

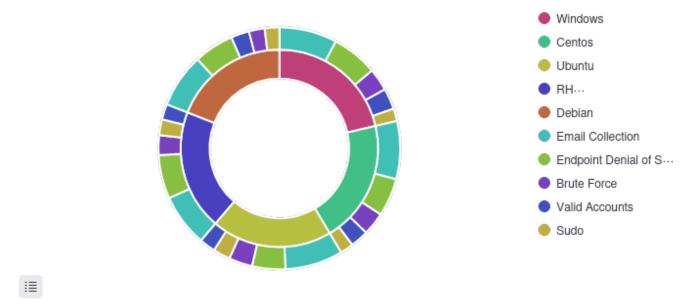
MITRE ATT&CK report

Security events from the knowledge base of adversary tactics and techniques based on realworld observations

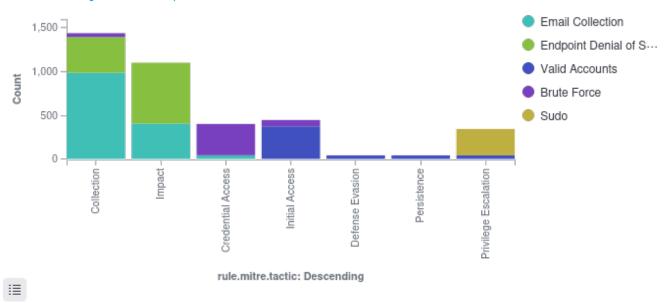
② 2021-09-24T02:58:53 to 2023-09-24T02:58:53

Q manager.name: thm-wazuh AND rule.mitre.id: *

Mitre techniques by agent



Attacks by technique

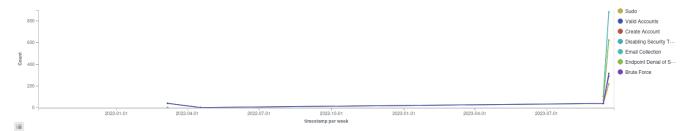




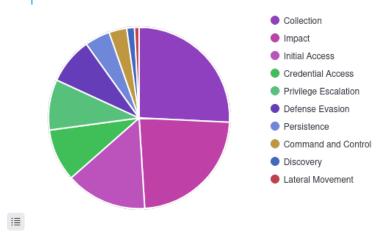
Top tactics by agent



Mitre alerts evolution



Top tactics





Alerts summary

3330 Postfix process error. 10 47 3751 maliscanner: Mutible attempts of spam. 6 44 4607 Imapd user login. 3 43 4507 Netscreen firewall: Sucressfull admin login 8 43 5501 PAM: Login session opened. 3 43 3156 sendmail: Mutible rejected emails from same source ip. 10 40 5132 Unsigned kernel morbide was loaded 11 40 5436 PIX Mutible AVA (VPN) authentication follures 10 40 5407 Successful suids to ROOT executed. 3 40 5408 PIX AVA (VPN) authentication successful. 3 40 5409 Successful suids to ROOT executed. 3 40 5400 Successful suids to ROOT executed. 3 40 5400 Successful suids to ROOT executed. 3 3 5415 Burstick Root Requirement of the note than one time 10 39 542 Burstick Root Root Root Root Root Root Root Roo	Rule ID	Description	Level	Count
3602 Imapd user login. 3 43 4507 Netscreen firewall Successful admin login 8 43 5601 PAM-1 login session opened. 3 43 3156 sendmali: Multiple rejected e-mails from same source ip. 10 40 4386 PX: Multiple AAA (VPN) authentication failures. 10 40 5132 Unsigned kernel module was loaded 11 40 5402 Successful sudo to ROOT executed. 3 40 5402 Syslog: User missed the password more than one time 10 39 3151 sendmali: Sender domain has bogus MX record. It should not be sending e-mail. 10 38 4335 PX: AAA (VPN) authentication successful. 3 38 553 File deleted. 7 38 3851 ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmali: Attempt to use mail server as relay (S5D. Requested action not taken). 6 36 3852 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35	3330	Postfix process error.	10	47
ASSOCIATION AND CONTROL ASSOCIATION	3751	mailscanner: Multiple attempts of spam.	6	44
5501 PAM. Login session opened. 3 43 3156 sendmall: Multiple rejected e-mals from same source ip. 10 40 4386 PX: Multiple AAA (VPN) authentication failures. 10 40 5132 Unsigned kernel module was loaded 11 40 5402 Successful sudo to ROOT executed. 3 40 2502 syslog: User missed the password more than one time 10 39 3151 sendmall: Sender domain has bogus MX record. It should not be sending e-mail. 10 38 4335 PIX: AM (VPN) authentication successful. 3 38 553 File deleted. 7 38 3851 mesexhange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmall: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4500 Netscreen firewall: Successful admin login 8 35 3302 User missed the password to change UID to root. 9 35 <td>3602</td> <td>Imapd user login.</td> <td>3</td> <td>43</td>	3602	Imapd user login.	3	43
3156 Sendmail: Multiple rejected e-mails from same source ip. 10 40	4507	Netscreen firewall: Successfull admin login	8	43
4386 PK: Mutbjele AAA (VPN) authentication failures. 10 40 5132 Unsigned kernel module was loaded 11 40 5402 Successful sudo to ROOT executed. 3 40 2502 syslogy User missed the password more than one time 10 39 3151 sendmail: sender domain has bogus MX record. It should not be sending e-mail. 10 38 4335 PIX: AAA (VPN) authentication successful. 3 38 553 File deleted. 7 38 3851 ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmail: Attempt to use mail server as relay (550. Requested action not taken). 6 36 3332 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Subject prequerings rejects. 10 34	5501	PAM: Login session opened.	3	43
5132 Unsigned kernel module was loaded 11 40 5402 Successful sudo to ROOT executed. 3 40 2502 syslog: User missed the password more than one time 10 39 3151 sendmail: Sender domain has bogus MX record. It should not be sending e-mail. 10 38 3151 sendmail: Sender domain has bogus MX record. It should not be sending e-mail. 10 38 3352 PIX: AAA (VPN) authentication successful. 7 38 3851 ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmail: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Multiple pre greetings rejects. 10 34 3206 Postfix: RBL lookup error: Host or do	3156	sendmail: Multiple rejected e-mails from same source ip.	10	40
5402 Successful sudo to ROOT executed. 3 40 2502 syslog: User missed the password more than one time 10 39 3151 sendmail: Sender domain has bogus MX record. It should not be sending e-mail. 10 38 4335 PIX. AMA (VPN) authentication successful. 3 38 553 File deleted. 7 38 3851 ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmail: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successful admin login 8 35 5002 User missed the password to change UID to root. 9 35 961 User added to group sudo. 5 34 3158 sendmail: Multiple pre-greetings rejects. 10 34 3369 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3379 Postfix: RBL lookup error: Host or domain name not found 6	4386	PIX: Multiple AAA (VPN) authentication failures.	10	40
2502 syslog: User missed the password more than one time 10 39 3151 sendmall: Sender domain has bogus MX record. It should not be sending e-mail. 10 38 4335 PIX: AAA (VPN) authentication successful. 3 38 553 File deleted. 7 38 3851 ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmall: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmall: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3307 Postfix: RBL lookup error: Host or domain name not found 6 34 3307 Postfix: RBL lookup error: Host or domain name not found </td <td>5132</td> <td>Unsigned kernel module was loaded</td> <td>11</td> <td>40</td>	5132	Unsigned kernel module was loaded	11	40
3151 sendmall: Sender domain has bogus MX record. It should not be sending e-mail. 10 38 4335 PIX: AAA (VPN) authentication successful. 3 38 553 File deleted. 7 38 3851 ms-exchanger: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmall: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Hosts or domain name not found 6 34 3852 ms-exchange: Multiple email 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins).	5402	Successful sudo to ROOT executed.	3	40
4335 PIX: AAA (VPN) authentication successful. 3 38 553 File deleted. 7 38 3851 ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmail: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Host or domain name not found 6 34 3852 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins). 10 34 4851 Sonickvall: Multiple invalle error messages. 10 34	2502	syslog: User missed the password more than one time	10	39
553 File deleted. 7 38 3851 ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmail: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Multiple per-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Host or domain name not found 6 34 3852 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins). 10 34 4851 Sonic-Wall: Multiple memall 500 error code (spam). 9 34 505 Ossec agent removed. 3 34	3151	sendmail: Sender domain has bogus MX record. It should not be sending e-mail.	10	38
ms-exchange: Multiple e-mail attempts to an invalid account. 9 37 3104 sendmail: Attempt to use mail server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Host or domain name not found 6 34 3892 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 5 33 335 Postfix: too many errors after RCPT from unknown 6 33 337 338 Postfix: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 335 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4329 PIX: Firewall configuration deleted.	4335	PIX: AAA (VPN) authentication successful.	3	38
3104 sendmall: Attempt to use mall server as relay (550: Requested action not taken). 6 36 3352 Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 6 35 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmall: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: IR Llookup error: Host or domain name not found 6 34 3852 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins). 10 34 4851 SonicWall: Multiple irrewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Sender domain is not found (553: Requested action not taken).	553	File deleted.	7	38
Postfix: Multiple attempts to send e-mail from a rejected sender IP (access). 4506 Netscreen firewall: Successfull admin login 8 35 5302 User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Host or domain name not found 6 34 3852 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins). 10 34 4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 5 33 333 Postfix: too many errors after RCPT from unknown 6 33 334 337 PIX: The PIX is disallowing new connections. 8 33 3433 PIX: The PIX is disallowing new connections. 8 33 390 Sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3439 PIX: The PIX is fixed by access and the properties of the propert	3851	ms-exchange: Multiple e-mail attempts to an invalid account.	9	37
4506Netscreen firewall: Successfull admin login8355302User missed the password to change UID to root.9352961User added to group sudo.5343158sendmail: Multiple pre-greetings rejects.10343306Postfix: IP Address black-listed by anti-spam (blocked).6343397Postfix: RBL lookup error: Host or domain name not found6343852ms-exchange: Multiple e-mail 500 error code (spam).9343910Courier brute force (multiple failed logins).10344851SonicWall: Multiple firewall error messages.1034505Ossec agent removed.3342301xinetd: Excessive number connections to a service.10333103sendmail: Rejected by access list (55x: Requested action not taken).6333105sendmail: Sender domain is not found (553: Requested action not taken).5333335Postfix: too many errors after RCPT from unknown6334337PIX: The PIX is disallowing new connections.833592Log file size reduced.8333303Postfix: Sender domain is not found (450: Requested mail action not taken).5323303Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.10324325PIX: ARP collision detected.8324339PIX: Firewall configuration deleted.832	3104	sendmail: Attempt to use mail server as relay (550: Requested action not taken).	6	36
User missed the password to change UID to root. 9 35 2961 User added to group sudo. 5 34 3158 sendmail: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Host or domain name not found 6 34 3852 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins). 10 34 4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 6 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 425 PIX: ARP collision detected. 8 32	3352	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	6	35
2961 User added to group sudo. 5 34 3158 sendmail: Multiple pre-greetings rejects. 10 34 3306 Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Host or domain name not found 6 34 3852 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins). 10 34 4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 6 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 592 Log file size reduced. 8 33 393 Postfix: Sender domain is not found (450: Requested mail action not taken). 5<	4506	Netscreen firewall: Successfull admin login	8	35
3158 sendmail: Multiple pre-greetings rejects. 3206 Postfix: IP Address black-listed by anti-spam (blocked). 3307 Postfix: RBL lookup error: Host or domain name not found 3852 ms-exchange: Multiple e-mail 500 error code (spam). 3910 Courier brute force (multiple failed logins). 4851 SonicWall: Multiple firewall error messages. 100 34 4855 Ossec agent removed. 3010 Seendmail: Rejected by access list (55x: Requested action not taken). 3010 sendmail: Sender domain is not found (553: Requested action not taken). 3010 sendmail: Sender domain is not found (553: Requested action not taken). 3010 sendmail: Sender domain is not found (553: Requested action not taken). 3010 sendmail: Sender domain is not found (553: Requested action not taken). 3010 sendmail: Sender domain is not found (553: Requested action not taken). 3010 sendmail: Sender domain is not found (553: Requested action not taken). 3010 sendmail: Sender domain is not found (553: Requested action not taken). 3010 sendmail: Sender domain is not found (450: Requested action not taken). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3010 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).	5302	User missed the password to change UID to root.	9	35
Postfix: IP Address black-listed by anti-spam (blocked). 6 34 3397 Postfix: RBL lookup error: Host or domain name not found 6 34 3852 ms-exchange: Multiple e-mail 500 error code (spam). 9 34 3910 Courier brute force (multiple failed logins). 10 34 4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 6 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 5 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32	2961	User added to group sudo.	5	34
Postfix: RBL lookup error: Host or domain name not found 3852 ms-exchange: Multiple e-mail 500 error code (spam). 3910 Courier brute force (multiple failed logins). 4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 5 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3303 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	3158	sendmail: Multiple pre-greetings rejects.	10	34
ms-exchange: Multiple e-mail 500 error code (spam). 3910 Courier brute force (multiple failed logins). 10 34 4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 6 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	3306	Postfix: IP Address black-listed by anti-spam (blocked).	6	34
3910Courier brute force (multiple failed logins).10344851SonicWall: Multiple firewall error messages.1034505Ossec agent removed.3342301xinetd: Excessive number connections to a service.10333103sendmail: Rejected by access list (55x: Requested action not taken).6333105sendmail: Sender domain is not found (553: Requested action not taken).5333335Postfix: too many errors after RCPT from unknown6334337PIX: The PIX is disallowing new connections.8335703sshd: Possible breakin attempt (high number of reverse lookup errors).1033592Log file size reduced.8333191sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).6323303Postfix: Sender domain is not found (450: Requested mail action not taken).5323353Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.10324325PIX: ARP collision detected.8324339PIX: Firewall configuration deleted.832	3397	Postfix: RBL lookup error: Host or domain name not found	6	34
4851 SonicWall: Multiple firewall error messages. 10 34 505 Ossec agent removed. 3 34 2301 xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 6 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted.	3852	ms-exchange: Multiple e-mail 500 error code (spam).	9	34
505Ossec agent removed.3342301xinetd: Excessive number connections to a service.10333103sendmail: Rejected by access list (55x: Requested action not taken).6333105sendmail: Sender domain is not found (553: Requested action not taken).5333335Postfix: too many errors after RCPT from unknown6334337PIX: The PIX is disallowing new connections.8335703sshd: Possible breakin attempt (high number of reverse lookup errors).1033592Log file size reduced.8333191sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).6323303Postfix: Sender domain is not found (450: Requested mail action not taken).5323353Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.10324325PIX: ARP collision detected.8324339PIX: Firewall configuration deleted.832	3910	Courier brute force (multiple failed logins).	10	34
xinetd: Excessive number connections to a service. 10 33 3103 sendmail: Rejected by access list (55x: Requested action not taken). 6 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	4851	SonicWall: Multiple firewall error messages.	10	34
sendmail: Rejected by access list (55x: Requested action not taken). 5 33 3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	505	Ossec agent removed.	3	34
3105 sendmail: Sender domain is not found (553: Requested action not taken). 5 33 3335 Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	2301	xinetd: Excessive number connections to a service.	10	33
Postfix: too many errors after RCPT from unknown 6 33 4337 PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	3103	sendmail: Rejected by access list (55x: Requested action not taken).	6	33
PIX: The PIX is disallowing new connections. 8 33 5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	3105	sendmail: Sender domain is not found (553: Requested action not taken).	5	33
5703 sshd: Possible breakin attempt (high number of reverse lookup errors). 10 33 592 Log file size reduced. 8 33 3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	3335	Postfix: too many errors after RCPT from unknown	6	33
592Log file size reduced.8333191sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).6323303Postfix: Sender domain is not found (450: Requested mail action not taken).5323353Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.10324325PIX: ARP collision detected.8324339PIX: Firewall configuration deleted.832	4337	PIX: The PIX is disallowing new connections.	8	33
3191 sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED). 6 32 3303 Postfix: Sender domain is not found (450: Requested mail action not taken). 5 32 3353 Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	5703	sshd: Possible breakin attempt (high number of reverse lookup errors).	10	33
3303Postfix: Sender domain is not found (450: Requested mail action not taken).5323353Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.10324325PIX: ARP collision detected.8324339PIX: Firewall configuration deleted.832	592	Log file size reduced.	8	33
Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain. 10 32 4325 PIX: ARP collision detected. 8 32 4339 PIX: Firewall configuration deleted. 8 32	3191	sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).	6	32
4325PIX: ARP collision detected.8324339PIX: Firewall configuration deleted.832	3303	Postfix: Sender domain is not found (450: Requested mail action not taken).	5	32
4339 PIX: Firewall configuration deleted. 8 32	3353	Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.	10	32
	4325	PIX: ARP collision detected.	8	32
5404 Three failed attempts to run sudo 10 32	4339	PIX: Firewall configuration deleted.	8	32
	5404	Three failed attempts to run sudo	10	32



Rule ID	Description	Level	Count
5405	Unauthorized user attempted to use sudo.	5	32
5601	telnetd: Connection refused by TCP Wrappers.	5	32
5705	sshd: Possible scan or breakin attempt (high number of login timeouts).	10	32
5706	sshd: insecure connection attempt (scan).	6	32
3304	Postfix: Improper use of SMTP command pipelining (503: Bad sequence of commands).	5	31
3351	Postfix: Multiple relaying attempts of spam.	6	31
4323	PIX: Successful login.	3	31
4509	Netscreen firewall: configuration changed.	8	31
518	Windows Adware/Spyware application found.	9	31
5631	telnetd: Multiple connection attempts from same source (possible scan).	10	31
593	Microsoft Event log cleared.	9	31