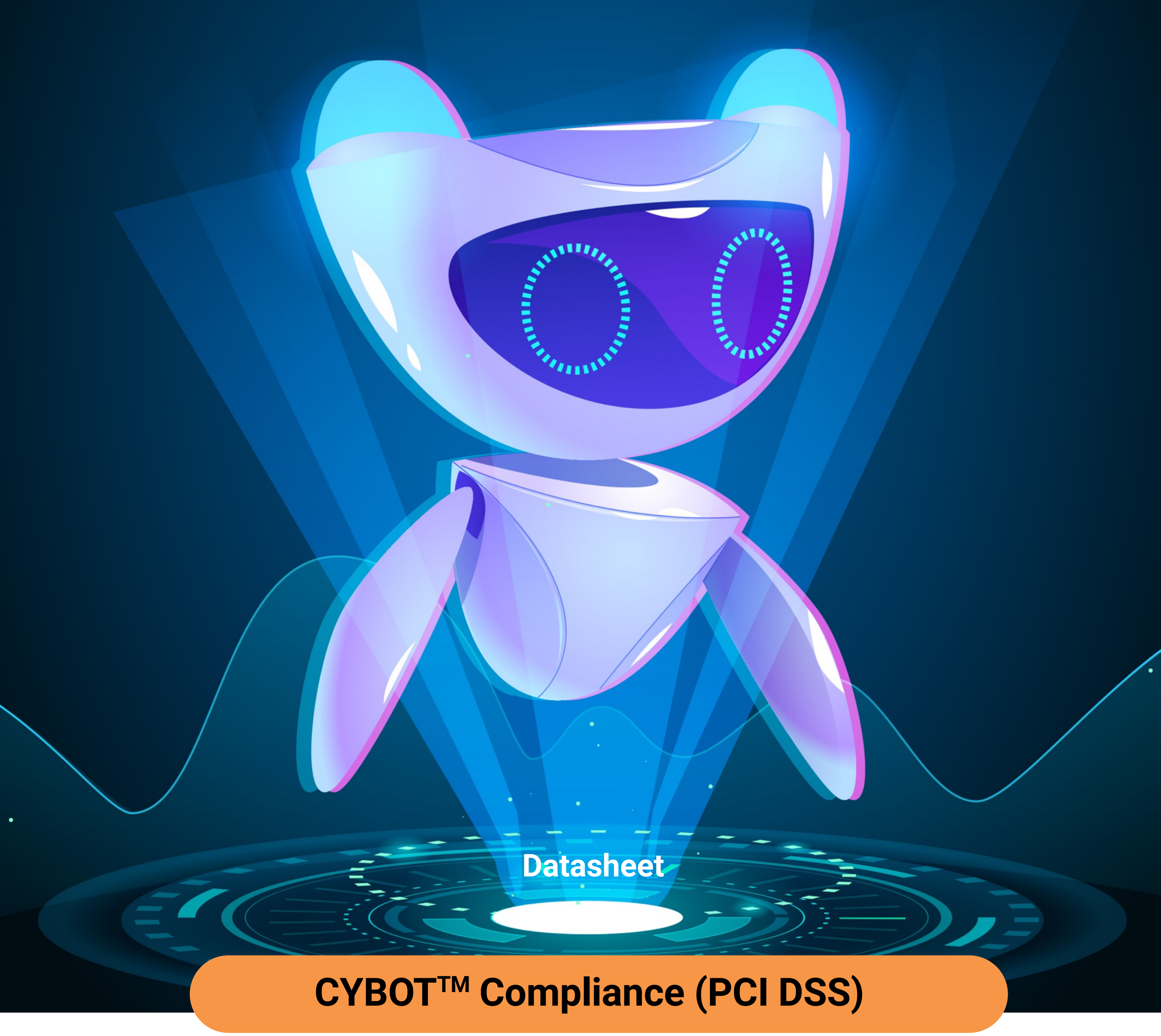
CYBOT™

Automated Investigation & Hunting Platform



Datasheet

CYBOT™ Compliance (PCI DSS)

activebytes innovations

www.active-bytes.com

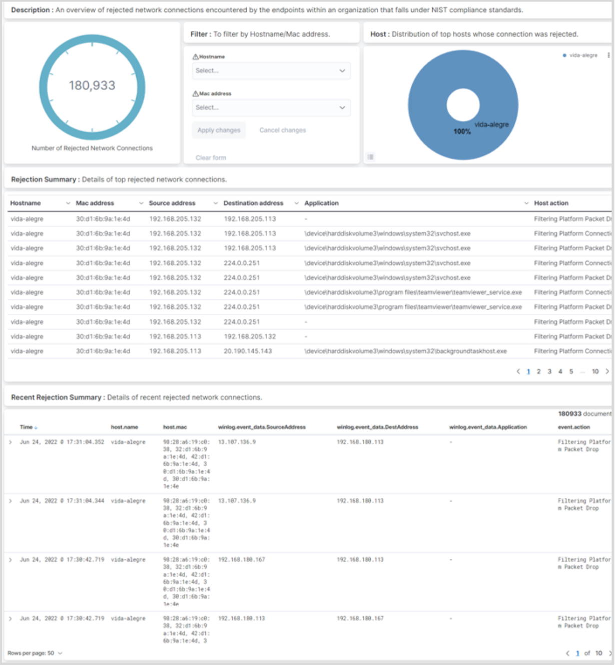
CYBOT™ Compliance

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



Description : An overview of rejected network connections encountered by the endpoints within an organization that falls under NIST compliance standards.

Filter : To filter by Hostname/Mac address.

Host : Distribution of top hosts whose connection was rejected.

Rejection Summary : Details of top rejected network connections.

Hostname	Mac address	Source address	Destination address	Application	Host action
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	192.168.205.113	-	Filtering Platform Packet D
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	192.168.205.113	\device\harddiskvolume3\windows\system32\svchost.exe	Filtering Platform Connecti
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	192.168.205.113	\device\harddiskvolume3\windows\system32\svchost.exe	Filtering Platform Packet D
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	224.0.0.251	\device\harddiskvolume3\windows\system32\svchost.exe	Filtering Platform Connecti
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	224.0.0.251	\device\harddiskvolume3\windows\system32\svchost.exe	Filtering Platform Packet D
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	224.0.0.251	\device\harddiskvolume3\program files\teamviewer\teamviewer_service.exe	Filtering Platform Connecti
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	224.0.0.251	\device\harddiskvolume3\program files\teamviewer\teamviewer_service.exe	Filtering Platform Packet D
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.132	224.0.0.251	-	Filtering Platform Packet D
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.113	192.168.205.132	-	Filtering Platform Packet D
vida-alegre	30:d1:6b:9a:1e:4d	192.168.205.113	20.190.145.143	\device\harddiskvolume3\windows\system32\backgroundtaskhost.exe	Filtering Platform Connecti

< 1 2 3 4 5 ... 10 >

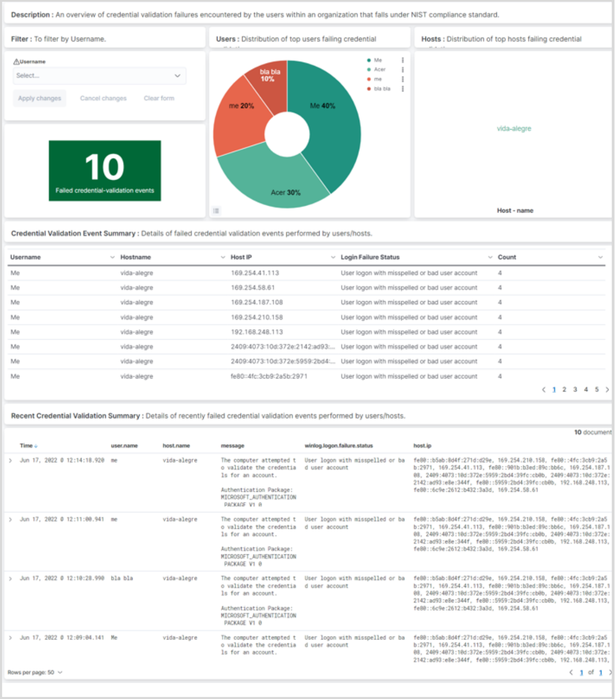
Recent Rejection Summary : Details of recent rejected network connections.

180933 document

Time	host.name	host.mac	winlog.event_data.SourceAddress	winlog.event_data.DestAddress	winlog.event_data.Application	event.action
Jun 24, 2022 @ 17:31:04.352	vida-alegre	98:28:a6:19:c0:38, 32:d1:6b:9a:1e:4d, 42:d1:6b:9a:1e:4d, 30:d1:6b:9a:1e:4d, 30:d1:6b:9a:1e:4e	13.107.136.9	192.168.180.113	-	Filtering Platform Packet Drop
Jun 24, 2022 @ 17:31:04.344	vida-alegre	98:28:a6:19:c0:38, 32:d1:6b:9a:1e:4d, 42:d1:6b:9a:1e:4d, 30:d1:6b:9a:1e:4d, 30:d1:6b:9a:1e:4e	13.107.136.9	192.168.180.113	-	Filtering Platform Packet Drop
Jun 24, 2022 @ 17:30:42.719	vida-alegre	98:28:a6:19:c0:38, 32:d1:6b:9a:1e:4d, 42:d1:6b:9a:1e:4d, 30:d1:6b:9a:1e:4d, 30:d1:6b:9a:1e:4e	192.168.180.167	192.168.180.113	-	Filtering Platform Packet Drop
Jun 24, 2022 @ 17:30:42.719	vida-alegre	98:28:a6:19:c0:38, 32:d1:6b:9a:1e:4d, 42:d1:6b:9a:1e:4d, 3	192.168.180.113	192.168.180.167	-	Filtering Platform Packet Drop

Rows per page: 50 < 1 of 10 >

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



Description : An overview of credential validation failures encountered by the users within an organization that falls under NIST compliance standard.

Filter : To filter by Username.

Users : Distribution of top users failing credential

Hosts : Distribution of top hosts failing credential

Credential Validation Event Summary : Details of failed credential validation events performed by users/hosts.

Username	Hostname	Host IP	Login Failure Status	Count
Me	vida-alegre	169.254.41.113	User logon with misspelled or bad user account	4
Me	vida-alegre	169.254.58.61	User logon with misspelled or bad user account	4
Me	vida-alegre	169.254.187.108	User logon with misspelled or bad user account	4
Me	vida-alegre	169.254.210.158	User logon with misspelled or bad user account	4
Me	vida-alegre	192.168.248.113	User logon with misspelled or bad user account	4
Me	vida-alegre	2409:4073:10d:372e:2142:ad93:...	User logon with misspelled or bad user account	4
Me	vida-alegre	2409:4073:10d:372e:5959:2bd4:...	User logon with misspelled or bad user account	4
Me	vida-alegre	fe80::4fc:3cb9:2a5b:2971	User logon with misspelled or bad user account	4

< 1 2 3 4 5 >

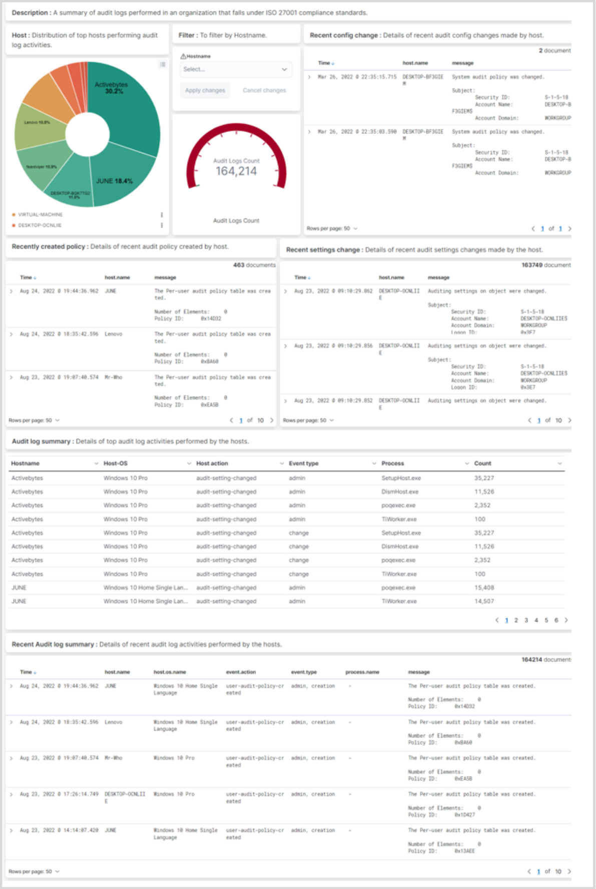
Recent Credential Validation Summary : Details of recently failed credential validation events performed by users/hosts.

10 document

Time	user.name	host.name	message	winlog.logon.failure.status	host.ip
Jun 17, 2022 @ 12:14:18.920	me	vida-alegre	The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION PACKAGE V1 0	User logon with misspelled or bad user account	fe80::b5ab:8d4f:271d:d29e, 169.254.210.158, fe80::4fc:3cb9:2a5b:2971, 169.254.41.113, fe80::901b:b3ed:89c:bb6c, 169.254.187.108, 2409:4073:10d:372e:5959:2bd4:39fc:cb0b, 2409:4073:10d:372e:2142:ad93:e8e:344f, fe80::5959:2bd4:39fc:cb0b, 192.168.248.113, fe80::6c9e:2612:b432:3a3d, 169.254.58.61
Jun 17, 2022 @ 12:11:00.941	me	vida-alegre	The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION PACKAGE V1 0	User logon with misspelled or bad user account	fe80::b5ab:8d4f:271d:d29e, 169.254.210.158, fe80::4fc:3cb9:2a5b:2971, 169.254.41.113, fe80::901b:b3ed:89c:bb6c, 169.254.187.108, 2409:4073:10d:372e:5959:2bd4:39fc:cb0b, 2409:4073:10d:372e:2142:ad93:e8e:344f, fe80::5959:2bd4:39fc:cb0b, 192.168.248.113, fe80::6c9e:2612:b432:3a3d, 169.254.58.61
Jun 17, 2022 @ 12:10:28.990	bla bla	vida-alegre	The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION PACKAGE V1 0	User logon with misspelled or bad user account	fe80::b5ab:8d4f:271d:d29e, 169.254.210.158, fe80::4fc:3cb9:2a5b:2971, 169.254.41.113, fe80::901b:b3ed:89c:bb6c, 169.254.187.108, 2409:4073:10d:372e:5959:2bd4:39fc:cb0b, 2409:4073:10d:372e:2142:ad93:e8e:344f, fe80::5959:2bd4:39fc:cb0b, 192.168.248.113, fe80::6c9e:2612:b432:3a3d, 169.254.58.61
Jun 17, 2022 @ 12:09:04.141	Me	vida-alegre	The computer attempted to validate the credentials for an account.	User logon with misspelled or bad user account	fe80::b5ab:8d4f:271d:d29e, 169.254.210.158, fe80::4fc:3cb9:2a5b:2971, 169.254.41.113, fe80::901b:b3ed:89c:bb6c, 169.254.187.108, 2409:4073:10d:372e:5959:2bd4:39fc:cb0b, 2409:4073:10d:372e:2142:ad93:e8e:344f, fe80::5959:2bd4:39fc:cb0b, 192.168.248.113,

Rows per page: 50 < 1 of 1 >

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



Description : A summary of audit logs performed in an organization that falls under ISO 27001 compliance standards.

Host : Distribution of top hosts performing audit log activities.

Filter : To filter by Hostname.

Recent config change : Details of recent audit config changes made by host.

2 document

Time	host.name	message
Mar 26, 2022 @ 22:35:15.715	DESKTOP-BF3GIEM	System audit policy was changed. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-BF3GIEM$ Account Domain: WORKGROUP
Mar 26, 2022 @ 22:35:03.590	DESKTOP-BF3GIEM	System audit policy was changed. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-BF3GIEM$ Account Domain: WORKGROUP

Rows per page: 50 ‹ 1 of 1 ›

Recently created policy : Details of recent audit policy created by host.

463 documents

Time	host.name	message
Aug 24, 2022 @ 19:44:36.962	JUNE	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x14D32
Aug 24, 2022 @ 18:35:42.596	Lenovo	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xBA60
Aug 23, 2022 @ 19:07:40.574	Mr-Who	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xEA5B

Rows per page: 50 ‹ 1 of 10 ›

Recent settings change : Details of recent audit settings changes made by the host.

163749 document

Time	host.name	message
Aug 23, 2022 @ 09:10:29.862	DESKTOP-OCNLIIE	Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-OCNLIIE$ Account Domain: WORKGROUP Logon ID: 0x3E7
Aug 23, 2022 @ 09:10:29.856	DESKTOP-OCNLIIE	Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-OCNLIIE$ Account Domain: WORKGROUP Logon ID: 0x3E7
Aug 23, 2022 @ 09:10:29.852	DESKTOP-OCNLIIE	Auditing settings on object were changed.

Rows per page: 50 ‹ 1 of 10 ›

Audit log summary : Details of top audit log activities performed by the hosts.

Hostname	Host-OS	Host action	Event type	Process	Count
Activebytes	Windows 10 Pro	audit-setting-changed	admin	SetupHost.exe	35,227
Activebytes	Windows 10 Pro	audit-setting-changed	admin	DismHost.exe	11,526
Activebytes	Windows 10 Pro	audit-setting-changed	admin	poqexec.exe	2,352
Activebytes	Windows 10 Pro	audit-setting-changed	admin	TiWorker.exe	100
Activebytes	Windows 10 Pro	audit-setting-changed	change	SetupHost.exe	35,227
Activebytes	Windows 10 Pro	audit-setting-changed	change	DismHost.exe	11,526
Activebytes	Windows 10 Pro	audit-setting-changed	change	poqexec.exe	2,352
Activebytes	Windows 10 Pro	audit-setting-changed	change	TiWorker.exe	100
JUNE	Windows 10 Home Single Lan...	audit-setting-changed	admin	poqexec.exe	15,408
JUNE	Windows 10 Home Single Lan...	audit-setting-changed	admin	TiWorker.exe	14,507

‹ 1 2 3 4 5 6 ›

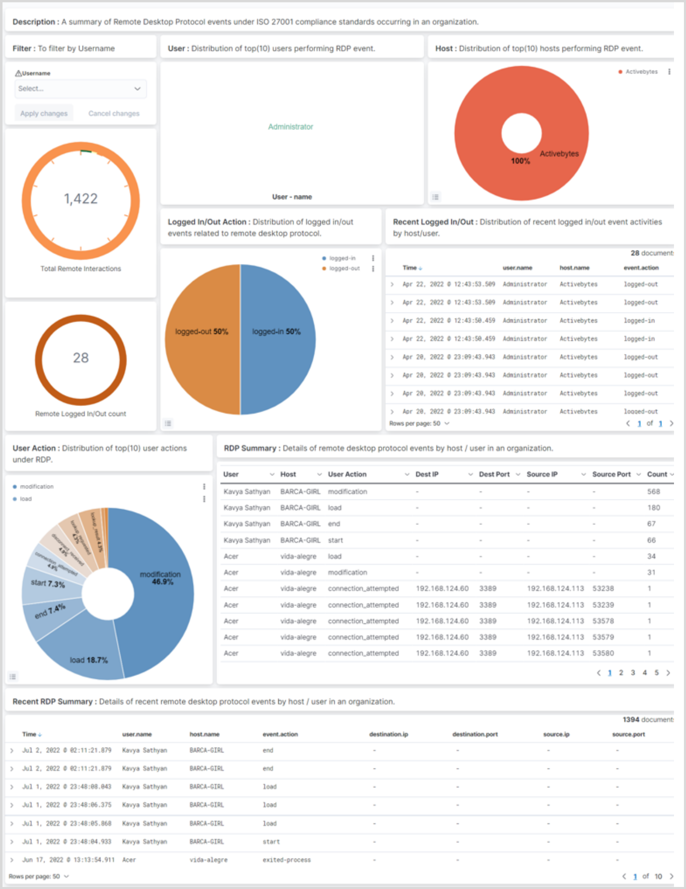
Recent Audit log summary : Details of recent audit log activities performed by the hosts.

164214 document

Time	host.name	host.os.name	event.action	event.type	process.name	message
Aug 24, 2022 @ 19:44:36.962	JUNE	Windows 10 Home Single Language	user-audit-policy-created	admin, creation	-	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x14D32
Aug 24, 2022 @ 18:35:42.596	Lenovo	Windows 10 Home Single Language	user-audit-policy-created	admin, creation	-	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xBA60
Aug 23, 2022 @ 19:07:40.574	Mr-Who	Windows 10 Pro	user-audit-policy-created	admin, creation	-	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xEA5B
Aug 23, 2022 @ 17:26:14.749	DESKTOP-OCNLIIE	Windows 10 Pro	user-audit-policy-created	admin, creation	-	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x1D427
Aug 23, 2022 @ 14:14:07.420	JUNE	Windows 10 Home Single Language	user-audit-policy-created	admin, creation	-	The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x13AEE

Rows per page: 50 ‹ 1 of 10 ›

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



Description : A summary of Remote Desktop Protocol events under ISO 27001 compliance standards occurring in an organization.

Filter : To filter by Username

User : Distribution of top(10) users performing RDP event.

Host : Distribution of top(10) hosts performing RDP event.

Logged In/Out Action : Distribution of logged in/out events related to remote desktop protocol.

Recent Logged In/Out : Distribution of recent logged in/out event activities by host/user.

28 document

Time	user.name	host.name	event.action
Apr 22, 2022 @ 12:43:53.509	Administrator	Activebytes	logged-out
Apr 22, 2022 @ 12:43:53.509	Administrator	Activebytes	logged-out
Apr 22, 2022 @ 12:43:50.459	Administrator	Activebytes	logged-in
Apr 22, 2022 @ 12:43:50.459	Administrator	Activebytes	logged-in
Apr 20, 2022 @ 23:09:43.943	Administrator	Activebytes	logged-out
Apr 20, 2022 @ 23:09:43.943	Administrator	Activebytes	logged-out
Apr 20, 2022 @ 23:09:43.943	Administrator	Activebytes	logged-out
Apr 20, 2022 @ 23:09:43.943	Administrator	Activebytes	logged-out

Rows per page: 50 ‹ 1 of 1 ›

User Action : Distribution of top(10) user actions under RDP.

RDP Summary : Details of remote desktop protocol events by host / user in an organization.

User	Host	User Action	Dest IP	Dest Port	Source IP	Source Port	Count
Kavya Sathyan	BARCA-GIRL	modification	-	-	-	-	568
Kavya Sathyan	BARCA-GIRL	load	-	-	-	-	180
Kavya Sathyan	BARCA-GIRL	end	-	-	-	-	67
Kavya Sathyan	BARCA-GIRL	start	-	-	-	-	66
Acer	vida-alegre	load	-	-	-	-	34
Acer	vida-alegre	modification	-	-	-	-	31
Acer	vida-alegre	connection_attempted	192.168.124.60	3389	192.168.124.113	53238	1
Acer	vida-alegre	connection_attempted	192.168.124.60	3389	192.168.124.113	53239	1
Acer	vida-alegre	connection_attempted	192.168.124.60	3389	192.168.124.113	53578	1
Acer	vida-alegre	connection_attempted	192.168.124.60	3389	192.168.124.113	53579	1
Acer	vida-alegre	connection_attempted	192.168.124.60	3389	192.168.124.113	53580	1

‹ 1 2 3 4 5 ›

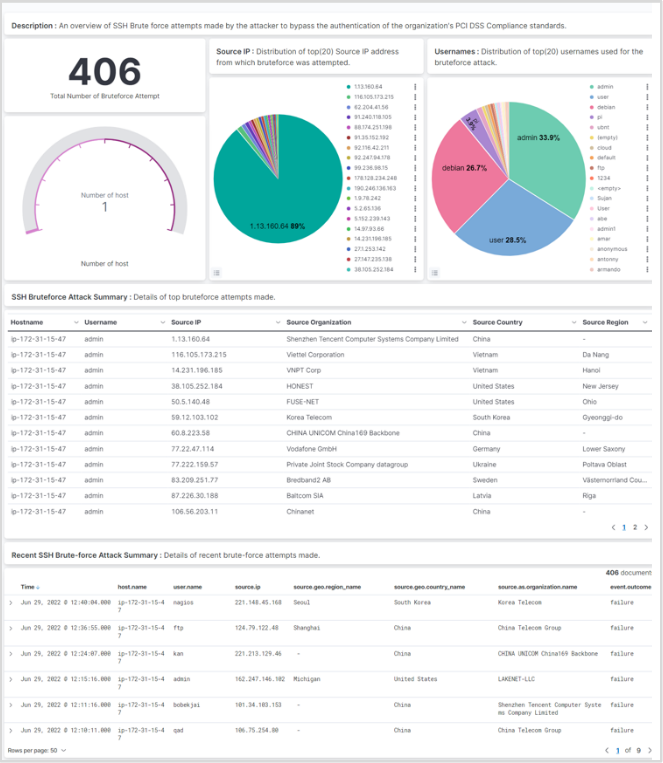
Recent RDP Summary : Details of recent remote desktop protocol events by host / user in an organization.

1394 document

Time	user.name	host.name	event.action	destination.ip	destination.port	source.ip	source.port
Jul 2, 2022 @ 02:11:21.879	Kavya Sathyan	BARCA-GIRL	end	-	-	-	-
Jul 2, 2022 @ 02:11:21.879	Kavya Sathyan	BARCA-GIRL	end	-	-	-	-
Jul 1, 2022 @ 23:48:08.043	Kavya Sathyan	BARCA-GIRL	load	-	-	-	-
Jul 1, 2022 @ 23:48:06.375	Kavya Sathyan	BARCA-GIRL	load	-	-	-	-
Jul 1, 2022 @ 23:48:05.868	Kavya Sathyan	BARCA-GIRL	load	-	-	-	-
Jul 1, 2022 @ 23:48:04.933	Kavya Sathyan	BARCA-GIRL	start	-	-	-	-
Jun 17, 2022 @ 13:13:54.911	Acer	vida-alegre	exited-process	-	-	-	-

Rows per page: 50 ‹ 1 of 10 ›

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



Description : An overview of SSH Brute force attempts made by the attacker to bypass the authentication of the organization's PCI DSS Compliance standards.

Source IP : Distribution of top(20) Source IP address from which bruteforce was attempted.

Usernames : Distribution of top(20) usernames used for the bruteforce attack.

SSH Bruteforce Attack Summary : Details of top bruteforce attempts made.

Hostname	Username	Source IP	Source Organization	Source Country	Source Region
ip-172-31-15-47	admin	1.13.160.64	Shenzhen Tencent Computer Systems Company Limited	China	-
ip-172-31-15-47	admin	116.105.173.215	Viettel Corporation	Vietnam	Da Nang
ip-172-31-15-47	admin	14.231.196.185	VNPT Corp	Vietnam	Hanoi
ip-172-31-15-47	admin	38.105.252.184	HONEST	United States	New Jersey
ip-172-31-15-47	admin	50.5.140.48	FUSE-NET	United States	Ohio
ip-172-31-15-47	admin	59.12.103.102	Korea Telecom	South Korea	Gyeonggi-do
ip-172-31-15-47	admin	60.8.223.58	CHINA UNICOM China169 Backbone	China	-
ip-172-31-15-47	admin	77.22.47.114	Vodafone GmbH	Germany	Lower Saxony
ip-172-31-15-47	admin	77.222.159.57	Private Joint Stock Company datagroup	Ukraine	Poltava Oblast
ip-172-31-15-47	admin	83.209.251.77	Bredband2 AB	Sweden	Västernorrland Cou...
ip-172-31-15-47	admin	87.226.30.188	Baltcom SIA	Latvia	Riga
ip-172-31-15-47	admin	106.56.203.11	Chinanet	China	-

‹ 1 2 ›

Recent SSH Brute-force Attack Summary : Details of recent brute-force attempts made.

406 document

Time	host.name	user.name	source.ip	source.geo.region_name	source.geo.country_name	source.as.organization.name	event.outcome
Jun 29, 2022 @ 12:40:04.000	ip-172-31-15-47	nagios	221.148.45.168	Seoul	South Korea	Korea Telecom	failure
Jun 29, 2022 @ 12:36:55.000	ip-172-31-15-47	ftp	124.79.122.48	Shanghai	China	China Telecom Group	failure
Jun 29, 2022 @ 12:24:07.000	ip-172-31-15-47	kan	221.213.129.46	-	China	CHINA UNICOM China169 Backbone	failure
Jun 29, 2022 @ 12:15:16.000	ip-172-31-15-47	admin	162.247.146.102	Michigan	United States	LAKENET-LLC	failure
Jun 29, 2022 @ 12:11:16.000	ip-172-31-15-47	bobekjai	101.34.103.153	-	China	Shenzhen Tencent Computer Systems Company Limited	failure
Jun 29, 2022 @ 12:10:11.000	ip-172-31-15-47	qad	106.75.254.80	-	China	China Telecom Group	failure

Rows per page: 50 ‹ 1 of 9 ›

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.

“PCI DSS” Dashboard compliance

NO:	Dashboard Name	PCI DSS Standard Control Number	Description
1	Compliance- PCI DSS- Host Configuration Change Summary	1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and theCDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity’s network. • Security controls are actively running. • Security controls are not alterable by users ofthe computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.
		6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		2.2.6	System security parameters are configured to prevent misuse.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity’s business and access needs. • Access to system components and data resources that is based on users’ job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
2	Compliance- PCI DSS - Data Transfer Summary	1.2.4	An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment
		6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
3	Compliance- PCI DSS - User Priv Escalation (Windows) Summary	6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity’s business and access needs. • Access to system components and data resources that is based on users’ job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities

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

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

		10.2.2	Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol)
10	Compliance- PCI DSS - Detailed File Share Summary	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
11	Compliance- PCI DSS - Suspected Wireless Connection Attempt Summary	1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.
		1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.
		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
12	Compliance- PCI DSS - Critical Environment Error Summary	6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
13	Compliance- PCI DSS - Failure Credential-validated Summary	6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.
		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
14		1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties

	Compliance- PCI DSS - Social Media Summary	1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity’s network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.
15	Compliance- PCI DSS - Failed File System Access (Linux)	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity’s business and access needs. • Access to system components and data resources that is based on users’ job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
		7.3.1	An access control system(s) is in place that restricts access based on a user’s need to know and covers all system components.
16	Compliance- PCI DSS - Rejected Connection to Network	1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.
		1.4.1	NSCs are implemented between trusted and untrusted networks.
		1.4.4	System components that store cardholder data are not directly accessible from untrusted networks
		1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied
		1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied
17	Compliance- PCI DSS - Detected Virus/Spyware Summary	5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware

		5.2.2	5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.
		5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection
		5.3.1	The anti-malware solution(s) is kept current via automatic updates
		6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		5.2.3.1.a	Examine the entity's targeted risk analysis for the frequency of periodic evaluations of system components identified as not at risk for malware to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1
		5.2.3.1.b	Examine documented results of periodic evaluations of system components identified as not at risk for malware and interview personnel to verify that evaluations are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement
		5.3.2.a	Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution(s) is configured to perform at least one of the elements specified in this requirement.
		5.3.2.b	Examine system components, including all operating system types identified as at risk for malware, to verify the solution(s) is enabled in accordance with at least one of the elements specified in this requirement
		5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1
		10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis
18	Compliance- PCI DSS - System File Permission Change (Linux)	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
		6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
		7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.

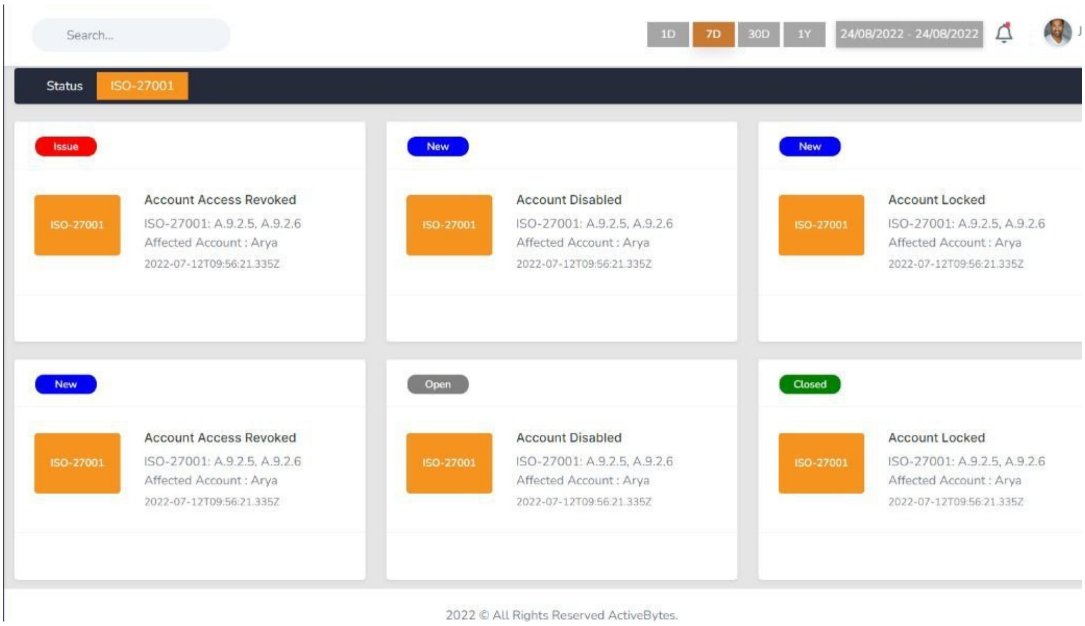
		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
19	Compliance- PCI DSS - Monitoring External Device Access	2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components
20	Compliance- PCI DSS - Detecting Brute Force Attack Summary	6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections
		6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.
21	Compliance- PCI-DSS - Physical Security Summary	7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.
22	Compliance- PCI-DSS - Unknown User Account Detail	7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.
23	Compliance- PCI-DSS - Time Sync Error Summary	6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections

		6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.
24	Compliance- PCI-DSS - System Log File Deletion Summary (Linux)	6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
25	Compliance- PCI-DSS - WebServer Access Logs Deleted Summary	6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections
		6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.
		7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.

Active Monitoring

Active monitoring is 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.



Account Access Revoked
ISO-27001: A.9.2.5, A.9.2.6
Affected Account : Arya
2022-07-12T09:56:21.335Z

Account Disabled
ISO-27001: A.9.2.5, A.9.2.6
Affected Account : Arya
2022-07-12T09:56:21.335Z

Account Locked
ISO-27001: A.9.2.5, A.9.2.6
Affected Account : Arya
2022-07-12T09:56:21.335Z

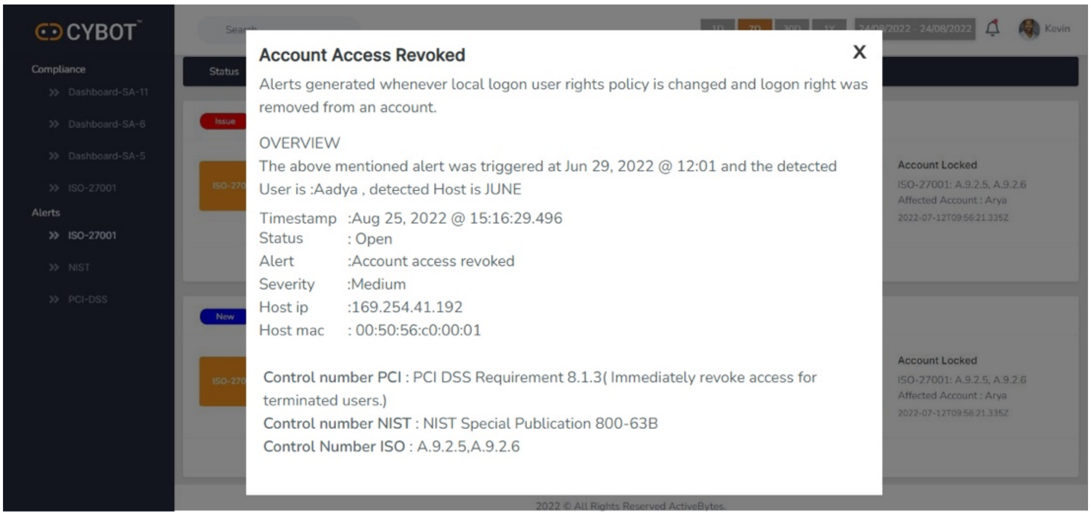
Account Access Revoked
ISO-27001: A.9.2.5, A.9.2.6
Affected Account : Arya
2022-07-12T09:56:21.335Z

Account Disabled
ISO-27001: A.9.2.5, A.9.2.6
Affected Account : Arya
2022-07-12T09:56:21.335Z

Account Locked
ISO-27001: A.9.2.5, A.9.2.6
Affected Account : Arya
2022-07-12T09:56:21.335Z

2022 © All Rights Reserved ActiveBytes.

Fig 1



Account Access Revoked

Alerts generated whenever local logon user rights policy is changed and logon right was removed from an account.

OVERVIEW

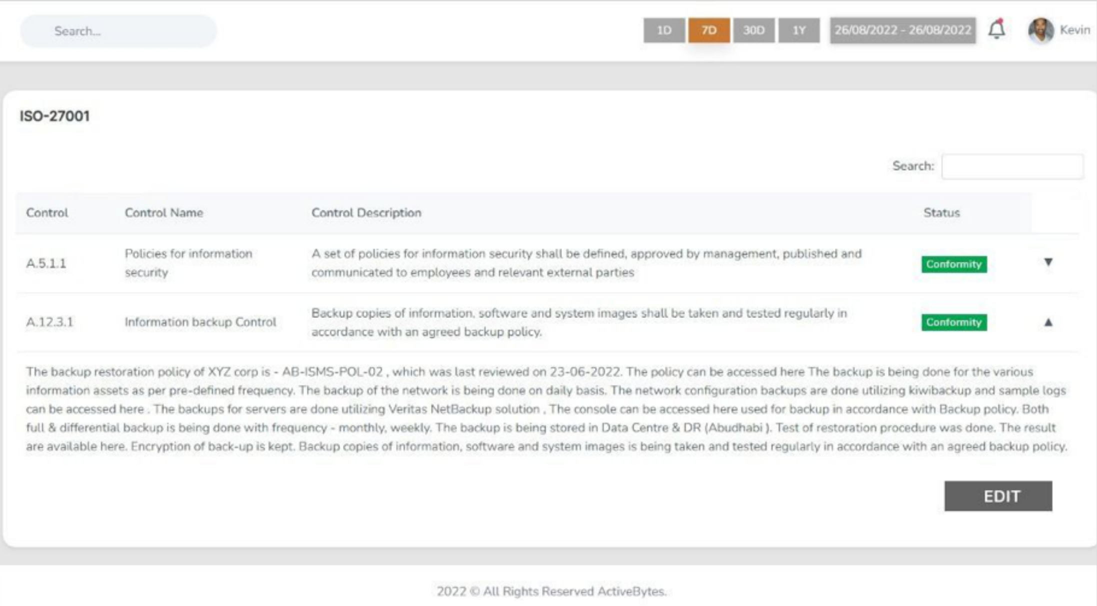
The above mentioned alert was triggered at Jun 29, 2022 @ 12:01 and the detected User is :Aadya , detected Host is JUNE

Timestamp :Aug 25, 2022 @ 15:16:29.496
Status : Open
Alert :Account access revoked
Severity :Medium
Host ip :169.254.41.192
Host mac : 00:50:56:c0:00:01

Control number PCI : PCI DSS Requirement 8.1.3(Immediately revoke access for terminated users.)
Control number NIST : NIST Special Publication 800-63B
Control Number ISO : A.9.2.5,A.9.2.6

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)



ISO-27001

Control	Control Name	Control Description	Status
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	Conformity
A.12.3.1	Information backup Control	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Conformity

The backup restoration policy of XYZ corp is - AB-ISMS-POL-02 , which was last reviewed on 23-06-2022. The policy can be accessed here The backup is being done for the various information assets as per pre-defined frequency. The backup of the network is being done on daily basis. The network configuration backups are done utilizing kiwibackup and sample logs can be accessed here . The backups for servers are done utilizing Veritas NetBackup solution , The console can be accessed here used for backup in accordance with Backup policy. Both full & differential backup is being done with frequency - monthly, weekly. The backup is being stored in Data Centre & DR (Abudhabi). Test of restoration procedure was done. The result are available here. Encryption of back-up is kept. Backup copies of information, software and system images is being taken and tested regularly in accordance with an agreed backup policy.

2022 © All Rights Reserved ActiveBytes.

Fig 3

The compliance list for active monitoring is shown below:

Compliance - Alert			
			Controls
#	**Alert name**	**Alert Description**	**PCI - DSS**
1	Logon from External Devices	A new external device was recognized by the system. This alert is generated when a new external device, such as a USB, is connected to the system.	2.2.4 Only necessary services, protocols, daemons,and functions are enabled, and all unnecessary functionality is removed or disabled. 3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. 5.3.3 For removable electronic media, the antimalware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted,OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.
2	Windows Firewall Service failed	This alert will triggered when the Windows Firewall Service failed to start.	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions.

			• Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
3	Windows Firewall Driver failed	This alert will triggered Windows Firewall Driver failed to start.	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
4	Windows Firewall Termination	The Windows Firewall Driver detected a critical runtime error (Terminating).	10.7.1 and 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
5	Detected Replay Attack	This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration.	8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks.
6	SMB Activity to the Internet	This rule detects network events that may indicate the use of SMB(Also known as Windows file sharing traffic to the Internet). SMB is commonly used within networks to share files, printers, and other system resources amongst trusted systems.	2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
7	User Remote Access Denied	A user was denied access to Remote Desktop. By default,	7.2.5 All application and system accounts and related access privileges are assigned and managed as follows:

		users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group.	• Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
8	Remote User Disconnected	If a user disconnects from an existing Terminal Services session, or switches away from an existing desktop using Fast User Switching, event 4779 is generated. This event is also triggered when a user disconnects from a virtual host.	7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
9	Active Directory Password Change	Alert makes Active Directory auditing very easy by tracking Password Status Changes for Users like password set or changed details with the help of pre-defined reports and instant alerts.	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:
10	Detecting Installed Applications	Alert will notify you when an installation is successfully completed. It also shows the user account that performed the installation process.	6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.
11	Detecting Uninstalled Applications	Alert will notify you when an uninstallation is successfully completed. It also shows the user account that performed the uninstallation process.	6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.
12	Critical Environment Error	This alert will trigger if any critical environmental error happened in an organization.	Requirement 10: Log and Monitor All Access to System Components and Cardholder Data 10.7.1 - Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS.

			• FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).
13	Encrypted Policy Change	This computer's Security Settings\Public Key Policies\Encrypting File System data recovery agent policy was modified - either via Local Security Policy or Group Policy in Active Directory.	3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely
14	System Audit Policy Change	This computer's system level audit policy was modified - either via Local Security Policy, Group Policy in Active Directory or the audipol command. According to Microsoft, this event is always logged when an audit policy is disabled, regardless of the "Audit Policy Change" sub-category setting. This and several other events can help identify when someone attempts to disable auditing to cover their tracks.	10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events
15	Audit Log was Cleared	The alert will trigger if the audit log was cleared.	10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events
16	Active Directory Password Reset	The alert attempt was made to reset an accounts password.	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:
17	Modified User Accounts	The user identified by Subject: changed the user identified by Target Account. Attributes show some	7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain

		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.	appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.
18	Device Disabled by the User	This event is generated when a user successfully disables a device.	10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.
19	SID History Added	This event generates when SID History was added to an account.	10.2.1 - Audit logs are enabled and active for all system components and cardholder data.
20	SID History Added Failed	This event generates when an attempt to add SID History to an account failed.	10.2.1 - Audit logs are enabled and active for all system components and cardholder data.
21	Kerberos Policy Changes	This alert detects a change to the the domain's Kerberos policy. Kerberos policy is defined in GPOs linked to the root of the domain under Computer Configuration\Windows Settings\Security Settings\Account Policy\Kerberos Policy.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.
22	Detected Incomming Messages	RPC detected an integrity violation while decrypting an incoming message.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.

23	Request Enabled Device	A request was made to enable a device. This alert is generated if a user attempts to enable a device on the system. This does not mean that a device was successfully enabled.	10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.
24	Sysmon Error	This alert is generated when an error occurred within Sysmon. They can happen if the system is under heavy load and certain tasked could not be performed or a bug exists in the Sysmon service.	10.2.1.7 Audit logs capture all creation and deletion of system-level objects.
25	Domain Policy Change	This alert is generated when an Active Directory Domain Policy is modified. It is logged on domain controllers and member computers.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.
26	Restore Administrator Password	An attempt was made to set the Directory Services Restore Mode administrator password. This alert is generated when DSRM administrator password is changed. It is logged only on domain controllers	8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.
27	Active Directory Privilege Operation	An operation was attempted on a privileged object.	A3.4.1 User accounts and access privileges to inscope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized.
28	Active Directory	A handle to an object was requested.	7.2 Access to system components and data is appropriately defined and assigned.

	Services Access		
29	Alert-Data Loss Prevention Rule	This Alert is generated when there is event associated with data loss	A3.2.6.1 Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss.
30	Error Logging Service	The event logging service encountered an error. This alert is generated when the event logging service encounters an error while processing an incoming event.	10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.
31	User Privilege Assigned	This Alert is generated when a user privilege is assigned	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)
32	User Privilege Removed	This Alert is generated when a user privilege is removed	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)
33	User Account Unlocked	This Alert is generated when a user account is unlocked	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 7.2 Access to system components and data is appropriately defined and assigned. 7.3 Access to system components and data is managed via an access control system(s)
34	Attempt to Disable Syslog Service	This Alert is generated when there is attempt to disable sys;og service	10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs
35	Attempt to Enable the Root Account	This Alert is generated when there is attempt	8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are

		to enable the root account	managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.
36	Blocked File Import/Export Attempt	This Alert is generated when there is attempt to import or export a blocked file	1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks.
37	Failed File System Access (Linux)	This alert is generated when permission to access the file system is denied.	10.2.1 Audit logs are enabled and active for all system components and cardholder data.
38	System File Permission Change (Linux)	This alert is generated when the system file permissions (Read, Write, Execute) are changed.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.
39	System File Permission Change (Windows)	Permissions on an object were changed. This alert is generated when someone changes the access control list on an object. The event identifies the object, who changed the permissions and the old an new permissions.	11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.

activebytes
innovations

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