CYBOT™

Automated Investigation & Hunting Platform

Datasheet

CYBOT™ Compliance (ISO 27001)

activebytes innovations

www.active-bytes.com

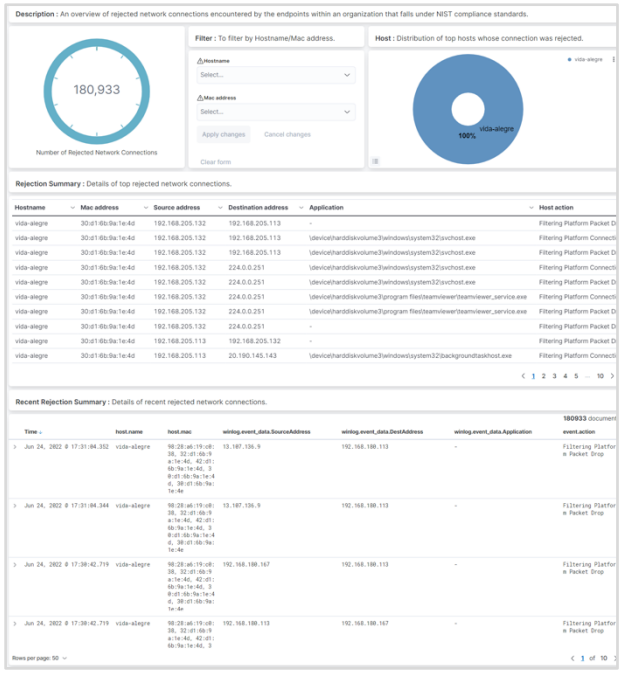
CYBOT™ Compliance

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

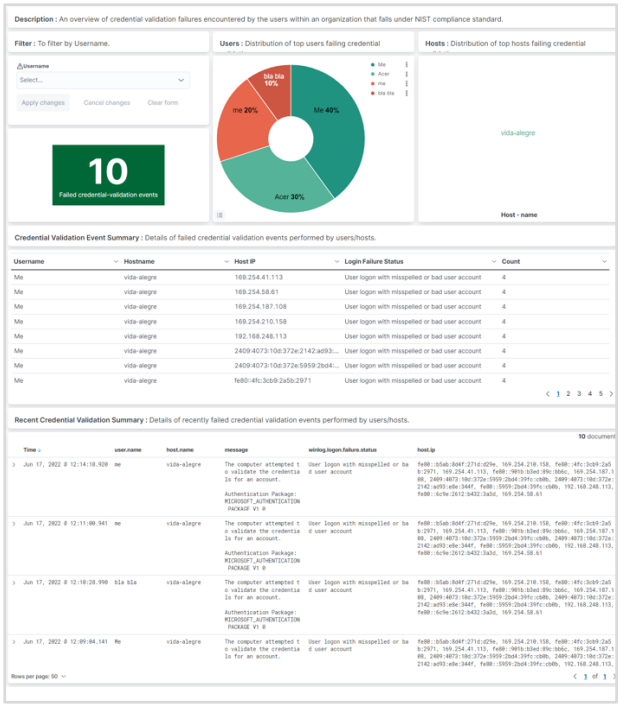
CYBOT compliance package consists of **compliance Dashboards** and **Active monitoring**

Dashboard for compliance

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

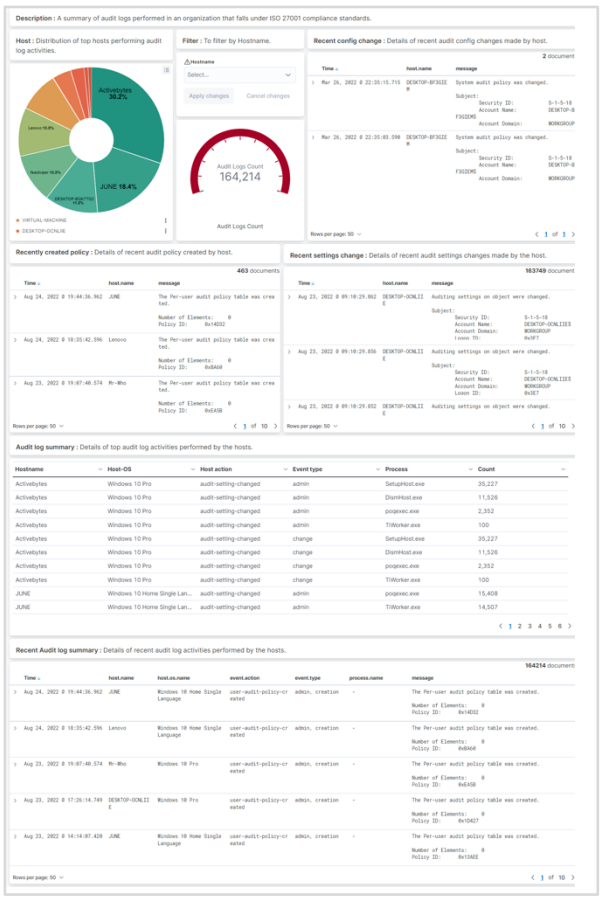


This dashboard shows an overview of rejected network connections encountered by the endpoints within an organization that falls under NIST compliance standards.

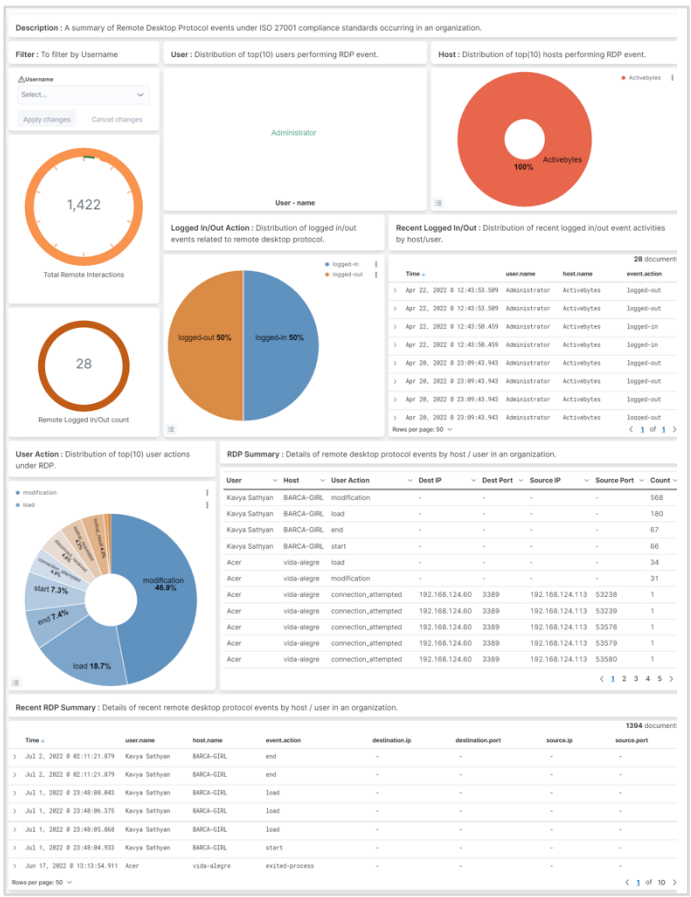


This dashboard gives an overview of credential validation failures encountered by the users within an organization that falls under NIST compliance standard.

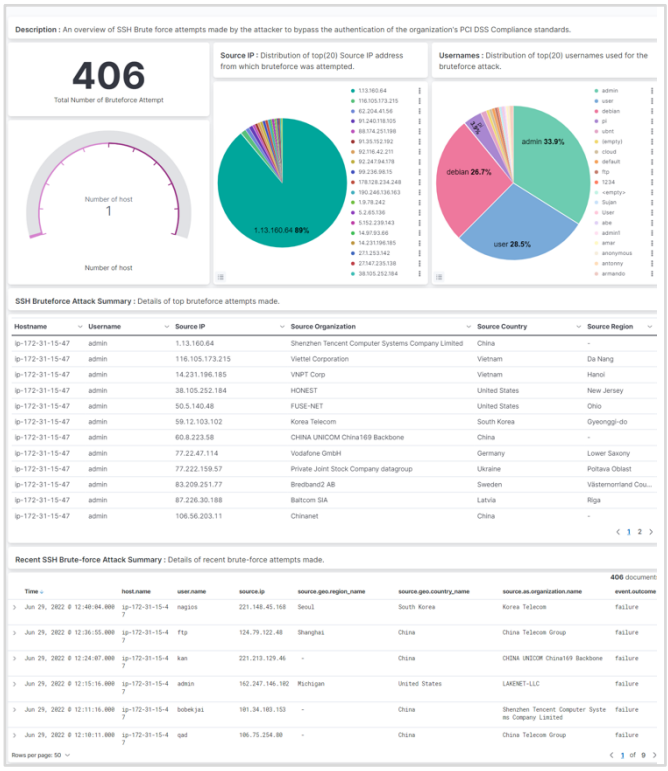
activebytes innovations



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

ISO 27001 Dashboard compliance list			
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

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.

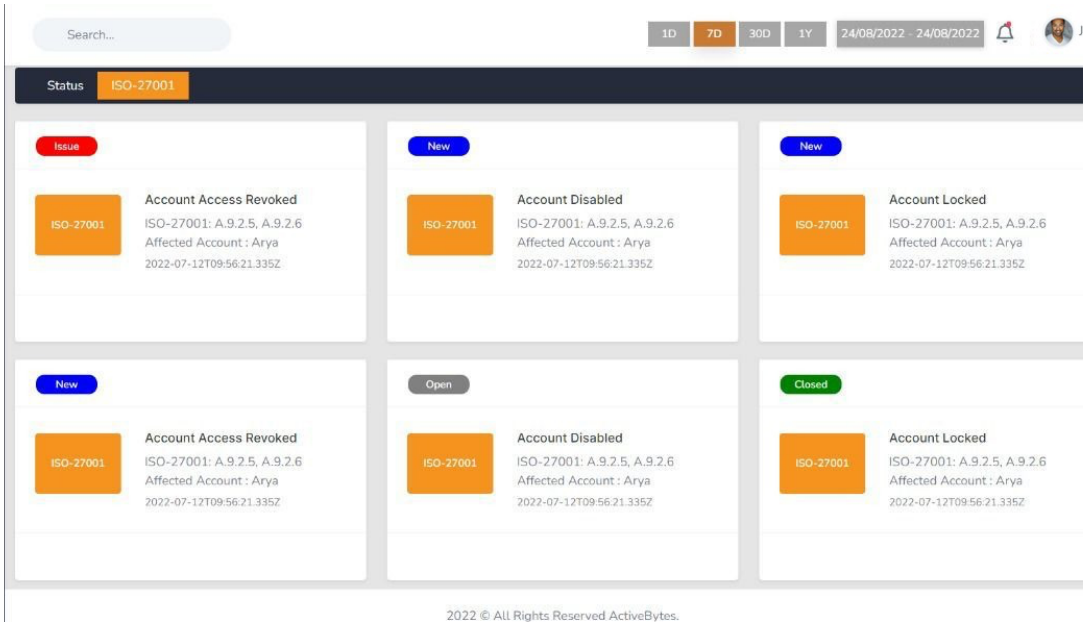


Fig 1

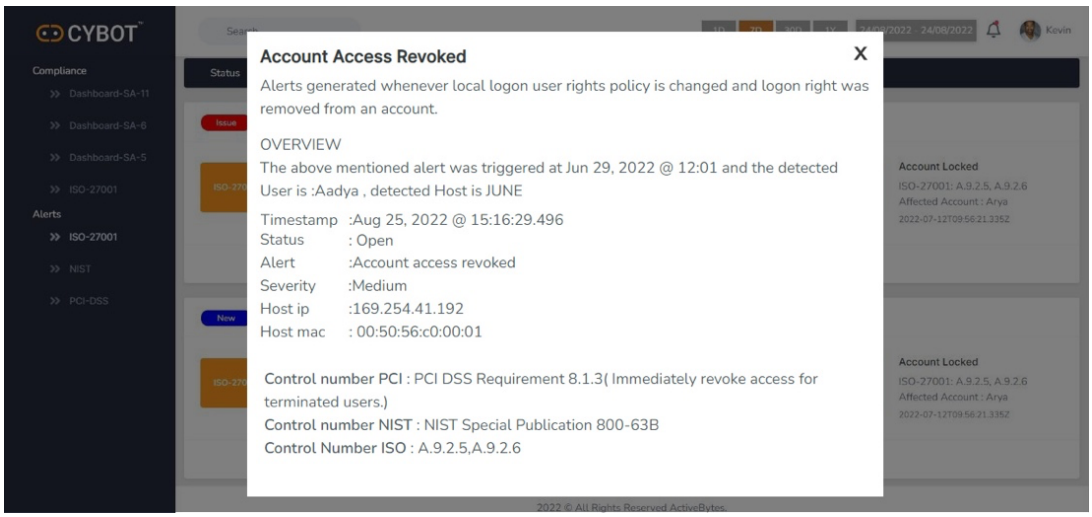


Fig 2

- ✓ 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)

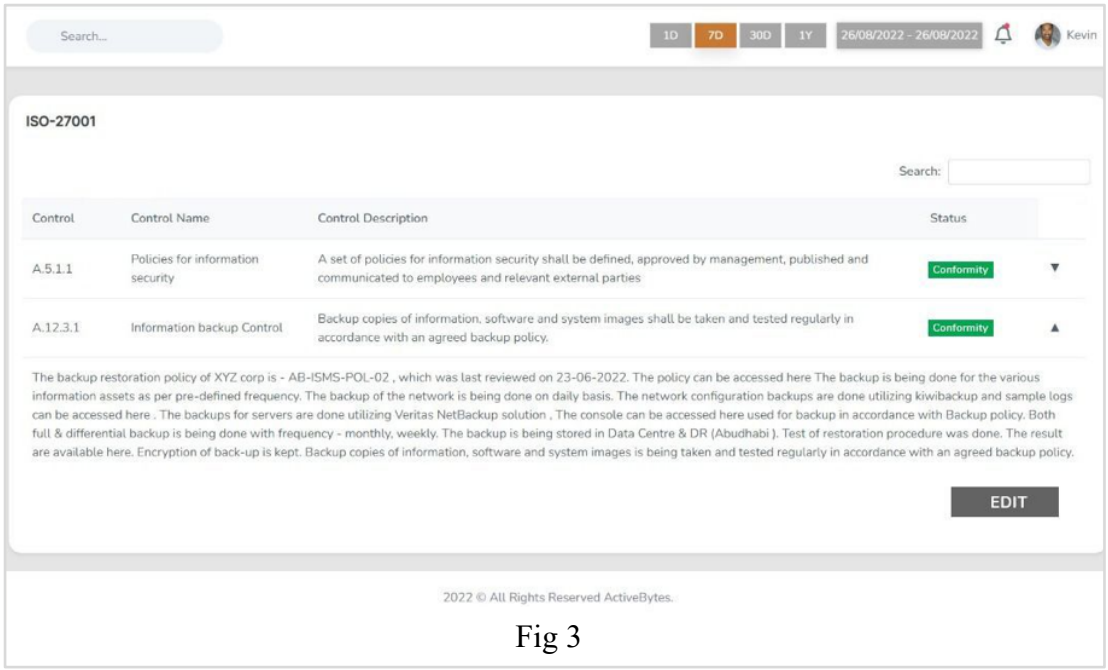


Fig 3

The compliance list for active monitoring is shown below:

Alert ISO 27001 compliance			
			Controls
#	**Alert name**	**Alert Description**	**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.	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.	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.	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).	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

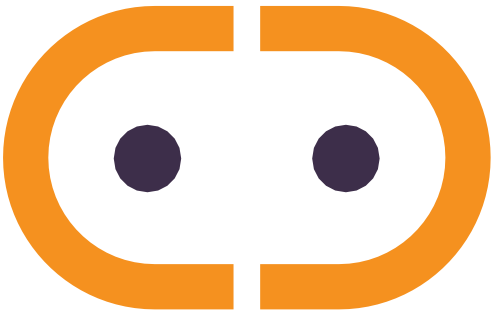
			packages are designed for the mass-market and are not really designed for organisations making their own changes to them. In fact most of the time the ability to make such changes is locked out by the vendor and customisation limited to within the package. Where open-source software is used, it is far 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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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	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.

		changed. This event is logged both for local SAM accounts and domain accounts.	
18	Device Disabled by the User	This event is generated when a user successfully disables a device.	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.
19	SID History Added	This event generates when SID History was added to an account.	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.	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.	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.
22	Detected Incomming Messages	RPC detected an integrity violation while decrypting an incoming message.	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.	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	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

		not be performed or a bug exists in the Sysmon service.	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.	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.
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	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.	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.	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	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.	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	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	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	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	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	A9.2.1 User registration and de-registration A9.2.2 User access provisioning A9.2.3 Management of privileged access rights
36	Blocked File Import/Export Attempt	This Alert is generated when there is attempt to import or export a blocked file	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.	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.	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.	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