

HIPAA report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	wazuh_agent_ub untu_2	172.20.0.7	Wazuh v4.9.0	wazuh- manager-4.9.0-71 02	Ubuntu 22.04.3 LTS	May 14, 2024 @ 14:50:11.000	May 16, 2024 @ 15:38:39.000

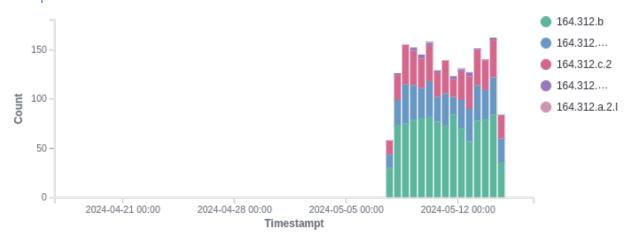
Group: default

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

2 2024-04-16T17:38:44 to 2024-05-16T17:38:44

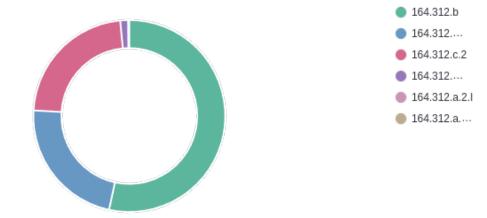
Q rule.hipaa: * AND cluster.name: wazuh AND agent.id: 002

Requirements over time

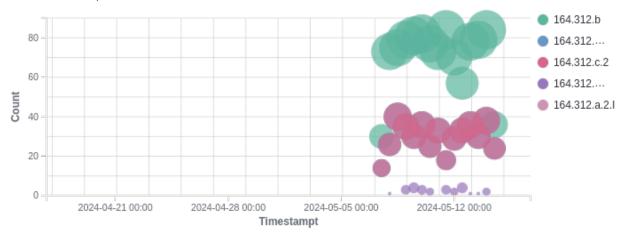




Top 10 requirements



HIPAA requirements



Requirements distribution by level



Most common alerts

164.312.a.2.l 164.312.c.2 164.312.b 164.312.c.1 164.312.a.1



Alerts summary

Requirement	Level	Description	Count
164.312.b	5	Apache: Attempt to access forbidden directory index.	297
164.312.b	3	Windows: Service startup type was changed.	153
164.312.c.1	7	Integrity checksum changed.	153
164.312.c.2	7	Integrity checksum changed.	153
164.312.c.1	7	File deleted.	149
164.312.c.2	7	File deleted.	149
164.312.c.1	5	File added to the system.	141
164.312.c.2	5	File added to the system.	141
164.312.b	5	sshd: Attempt to login using a non-existent user	93
164.312.b	5	Logon Failure - Unknown user or bad password	48
164.312.b	5	sshd: authentication failed.	45
164.312.b	5	unix_chkpwd: Password check failed.	43
164.312.b	5	PAM: User login failed.	42
164.312.b	10	sshd: Multiple authentication failures.	42
164.312.b	10	sshd: brute force trying to get access to the system.	38
164.312.b	8	Netscreen firewall: Successfull admin login	10
164.312.b	6	Postfix: Multiple relaying attempts of spam.	10
164.312.b	3	Imapd user login.	8
164.312.b	6	Postfix: too many errors after RCPT from unknown	8
164.312.b	3	Cisco IOS: Successful login to the router.	7
164.312.b	3	User successfully changed UID.	7
164.312.b	10	Courier brute force (multiple failed logins).	7
164.312.b	8	Interface entered in promiscuous(sniffing) mode.	7
164.312.b	8	PIX: Firewall configuration changed.	7
164.312.a.1	8	PIX: Firewall configuration changed.	7
164.312.b	3	SonicWall: Firewall administrator login.	6
164.312.b	3	User successfully changed UID to root.	6
164.312.b	10	Netscreen firewall: Multiple critical messages from same source IP.	6
164.312.b	10	Postfix process error.	6
164.312.b	10	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	6
164.312.b	10	SonicWall: Multiple firewall error messages.	6
164.312.b	8	Root's crontab entry changed.	6
164.312.b	6	Postfix: Rejected by access list (Requested action not taken).	6
164.312.a.1	10	Netscreen firewall: Multiple critical messages from same source IP.	6
164.312.b	3	Ossec agent removed.	5
164.312.b	3	PIX: AAA (VPN) authentication successful.	5
164.312.b	10	Courier: Multiple connection attempts from same source.	5
164.312.b	8	Log file size reduced.	5
164.312.b	8	PIX: Firewall configuration deleted.	5



164.312.b 6 Postfix: IP Address black listed by anti-spam (blockad): 5 164.312.b 6 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 5 164.312.b 9 Microsoft Fivent log cleared. 5 164.312.b 9 miss-exchange Multiple e-mail 500 error code (spam). 5 164.312.b 11 Netscreen Eriase sequence started. 5 164.312.a.1 8 PIX: Flewall configuration deleted. 5 164.312.b.1 10 Settoree Eriase sequence started. 5 164.312.b.1 10 Postfix: Sender domain is not found (450: Requested mail action not taken). 4 164.312.b.1 10 spolag, User missed the password more than one time. 4 164.312.b.2 10 spolag, User missed the password to change UID to root. 4 164.312.b.3 9 User missed the password to change UID to root. 4 164.312.b.3 9 mis exchange. Multiple e-mail attempts to an invalid account. 4 164.312.b.3 10 Registry integrity Checksum Changed. 4 164.312.b.3 2 <th>Requirement</th> <th>Level</th> <th>Description</th> <th>Count</th>	Requirement	Level	Description	Count
164.312.b 9 Microsoft Event log cleared. 5 164.312.b 9 miseachanger, Multiple email 500 error code (spam). 5 164.312.b 11 Netscreen Erase sequence started. 5 164.312.a.1 11 Netscreen Erase sequence started. 5 164.312.b.1 11 Netscreen Erase sequence started. 5 164.312.b.1 11 Netscreen Erase sequence started. 5 164.312.b.1 10 syclog: User missed the password more than one time 4 164.312.b.1 10 sinetd: Excessive number connections. 4 164.312.b.1 10 sinetd: Excessive number connections. 4 164.312.b.2 9 User missed the password to change up. Ulto to root. 4 164.312.b.3 9 User missed the password to change. Ulto to root. 4 164.312.b.3 9 User missed the password to change. Ulto to root. 4 164.312.b.3 9 User missed the password to change. 4 164.312.b.3 5 Registry Integrity Checksum Change. 4 164.312.b.	164.312.b	6	Postfix: IP Address black-listed by anti-spam (blocked).	5
164.312.b 9 mis-exchange: Multiple e-mail 500 error code (spsm). 5 164.312.b 11 Netscreen Frase sequence started. 5 164.312.b 11 Netscreen Frase sequence started. 5 164.312.b 11 Netscreen Frase sequence started. 5 164.312.b 10 syslog: User missed the password more than one time. 4 164.312.b 10 syslog: User missed the password nor change UID to root. 4 164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 missexchange: Multiple e-mail attempts to an invalid account. 4 164.312.b 9 missexchange: Multiple e-mail attempts to an invalid account. 4 164.312.b 3 Registry integrity Checksum Changed 4 164.312.b 3 Registry integrity Checksum Changed 4 164.312.b 3 Courier (imaphops3) authentication success.	164.312.b	6	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	5
164312.b 11 Netscreen Erase sequence started. 5 164312.b 18 PIX: Firewall configuration deleted. 5 164312.b 10 Pestific Seconder domain is not found (450. Requested mail action not taken). 4 164312.b 5 Postific Seconder domain is not found (450. Requested mail action not taken). 4 164312.b 10 syslog: User missed the password more than one time 4 164312.b 10 vinetd: Excessive number connections. 4 164312.b 3 PIX: The PIX is disallowing new connections. 4 164312.b 9 User missed the password to change UID to root. 4 164312.b 9 User missed the password to change UID to root. 4 164312.c 5 Registry integrity Checksum Changed 4 164312.c 5 Registry integrity Checksum Changed 4 164312.b 5 syslog: Connection blocked by Tcp Wrappers. 3 164312.b 3 Courier (imar/pop3) authentication success. 3 164312.b 10 Connection to rabid from unprivileged port. Possible n	164.312.b	9	Microsoft Event log cleared.	5
164.312.a.1 8 PDK. Firowall configuration deleted. 5 164.312.b.1 11 Netscreen Frose sequence started. 5 164.312.b.5 Postfix: Sender domain is not found (450: Requested mail action not taken). 4 164.312.b.1 10 syslog! User missed the password more than one time. 4 164.312.b.1 10 xineed: Excessive number connections to a service. 4 164.312.b.2 9 User missed the password to change UID to root. 4 164.312.b.9 9 user missed the password to change UID to root. 4 164.312.b.9 9 ms exchange: Multiple e-mail attempts to an invalid account. 4 164.312.b.9 9 ms exchange: Multiple e-mail attempts to an invalid account. 4 164.312.b.5 5 Registry integrity Checksum Changed 4 164.312.b.5 5 sylog. Connection blocked by Tcp Wrappers. 3 164.312.b.5 5 sylog. Connection blocked by Tcp Wrappers. 3 164.312.b.1 10 Connection to rish from unprivileged port. Possible network scan. 3 164.312.b.1 10	164.312.b	9	ms-exchange: Multiple e-mail 500 error code (spam).	5
164.312.b.1 11 Netscreen Erase sequence started. 5 164.312.b.5 5 Postfix: Sender domain is not found (450: Requested mail action not taken). 4 164.312.b.1 10 systog: User missed the password more than one time. 4 164.312.b.1 10 systog: User missed the password to change under the content of the content. 4 164.312.b.9 10 User missed the password to change UID to root. 4 164.312.b.9 9 User missed the password to change UID to root. 4 164.312.b.1 9 ms-exchange: Multiple e-mail attempts to an invalid account. 4 164.312.b.1 9 ms-exchange: Multiple ermail attempts to an invalid account. 4 164.312.b.2 10 ms-exchange: Multiple ermail attempts to an invalid account. 4 164.312.b.1 5 segistry integrity Checksum Changed 4 164.312.b.2 5 systog: Connection blocked by Tcp Wrappers. 3 164.312.b.3 6 Curier (imap/pop3) authentication success. 3 164.312.b.3 7 PAM: Login session opened. 3 164.312.b.	164.312.b	11	Netscreen Erase sequence started.	5
164.312.b 5 Postfix Sender domain is not found (450. Requested mail action not taken). 4 164.312.b 10 syslog: User missed the password more than one time 4 164.312.b 10 xinerdi. Excessive number connections to a service. 4 164.312.b 8 PIX: The PIX is disallowing new connections. 4 164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 ms-exchange: Multiple e-mail attempts to an invalid account. 4 164.312.c 5 Registry Integrity Checksum Changed 4 164.312.b 5 Registry Integrity Checksum Changed 4 164.312.b 5 Registry Integrity Checksum Changed 4 164.312.b 5 syslog: Connection blocked by Top Wrappers. 3 164.312.b 5 syslog: Connection blocked by Top Wrappers. 3 164.312.b 10 Connection to rishd from unprivileged port. Possible network scan. 3 164.312.b 10 Connection to rishd from unprivileged port. Possible network scan. 3 164.312.b 10	164.312.a.1	8	PIX: Firewall configuration deleted.	5
164.312.b 10 syslog: User missed the password more than one time 4 164.312.b 10 xinetd: Excessive number connections to a service. 4 164.312.b 8 PVE The PIX is disallowing new connections. 4 164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 ms exchange: Multiple e-mail attempts to an invalid account. 4 164.312.c.1 5 Registry Integrity Checksum Changed 4 164.312.b 5 Registry Integrity Checksum Changed 4 164.312.b 5 syslog: Connection blocked by Tcp Wrappers. 3 164.312.b 5 syslog: Connection blocked by Tcp Wrappers. 3 164.312.b 3 Courier (imap/oop3) authentication success. 3 164.312.b 10 Connection to rishd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple alled logins in a small period of time. 3 164.312.b 10 POX MITCPLE AMP (PN) authentication failures. 3 164.312.b 10 POX Multiple attempts to send	164.312.a.1	11	Netscreen Erase sequence started.	5
164.312.b 10 xinetd: Excessive number connections to a service. 4 164.312.b 8 PBC The PIX is disallowing new connections. 4 164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 ms-exchange: Multiple e-mail attempts to an invalid account. 4 164.312.c.1 5 Registry Integrity Checksum Changed 4 164.312.b 5 Registry Integrity Checksum Changed 4 164.312.b 5 sysiog: Connection blocked by Tcp Wrappers. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple falled logins in a small period of time. 3 164.312.b 10 PAM: Multiple mails logins in a small period of time. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 10	164.312.b	5	Postfix: Sender domain is not found (450: Requested mail action not taken).	4
164.312.b 8 PDK: The PIX is disallowing new connections. 4 164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 ms-exchange: Multiple e-mail attempts to an invalid account. 4 164.312.c.1 5 Registry Integrity Checksum Changed 4 164.312.b 5 Registry Integrity Checksum Changed 4 164.312.b 5 Syslog. Connection blocked by Tcp Wrappers. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 3 PAM: Login session opened. 3 164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 Pox. Multiple failed logins in a small period of time. 3 164.312.b 10 Pox. Multiple failed logins in a small period of time. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8	164.312.b	10	syslog: User missed the password more than one time	4
164.312.b 9 User missed the password to change UID to root. 4 164.312.b 9 ms-exchange: Multiple e-mail attempts to an invalid account. 4 164.312.c.1 5 Registry Integrity Checksum Changed 4 164.312.b 5 Registry Integrity Checksum Changed 4 164.312.b 5 syslog: Connection blocked by Top Wrappers. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 3 PAM: Login session opened. 3 164.312.b 10 Connection to rishd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple failed logins in a small period of time. 3 164.312.b 10 Pix: Multiple attempts of span. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 6 maliscanner: Multiple attempts of spam. 3 164.312.b 6 maliscanner: Multiple attempts of spam. 3 164.312.b 7 System is shutting down. 3 164.312.b 7 System is shutting down. 3 164.312.b 7 System is shutting down. 3 164.312.b 5 Failed	164.312.b	10	xinetd: Excessive number connections to a service.	4
164.312.b 9 mis-exchange: Multiple e-mail attempts to an invalid account. 4 164.312.c.1 5 Registry Integrity Checksum Changed 4 164.312.b 5 Registry Integrity Checksum Changed 4 164.312.b 5 syslog: Connection blocked by Tcp Wrappers. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 3 PAM: Logis session opened. 3 164.312.b 10 Connection to rishd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple falled logins in a small period of time. 3 164.312.b 10 Pix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 5 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b	164.312.b	8	PIX: The PIX is disallowing new connections.	4
164.312.c.1 5 Registry Integrity Checksum Changed 4 164.312.c.2 5 Registry Integrity Checksum Changed 4 164.312.b 5 syslog: Connection blocked by Tcp Wrappers. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple failed logins in a small period of time. 3 164.312.b 10 POSTIX: Multiple attempts to send e-mall from invalid/unknown sender domain. 3 164.312.b 10 Postix: Multiple attempts to send e-mall from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 7 System is shutting down. 3 164.312.b 7 System is shutting down. 3<	164.312.b	9	User missed the password to change UID to root.	4
164.312.c.2 5 Registry Integrity Checksum Changed 4 164.312.b 5 syslog: Connection blocked by Tcp Wrappers. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 3 PAM: Login session opened. 3 164.312.b 10 Connection to rishd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple failed logins in a small period of time. 3 164.312.b 10 PIX: MINIBIPLE ANA (VPN) authentication failures. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 12 Postfix: Multiple attempts of spam. 3 164.312.b 7 System is shutting down. 3 <td>164.312.b</td> <td>9</td> <td>ms-exchange: Multiple e-mail attempts to an invalid account.</td> <td>4</td>	164.312.b	9	ms-exchange: Multiple e-mail attempts to an invalid account.	4
164.312.b 5 syslog: Connection blocked by Tcp Wrappers. 3 164.312.b 3 Courier (imap/pop3) authentication success. 3 164.312.b 3 PAM: Login session opened. 3 164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple failed logins in a small period of time. 3 164.312.b 10 Pix: Multiple AAA (VPN) authentication failures. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 7 System is shutting down. 3 164.312.b 8 Netscreen firewall: configuration changed. 3	164.312.c.1	5	Registry Integrity Checksum Changed	4
164,312.b 3 Courier (imap/pop3) authentication success. 3 164,312.b 3 PAM: Login session opened. 3 164,312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164,312.b 10 PAM: Multiple failed logins in a small period of time. 3 164,312.b 10 PIX: Multiple AAA (VPN) authentication failures. 3 164,312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164,312.b 8 PIX: ARP collision detected. 3 164,312.b 6 mailscanner: Multiple attempts of spam. 3 164,312.b 9 syslog: Illegal root login. 3 164,312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164,312.b 7 System is shutting down. 3 164,312.b 7 System is shutting down. 3 164,312.b 8 Netscreen firewall: configuration changed. 3 164,312.b 5 Failed attempt to run sudo. 2 <t< td=""><td>164.312.c.2</td><td>5</td><td>Registry Integrity Checksum Changed</td><td>4</td></t<>	164.312.c.2	5	Registry Integrity Checksum Changed	4
164.312.b 3 PAM: Login session opened. 3 164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple failed logins in a small period of time. 3 164.312.b 10 PDX: Multiple AAA (VPN) authentication failures. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 6 mailscanner: Multiple attempts of spam. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 7 System is shutting down. 3 164.312.b 7 System is shutting down. 3 164.312.b 5 Failed attempt to run sudo. 2 164.312.b 5 Failed attempt to run sudo. 2 164.312.b 5 Postfix: Recipient address must contain FQDN (504: Command parameter not implemented). 2 164.312.b 5 Postfix: Recipient address must	164.312.b	5	syslog: Connection blocked by Tcp Wrappers.	3
164.312.b 10 Connection to rshd from unprivileged port. Possible network scan. 3 164.312.b 10 PAM: Multiple failed logins in a small period of time. 3 164.312.b 10 PDIX: Multiple alled logins in a small period of time. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 6 mailscanner: Multiple attempts of spam. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 7 System is shutting down. 3 164.312.a.1 8 Netscreen firewall: configuration changed. 3 164.312.b. 5 Failed attempt to run sudo. 2 164.312.b. 5 Postfix: Recipient address must contain FQDN (504: Command parameter not implemented). 2 164.312.b 5 Postfix: Recipient address must contain FQDN (504: Command parameter not implemented). 2 164.312.b 10 Imapd Multiple failed logins from same source ip. <td< td=""><td>164.312.b</td><td>3</td><td>Courier (imap/pop3) authentication success.</td><td>3</td></td<>	164.312.b	3	Courier (imap/pop3) authentication success.	3
164.312.b 10 PAM: Multiple failed logins in a small period of time. 3 164.312.b 10 PIX: Multiple AAA (VPN) authentication failures. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 6 mailscanner: Multiple attempts of spam. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 7 System is shutting down. 3 164.312.a.1 8 Netscreen firewall: configuration changed. 3 164.312.b. 5 Failed attempt to run sudo. 2 164.312.b. 5 Postfix: Recipient address must contain FQDN (504: Command parameter not implemented). 2 164.312.b. 5 Postfix: Recipient address must contain FQDN (504: Command parameter not implemented). 2 164.312.b. 5 Unauthorized user attempted to use sudo. 2 164.312.b. 6 Postfix: Successful login. 2 164.312.b.	164.312.b	3	PAM: Login session opened.	3
164.312.b 10 PIX: Multiple AAA (VPN) authentication failures. 3 164.312.b 10 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 3 164.312.b 8 PIX: ARP collision detected. 3 164.312.b 6 mailscanner: Multiple attempts of spam. 3 164.312.b 9 syslog: Illegal root login. 3 164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 7 System is shutting down. 3 164.312.a.1 8 Netscreen firewall: configuration changed. 3 164.312.b. 5 Failed attempt to run sudo. 2 164.312.b. 5 Postfix: Recipient address must contain FQDN (504: Command parameter not implemented). 2 164.312.b. 5 Unauthorized user attempted to use sudo. 2 164.312.b. 5 Unauthorized user attempted to use sudo. 2 164.312.b. 10 Imapd Multiple failed logins from same source ip. 2 164.312.b. 8 PIX: User created or modified on the Firewall. 2 164.312.b. 6 Pos	164.312.b	10	Connection to rshd from unprivileged port. Possible network scan.	3
164.312.b10Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.3164.312.b8PIX: ARP collision detected.3164.312.b6mailscanner: Multiple attempts of spam.3164.312.b9syslog: Illegal root login.3164.312.b12Postfix: Multiple misuse of SMTP service (bad sequence of commands).3164.312.b7System is shutting down.3164.312.a.18Netscreen firewall: configuration changed.3164.312.b5Failed attempt to run sudo.2164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: BlL lookup error: Host or domain name not found2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a2PIX: User created or modified on the Firewall.	164.312.b	10	PAM: Multiple failed logins in a small period of time.	3
164.312.b8PIX: ARP collision detected.3164.312.b6mailscanner: Multiple attempts of spam.3164.312.b9syslog: Illegal root login.3164.312.b12Postfix: Multiple misuse of SMTP service (bad sequence of commands).3164.312.b7System is shutting down.3164.312.a.18Netscreen firewall: configuration changed.3164.312.b5Failed attempt to run sudo.2164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a12System running out of memory. Availability of the system is in risk.2164.312.a12System running out of memory. Availability of the system is in risk.2	164.312.b	10	PIX: Multiple AAA (VPN) authentication failures.	3
164.312.b6mailscanner: Multiple attempts of spam.3164.312.b9syslog: Illegal root login.3164.312.b12Postfix: Multiple misuse of SMTP service (bad sequence of commands).3164.312.b7System is shutting down.3164.312.a.18Netscreen firewall: configuration changed.3164.312.b5Failed attempt to run sudo.2164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	10	Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.	3
164.312.b9syslog: Illegal root login.3164.312.b12Postfix: Multiple misuse of SMTP service (bad sequence of commands).3164.312.b7System is shutting down.3164.312.a.18Netscreen firewall: configuration changed.3164.312.b5Failed attempt to run sudo.2164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	8	PIX: ARP collision detected.	3
164.312.b 12 Postfix: Multiple misuse of SMTP service (bad sequence of commands). 3 164.312.b 7 System is shutting down. 3 164.312.a.1 8 Netscreen firewall: configuration changed. 3 164.312.b 5 Failed attempt to run sudo. 2 164.312.b 5 Postfix: Recipient address must contain FQDN (504: Command parameter not implemented). 2 164.312.b 5 Unauthorized user attempted to use sudo. 2 164.312.b 3 PIX: Successful login. 2 164.312.b 10 Imapd Multiple failed logins from same source ip. 2 164.312.b 8 PIX: User created or modified on the Firewall. 2 164.312.b 6 Postfix: Attempt to use mail server as relay (client host rejected). 2 164.312.b 6 Postfix: Illegal address from unknown sender 2 164.312.b 6 Postfix: RBL lookup error: Host or domain name not found 2 164.312.b 6 Postfix: hostname verification failed 2 164.312.b 12 System running out of memory. Availability of the system is in risk. 2 164.312.a.2.l 8 PIX: User created or modified on the Firewall. 2	164.312.b	6	mailscanner: Multiple attempts of spam.	3
164.312.b7System is shutting down.3164.312.a.18Netscreen firewall: configuration changed.3164.312.b5Failed attempt to run sudo.2164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	9	syslog: Illegal root login.	3
164.312.a.18Netscreen firewall: configuration changed.3164.312.b5Failed attempt to run sudo.2164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	12	Postfix: Multiple misuse of SMTP service (bad sequence of commands).	3
164.312.b5Failed attempt to run sudo.2164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	7	System is shutting down.	3
164.312.b5Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).2164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.a.1	8	Netscreen firewall: configuration changed.	3
164.312.b5Unauthorized user attempted to use sudo.2164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	5	Failed attempt to run sudo.	2
164.312.b3PIX: Successful login.2164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	5	Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).	2
164.312.b10Imapd Multiple failed logins from same source ip.2164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	5	Unauthorized user attempted to use sudo.	2
164.312.b8PIX: User created or modified on the Firewall.2164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	3	PIX: Successful login.	2
164.312.b6Postfix: Attempt to use mail server as relay (client host rejected).2164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	10	Imapd Multiple failed logins from same source ip.	2
164.312.b6Postfix: Illegal address from unknown sender2164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	8	PIX: User created or modified on the Firewall.	2
164.312.b6Postfix: RBL lookup error: Host or domain name not found2164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	6	Postfix: Attempt to use mail server as relay (client host rejected).	2
164.312.b6Postfix: hostname verification failed2164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	6		2
164.312.b12System running out of memory. Availability of the system is in risk.2164.312.a.2.l8PIX: User created or modified on the Firewall.2	164.312.b	6	Postfix: RBL lookup error: Host or domain name not found	2
164.312.a.2.l 8 PIX: User created or modified on the Firewall. 2	164.312.b	6	Postfix: hostname verification failed	2
164.312.a.2.l 8 PIX: User created or modified on the Firewall. 2	164.312.b	12	System running out of memory. Availability of the system is in risk.	2
164.312.a.2.II 8 PIX: User created or modified on the Firewall. 2	164.312.a.2.l	8	PIX: User created or modified on the Firewall.	2
	164.312.a.2.II	8	PIX: User created or modified on the Firewall.	2



Requirement	Level	Description	Count
164.312.b	5	Postfix: Improper use of SMTP command pipelining (503: Bad sequence of commands).	1
164.312.b	3	Successful sudo to ROOT executed.	1
164.312.b	10	Postfix: Multiple SASL authentication failures.	1
164.312.b	10	Postfix: Multiple attempts to send e-mail to invalid recipient or from unknown sender domain.	1
164.312.b	10	Three failed attempts to run sudo	1
164.312.b	8	PIX: AAA (VPN) user locked out.	1