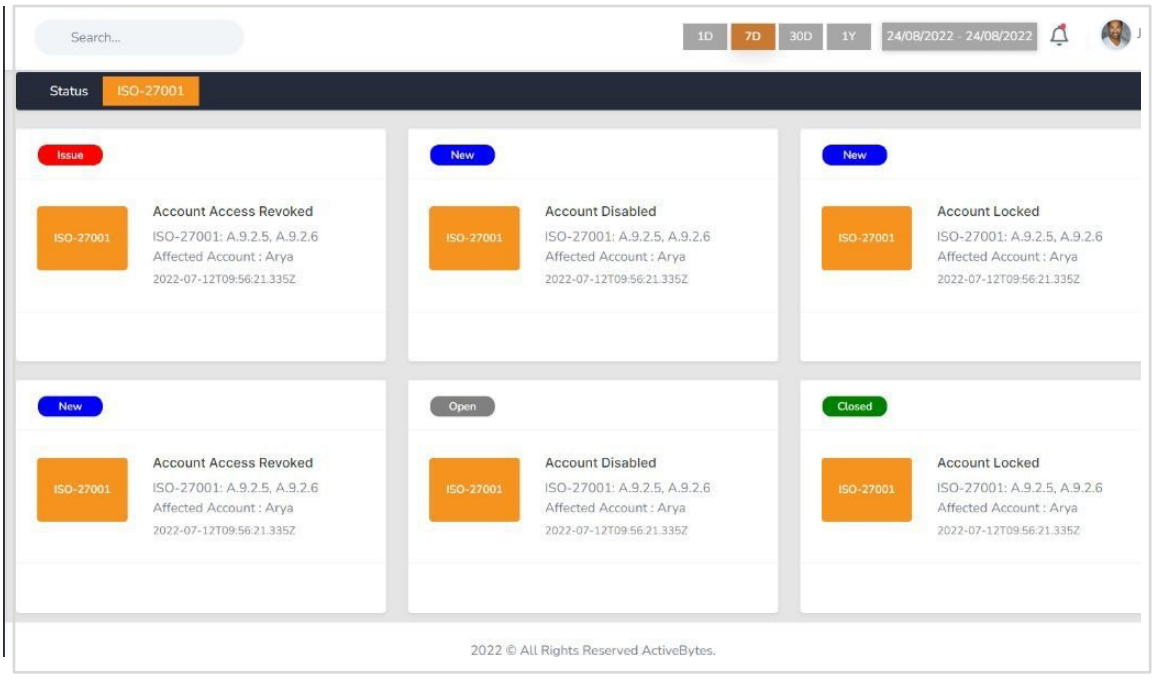


Fig 1

activebytes innovations

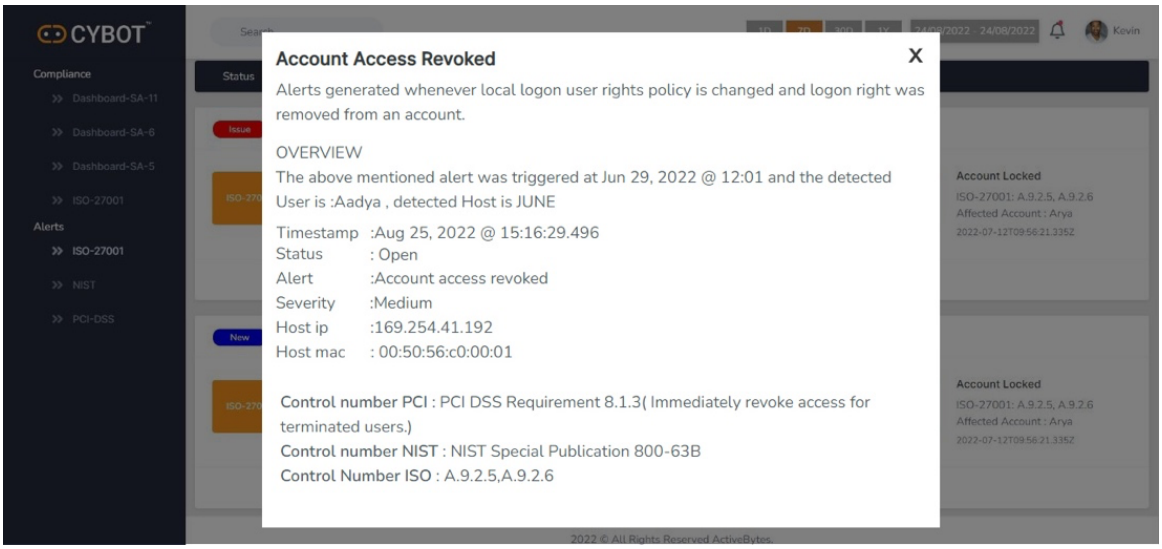


Fig 2

- ✓ The pop-up window (fig 2) shows the content of an Active compliance module, along with a description of the triggered event, details regarding that event, and Control numbers that map it to the compliance standards
- ✓ Also, a wholistic view of the compliance is available as in (fig 3)

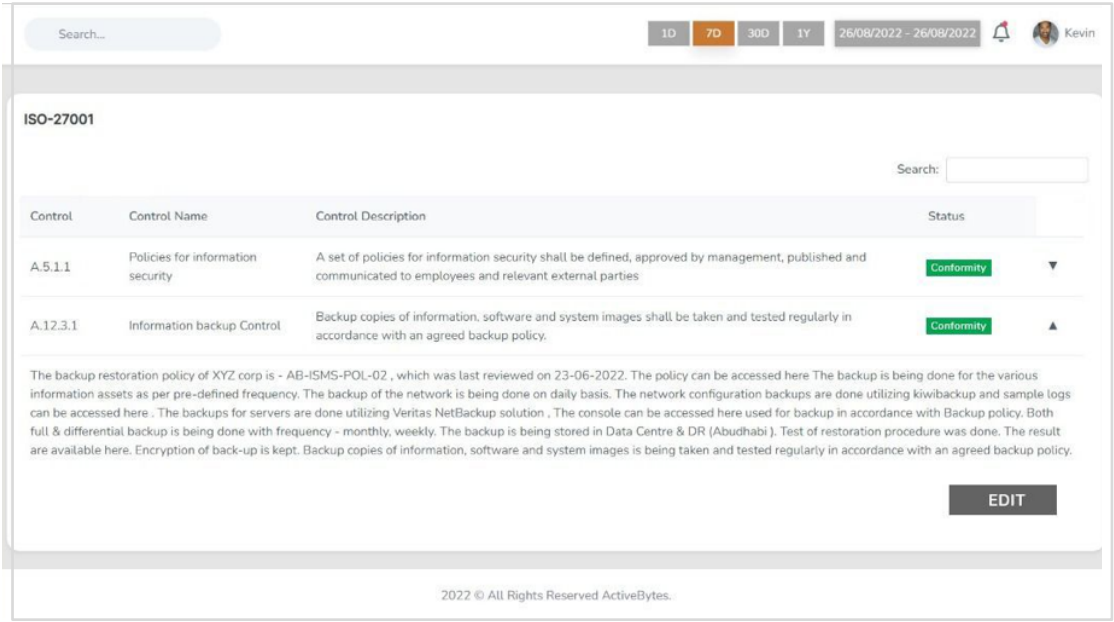


Fig 3

The compliance list for active monitoring is shown below:

Compliance - Alert					
			Controls		
#	Alert name	Alert Description	PCI - DSS	NIST	ISO - 27001
1	Logon from External Devices	A new external device was recognized by the system. This alert is generated when a new external device, such as a USB, is connected to the system.	2.2.4 Only necessary services, protocols, daemons,and functions are enabled, and all unnecessary functionality is removed or disabled. 3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. 5.3.3 For removable electronic media, the antimalware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted,OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	AC-19 -a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems AC-20 - 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organizationally-defined types of external systems]	A.8.3.1 Management of Removable Media Procedures must be put in place for the management of removable media in accordance with the classification scheme. General use of removable media must be risk assessed and it may be necessary to carry out use-specific risk assessments beyond that too. Removable media should only be allowed if there is a justified business reason.

2	Windows Firewall Service failed	This alert will triggered when the Windows Firewall Service failed to start.	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	SR-9 TAMPER RESISTANCE AND DETECTION Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.	A.14.2.4 Restrictions on Changes to Software Packages Modifications to software packages need to be discouraged, limited to necessary changes and all changes should be strictly controlled. Vendor supplied software packages are designed for the mass-market and are not really designed for organisations making their own changes to them. In fact most of the time the ability to make such changes is locked out by the vendor and customisation limited to within the package. Where open-source software is used, it is far more likely that changes can be made by the organisation, however, this should be restricted and controlled to ensure that the changes made do not have an adverse impact on the internal integrity or security of the software.
3	Windows Firewall Driver failed	This alert will triggered Windows Firewall Driver failed to start.	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	SR-9 TAMPER RESISTANCE AND DETECTION Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.	A.14.2.4 Restrictions on Changes to Software Packages Modifications to software packages need to be discouraged, limited to necessary changes and all changes should be strictly controlled. Vendor supplied software packages are designed for the mass-market and are not really designed for organisations making their own changes to them. In fact most of the time the ability to make such changes is locked out by the vendor and customisation limited to within the package. Where open-source software is used, it is far more likely that changes can be made by the organisation, however, this should be restricted and controlled to ensure that the changes made do not have an adverse impact on the internal integrity or security of the software.

4	Windows Firewall Termination	The Windows Firewall Driver detected a critical runtime error (Terminating).	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	SR-9 TAMPER RESISTANCE AND DETECTION Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.	A.14.2.4 Restrictions on Changes to Software Packages Modifications to software packages need to be discouraged, limited to necessary changes and all changes should be strictly controlled. Vendor supplied software packages are designed for the mass-market and are not really designed for organisations making their own changes to them. In fact most of the time the ability to make such changes is locked out by the vendor and customisation limited to within the package. Where open-source software is used, it is far more likely that changes can be made by the organisation, however, this should be restricted and controlled to ensure that the changes made do not have an adverse impact on the internal integrity or security of the software.
5	Detected Replay Attack	This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration.	8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks.	IA-4 IDENTIFIER MANAGEMENT Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.	A.9.4.2 Secure log-on Procedures Access to systems and applications must be controlled by a secure log-on procedure to prove the identity of the user. This can go beyond the typical password approach into multi-factor authentication, biometrics, smart cards, and other means of encryption based on the risk being considered. Secure log on should be designed so it cannot be easily circumvented and that any authentication information is transmitted and stored encrypted to prevent interception and misuse.

6	SMB Activity to the Internet	This rule detects network events that may indicate the use of SMB(Also known as Windows file sharing traffic to the Internet). SMB is commonly used within networks to share files, printers, and other system resources amongst trusted systems.	2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	SC-4 INFORMATION IN SHARED SYSTEM RESOURCES Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system.	A.13.1.2 Security of Network Services Security mechanisms, service levels and management requirements of all network services need to be identified and included in network services agreements, whether these services are provided in-house or outsourced
7	User Remote Access Denied	A user was denied access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group.	7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	AC-17 - Remote Access a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.	A.9.1.2 Access to Networks and Network Services The principle of least access is the general approach favoured for protection, rather than unlimited access and superuser rights without careful consideration. As such users should only get access to the network and network services they need to use or know about for their job. The policy therefore needs to address; The networks and network services in scope for access; Authorisation procedures for showing who (role based) is allowed to access to what and when; and Management controls and procedures to prevent access and monitor it in life. This also needs to be considered during onboarding and offboarding, and is closely related to the access control policy itself.

8	Remote User Disconnected	If a user disconnects from an existing Terminal Services session, or switches away from an existing desktop using Fast User Switching, event 4779 is generated. This event is also triggered when a user disconnects from a virtual host.	7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	AC-17 - Remote Access a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.	A.9.1.2 Access to Networks and Network Services The principle of least access is the general approach favoured for protection, rather than unlimited access and superuser rights without careful consideration. As such users should only get access to the network and network services they need to use or know about for their job. The policy therefore needs to address; The networks and network services in scope for access; Authorisation procedures for showing who (role based) is allowed to access to what and when; and Management controls and procedures to prevent access and monitor it in life. This also needs to be considered during onboarding and offboarding, and is closely related to the access control policy itself.

9	Active Directory Password Change	Alert makes Active Directory auditing very easy by tracking Password Status Changes for Users like password set or changed details with the help of pre-defined reports and instant alerts.	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:	AC-2 ACCOUNT MANAGEMENT f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and	A.9.4.3 Password Management System The purpose of a password management system is to ensure quality passwords meet the required level and are consistently applied. Password generation and management systems provide a good way of centralising the provisioning of access and they serve to reduce the risk of people using the same login for everything As with any control mechanism, password generation and management systems need to be carefully implemented to ensure adequate and proportionate levels of protection.
10	Detecting Installed Applications	Alert will notify you when an installation is successfully completed. It also shows the user account that performed the installation process.	6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Direct- CM-11, a. Establish organization-defined policies governing the installation of software by users; b. Enforce software installation policies c. Monitor policy compliance	A.12.5.1 Installation of Software on Operational Systems Procedures must be implemented to control the installation of software on operational systems. As with any security related control it is important that the installation of software on operational systems is formally controlled.

11	Detecting Uninstalled Applications	Alert will notify you when an uninstallation is successfully completed. It also shows the user account that performed the uninstallation process.	6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Direct- CM-11, a. Establish organization-defined policies governing the installation of software by users; b. Enforce software installation policies c. Monitor policy compliance	A.12.5.1 Installation of Software on Operational Systems Procedures must be implemented to control the installation of software on operational systems. As with any security related control it is important that the installation of software on operational systems is formally controlled.
12	Critical Environment Error	This alert will trigger if any critical environmental error happened in an organization.	Requirement 10: Log and Monitor All Access to System Components and Cardholder Data 10.7.1 - Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	SI-4 SYSTEM MONITORING a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the organziation's monitoring objectives: and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and	A.11.2.6 Security of Equipment & Assets Off-Premises Security controls need to be applied to off-site assets, taking into account the different risks involved with working outside the organisation's premises. This is a common area of vulnerability and it is therefore important that the appropriate level of controls is implemented and tie into other mobile controls and policies for homeworkers etc.

13	Encrypted Policy Change	This computer's Security Settings\Public Key Policies\Encrypting File System data recovery agent policy was modified - either via Local Security Policy or Group Policy in Active Directory.	3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on	A.10.1.1 Policy on the use of Cryptographic Controls A policy on the use of encryption can be a good place to identify the business requirements for when encryption must be used and the standards that are to be implemented.
14	System Audit Policy Change	This computer's system level audit policy was modified - either via Local Security Policy, Group Policy in Active Directory or the audipol command. According to Microsoft, this event is always logged when an audit policy is disabled, regardless of the "Audit Policy Change" sub-category setting. This and several other events can help identify when someone attempts to disable auditing to cover their tracks.	10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure;	A.12.7.1 Information Systems Audit Controls Audit requirements and activities involving verification of operational systems need to be carefully planned and agreed on to minimise disruptions to the business processes.
15	Audit Log was Cleared	The alert will trigger if the audit log was cleared.	10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure;	A.12.7.1 Information Systems Audit Controls Audit requirements and activities involving verification of operational systems need to be carefully planned and agreed on to minimise disruptions to the business processes.

16	Active Directory Password Reset	The alert attempt was made to reset an accounts password.	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:	AC-2 ACCOUNT MANAGEMENT f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and	A.9.4.3 Password Management System The purpose of a password management system is to ensure quality passwords meet the required level and are consistently applied. Password generation and management systems provide a good way of centralising the provisioning of access and they serve to reduce the risk of people using the same login for everything As with any control mechanism, password generation and management systems need to be carefully implemented to ensure adequate and proportionate levels of protection.
17	Modified User Accounts	The user identified by Subject: changed the user identified by Target Account. Attributes show some of the properties that were set at the time the account was changed. This event is logged both for local SAM accounts and domain accounts.	7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	AC-2 ACCOUNT MANAGEMENT Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by for requests to create accounts; f. Create, enable, modify,	A.9.4.2 Secure log-on Procedures Access to systems and applications must be controlled by a secure log-on procedure to prove the identity of the user.

				disable, and remove accounts in accordance with g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. when accounts are no longer required; 2. when users are terminated or transferred; and 3. when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and j. Review accounts for compliance with account management requirements k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.	
18	Device Disabled by the User	This event is generated when a user successfully disables a device.	10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects 10.6 Review logs and security events for all system components to identify anomalies or suspicious	CM-6 CONFIGURATION SETTINGS a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	A.14.2.2 System Change Control Procedures Changes to systems within the development lifecycle must be controlled by the use of formal change control procedures. System change control procedures should integrate with, be aligned to and support operational change control. Formal change management procedures are designed to reduce the risk of accidental or deliberate development of vulnerabilities that may allow systems to be compromised once the changes are put live. For system change control, it is important that the system owner understands what changes are being made to their system, why and by whom. It is their responsibility to ensure that their systems are not compromised through poor or malicious development.

			activity. Perform critical log reviews at least daily.		
19	SID History Added	This event generates when SID History was added to an account.	10.2.1 - Audit logs are enabled and active for all system components and cardholder data.	AU-2 - EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a “defence-in-depth” strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.

20	SID History Added Failed	This event generates when an attempt to add SID History to an account failed.	10.2.1 - Audit logs are enabled and active for all system components and cardholder data.	AU-2 - EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a "defence-in-depth" strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.
21	Kerberos Policy Changes	This alert detects a change to the the domain's Kerberos policy. Kerberos policy is defined in GPOs linked to the root of the domain under Computer Configuration\Windows Settings\Security Settings\Account Policy\Kerberos Policy.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment:	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a "defence-in-depth" strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.

				organization-defined frequency].	
22	Detected Incomming Messages	RPC detected an integrity violation while decrypting an incoming message.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a “defence-in-depth” strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.

23	Request Enabled Device	A request was made to enable a device. This alert is generated if a user attempts to enable a device on the system. This does not mean that a device was successfully enabled.	10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.	CM-6 CONFIGURATION SETTINGS a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	A.14.2.2 System Change Control Procedures Changes to systems within the development lifecycle must be controlled by the use of formal change control procedures. System change control procedures should integrate with, be aligned to and support operational change control. Formal change management procedures are designed to reduce the risk of accidental or deliberate development of vulnerabilities that may allow systems to be compromised once the changes are put live. For system change control, it is important that the system owner understands what changes are being made to their system, why and by whom. It is their responsibility to ensure that their systems are not compromised through poor or malicious development.

24	Sysmon Error	This alert is generated when an error occurred within Sysmon. They can happen if the system is under heavy load and certain tasked could not be performed or a bug exists in the Sysmon service.	10.2.1.7 Audit logs capture all creation and deletion of system-level objects.	SI-4 SYSTEM MONITORING a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a "defence-in-depth" strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.
25	Domain Policy Change	This alert is generated when an Active Directory Domain Policy is modified. It is logged on domain controllers and member computers.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a "defence-in-depth" strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.

				event types selected for logging [Assignment: organization-defined frequency].	
26	Restore Administrator Password	An attempt was made to set the Directory Services Restore Mode administrator password. This alert is generated when DSRM administrator password is changed. It is logged only on domain controllers	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	IA-5 AUTHENTICATOR MANAGEMENT Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.	A. 9.4. 3 Password Management System Impose the use of individual user IDs and passwords in order to ensure accountability; Enable users to select and update their own passwords and provide a validation process to enable input errors; Enforce the selection of quality passwords;

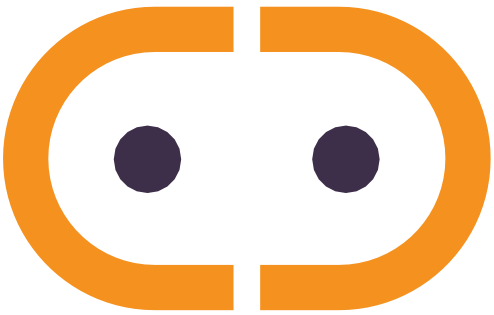
27	Active Directory Privilege Operation	An operation was attempted on a privileged object.	A3.4.1 User accounts and access privileges to inscope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a “defence-in-depth” strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.
28	Active Directory Services Access	A handle to an object was requested.	7.2 Access to system components and data is appropriately defined and assigned.	CM-5 ACCESS RESTRICTIONS FOR CHANGE Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	A.14.2.2 System Change Control Procedures Changes to systems within the development lifecycle must be controlled by the use of formal change control procedures. System change control procedures should integrate with, be aligned to and support operational change control. Formal change management procedures are designed to reduce the risk of accidental or deliberate development of vulnerabilities that may allow systems to be compromised once the changes are put live. For system change control, it is important that the system owner understands what changes are being made to their system, why and by whom. It is their responsibility to ensure that their systems are not compromised through poor or malicious development.

29	Alert-Data Loss Prevention Rule	This Alert is generated when there is event associated with data loss	A3.2.6.1 Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss.	SC-7 BOUNDARY PROTECTION a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	A12.1 Operational procedures and responsibilities
30	Error Logging Service	The event logging service encountered an error. This alert is generated when the event logging service encounters an error while processing an incoming event.	10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure; and	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a “defence-in-depth” strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.
31	User Privilege Assigned	This Alert is generated when a user privilege is assigned	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.	A9.2.1 User registration and de-registration A9.2.2 User access provisioning A9.2.3 Management of privileged access rights A9.2.6 Removal or adjustment of access rights

32	User Privilege Removed	This Alert is generated when a user privilege is removed	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.	A9.2.1 User registration and de-registration A9.2.2 User access provisioning A9.2.3 Management of privileged access rights A9.2.6 Removal or adjustment of access rights
33	User Account Unlocked	This Alert is generated when a user account is unlocked	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.	A9.2.1 User registration and de-registration A9.2.2 User access provisioning A9.2.3 Management of privileged access rights A9.2.6 Removal or adjustment of access rights
34	Attempt to Disable Syslog Service	This Alert is generated when there is attempt to disable sys;og service	10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs	IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION Uniquely identify and authenticate] before establishing communications with devices, users, or other services or applications.	A13.1.2 Security of network services A9.1.2 Access to networks and network services
35	Attempt to Enable the Root Account	This Alert is generated when there is attempt to enable the root account	8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an	AC-2 ACCOUNT MANAGEMENT a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) Require approvals by for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with g. Monitor the use of accounts; h. Notify account managers when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage;	A9.2.1 User registration and de-registration A9.2.2 User access provisioning A9.2.3 Management of privileged access rights

			individual user.	and j. Review accounts for compliance with account management requirements; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.	
36	Blocked File Import/Export Attempt	This Alert is generated when there is attempt to import or export a blocked file	1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks.	SC-7 BOUNDARY PROTECTION . Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	A14.1.2 Securing application services on public networks A14.1.3 Protecting application services transactions
37	Failed File System Access (Linux)	This alert is generated when permission to access the file system is denied.	10.2.1 Audit logs are enabled and active for all system components and cardholder data.	AC-3 ACCESS ENFORCEMENT Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	A9.1.1 Access control policy A9.1.2 Access to networks and network services

38	System File Permission Change (Linux)	This alert is generated when the system file permissions (Read, Write, Execute) are changed.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a "defence-in-depth" strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.
39	System File Permission Change (Windows)	Permissions on an object were changed. This alert is generated when someone changes the access control list on an object. The event identifies the object, who changed the permissions and the old an new permissions.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	AU-2 EVENT LOGGING a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging	A.12.4.1 Event Logging Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly. Logging and monitoring mechanisms form an important part of a "defence-in-depth" strategy for security management by providing both detective and investigation capabilities. Event logs of all types, e.g. system logs, access control logs, etc., may be required, especially regarding incident management and auditing.



activebytes innovations

www.active-bytes.com / contact@active-bytes.com
+971 50 513 3973