CYBOT™

Automated Investigation & Hunting Platform

Datasheet

CYBOT™ Compliance (NIST)

activebytes innovations

www.active-bytes.com

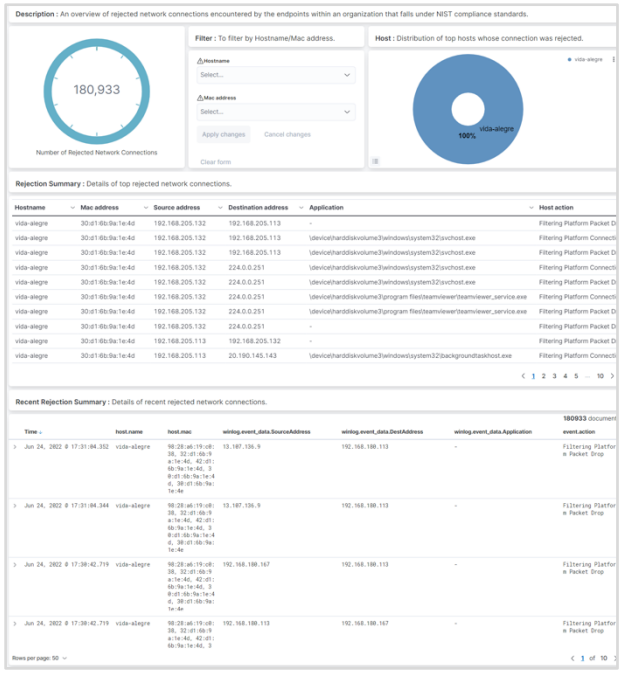
CYBOT™ Compliance

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

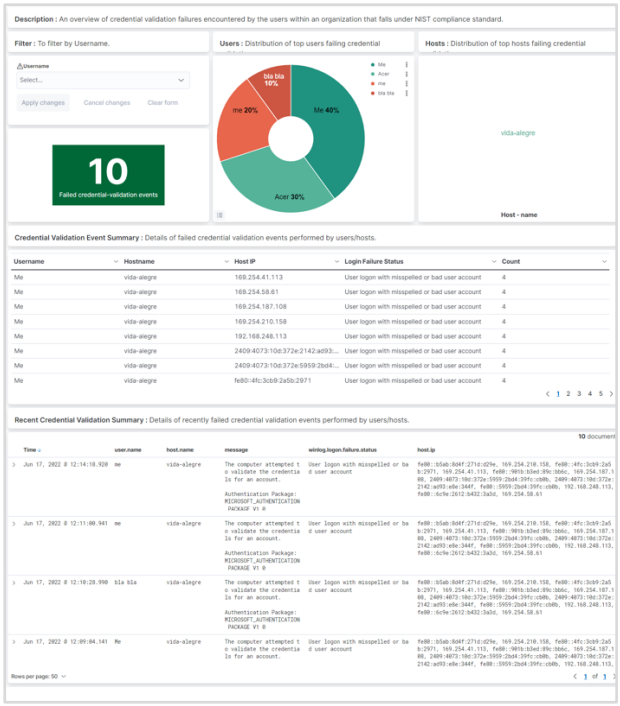
CYBOT compliance package consists of **compliance Dashboards** and **Active monitoring**

Dashboard for compliance

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

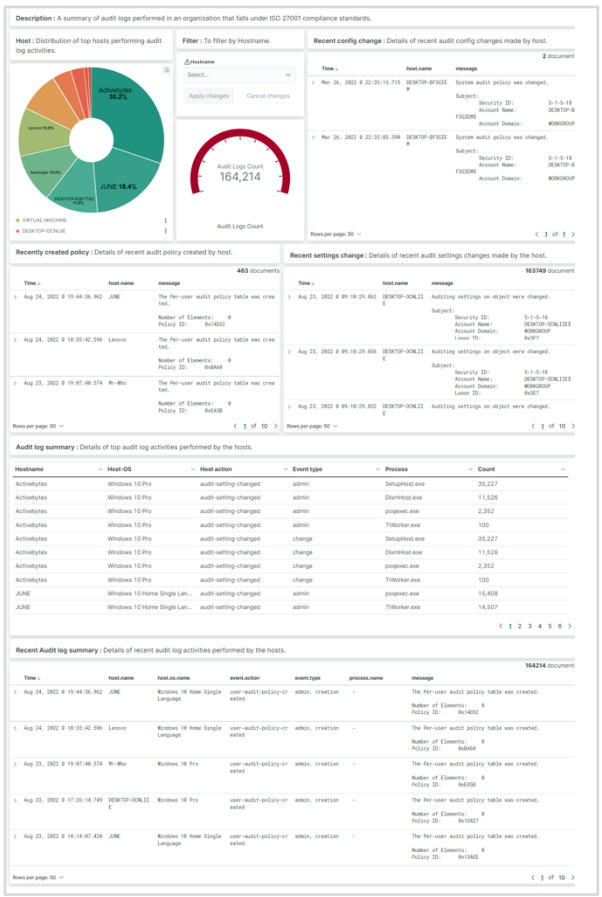


This dashboard shows an overview of rejected network connections encountered by the endpoints within an organization that falls under NIST compliance standards.

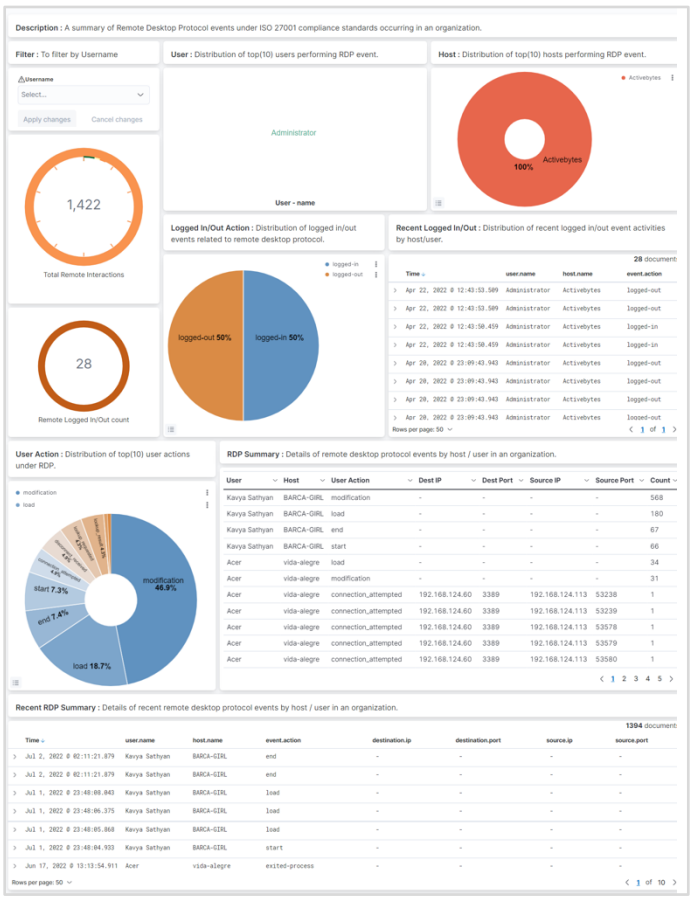


This dashboard gives an overview of credential validation failures encountered by the users within an organization that falls under NIST compliance standard.

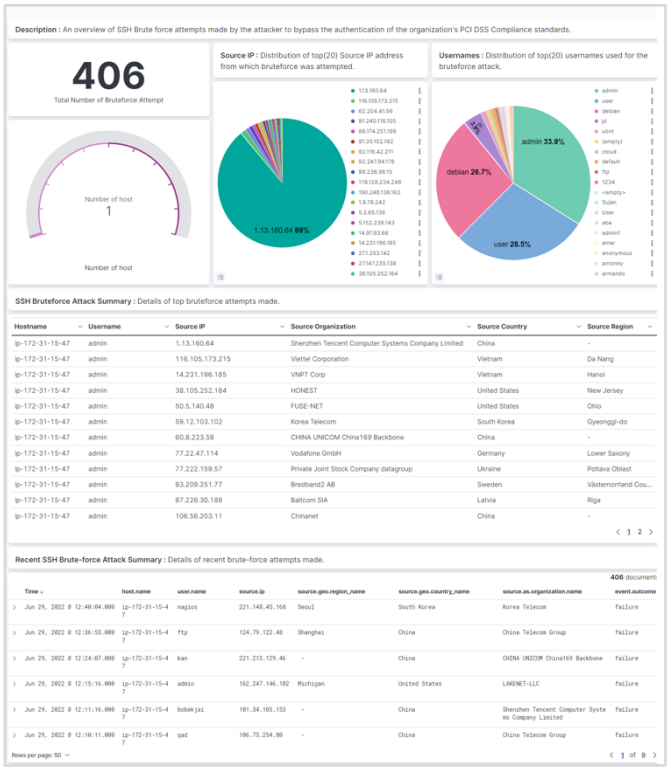
activebytes innovations



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

NIST Dashboard compliance			
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		SC-16 (1)	Verify the integrity of transmitted security and privacy attributes.

	NIST -08- File Integrity Monitor Log Summary	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		AC-2(4)	Automatically audit account creation, modification, enabling, disabling, and removal actions.

	NIST- 31 - Failed File System Access (Linux)	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.

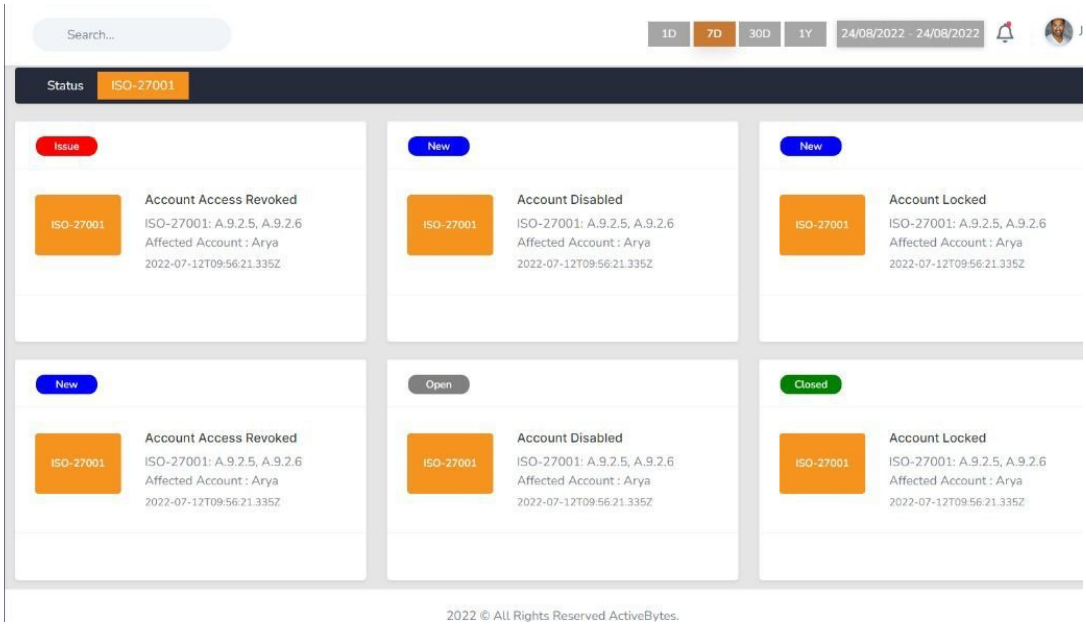


Fig 1

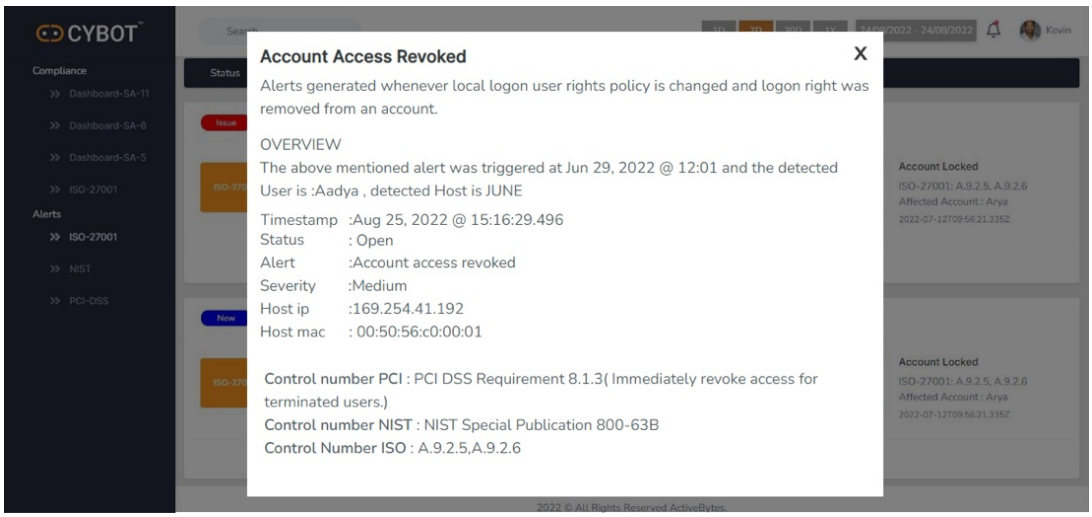


Fig 2

- ✓ 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)

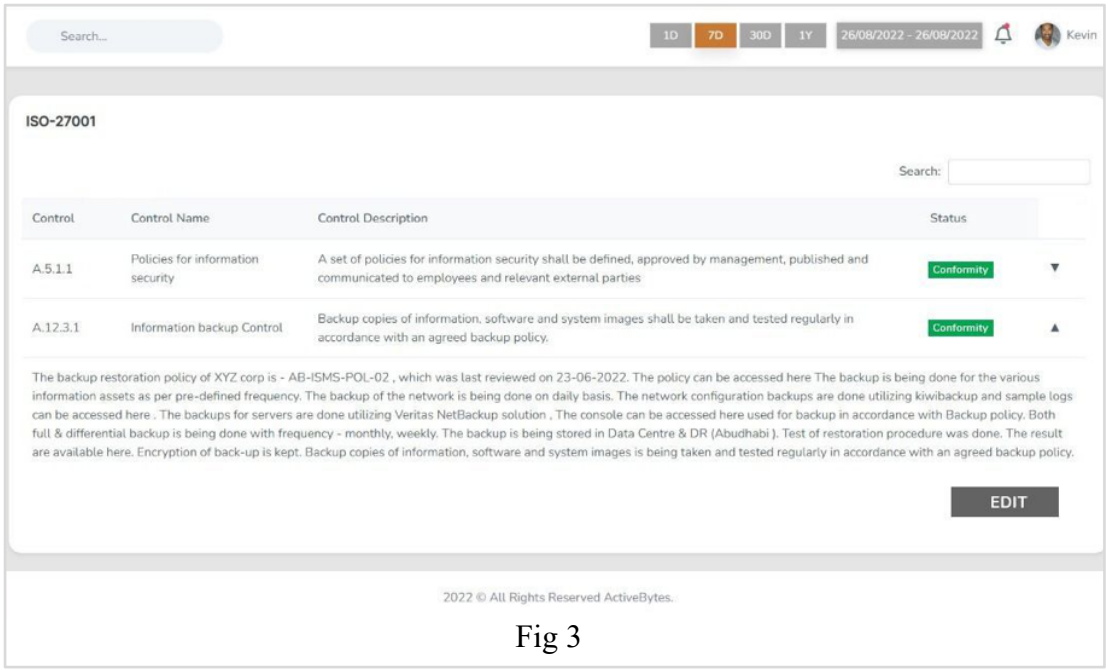


Fig 3

The compliance list for active monitoring is shown below:

Alert NIST compliance			
			Controls
#	**Alert name**	**Alert Description**	**NIST**
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.	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]
2	Windows Firewall Service failed	This alert will triggered when the Windows Firewall Service failed to start.	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.
3	Windows Firewall Driver failed	This alert will triggered Windows Firewall Driver failed to start.	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.
4	Windows Firewall Termination	The Windows Firewall Driver detected a critical runtime error (Terminating).	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.
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.	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.
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.	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.
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.	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.
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	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.

		disconnects from a virtual host.	
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.	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
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.	Direct- CM-11, a. Establish organization-defined policies governing the installation of software by users; b. Enforce software installation policies c. Monitor policy compliance
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.	Direct- CM-11, a. Establish organization-defined policies governing the installation of software by users; b. Enforce software installation policies c. Monitor policy compliance
12	Critical Environment Error	This alert will trigger if any critical environmental error happened in an organization.	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
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.	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on
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.	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure;
15	Audit Log was Cleared	The alert will trigger if the audit log was cleared.	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure;
16	Active Directory Password Reset	The alert attempt was made to reset an accounts password.	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
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.	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, 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.	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.
19	SID History Added	This event generates when SID History was added to an account.	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

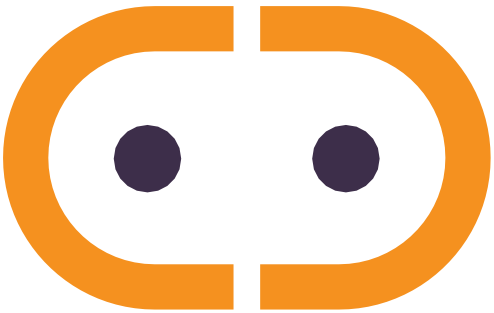
			entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (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].
20	SID History Added Failed	This event generates when an attempt to add SID History to an account failed.	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].
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.	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].
22	Detected Incomming Messages	RPC detected an integrity violation while decrypting an incoming message.	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].
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.	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.
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.	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
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.	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].

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	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.
27	Active Directory Privilege Operation	An operation was attempted on a privileged object.	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
28	Active Directory Services Access	A handle to an object was requested.	CM-5 ACCESS RESTRICTIONS FOR CHANGE Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
29	Alert-Data Loss Prevention Rule	This Alert is generated when there is event associated with 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.
30	Error Logging Service	The event logging service encountered an error. This alert is generated when the event logging service encounters an error	AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES a. Alert in the event of an audit logging process failure; and

		while processing an incoming event.	
31	User Privilege Assigned	This Alert is generated when a user privilege is assigned	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.
32	User Privilege Removed	This Alert is generated when a user privilege is removed	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.
33	User Account Unlocked	This Alert is generated when a user account is unlocked	AC-24 ACCESS CONTROL DECISIONS Establish procedures; Implement mechanisms] to ensureare applied to each access request prior to access enforcement.
34	Attempt to Disable Syslog Service	This Alert is generated when there is attempt to disable sys;og service	IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION Uniquely identify and authenticate] before establishing communications with devices, users, or other services or applications.
35	Attempt to Enable the Root Account	This Alert is generated when there is attempt to enable the root account	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; 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	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.
37	Failed File System	This alert is generated when permission to	AC-3 ACCESS ENFORCEMENT Enforce approved authorizations for logical access to information

	Access (Linux)	access the file system is denied.	and system resources in accordance with applicable access control policies.
38	System File Permission Change (Linux)	This alert is generated when the system file permissions (Read, Write, Execute) are changed.	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
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.	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



activebytes
innovations

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