OpenSearch Dashboards Reports

Search

28 Sep, 2025 @ 21:51:54.90 → 29 Sep, 2025 @ 22:00:00.00

Total Successful Login Events

236
Successful Login Events

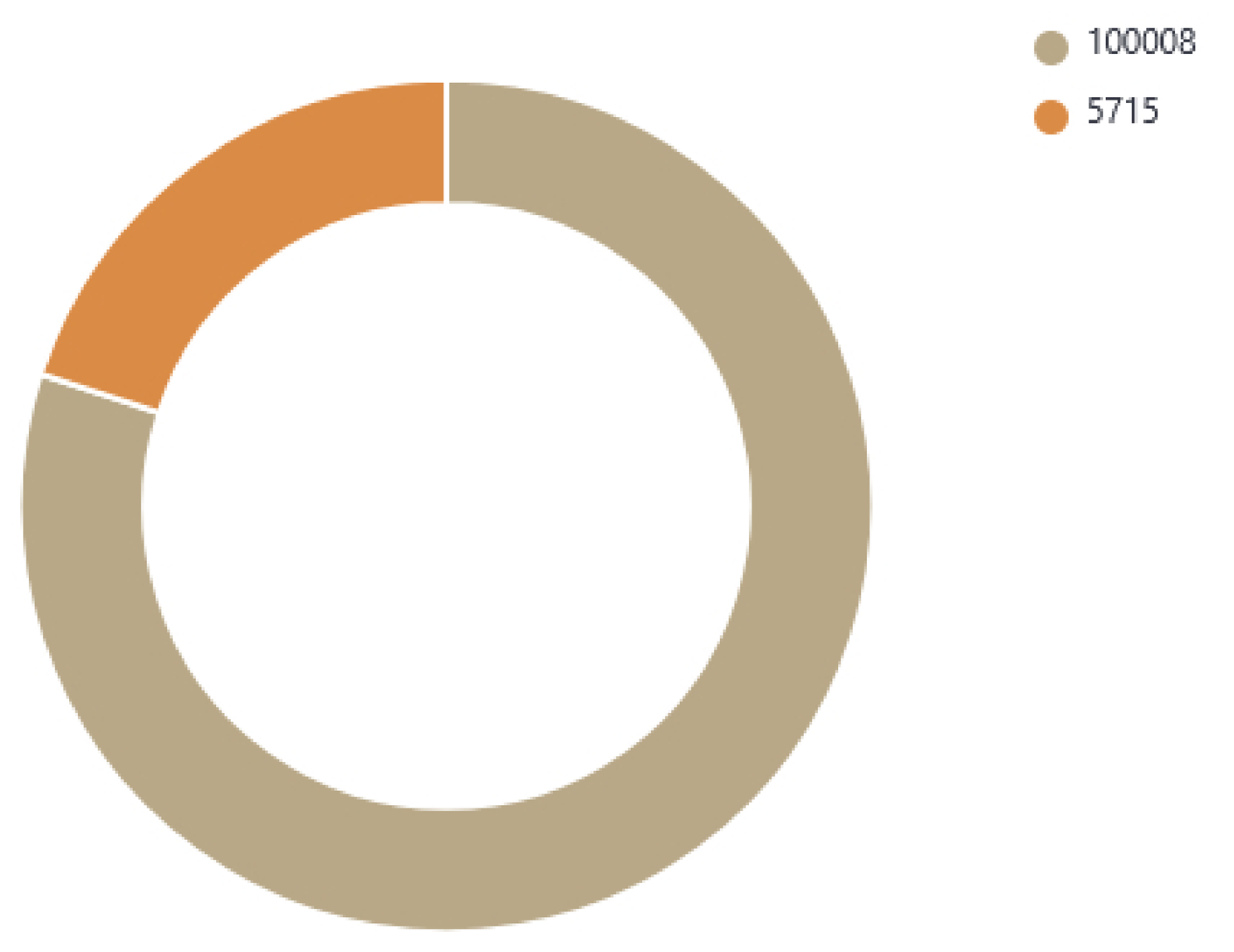
Total Failed Login Events

1,499
Failed Login Events

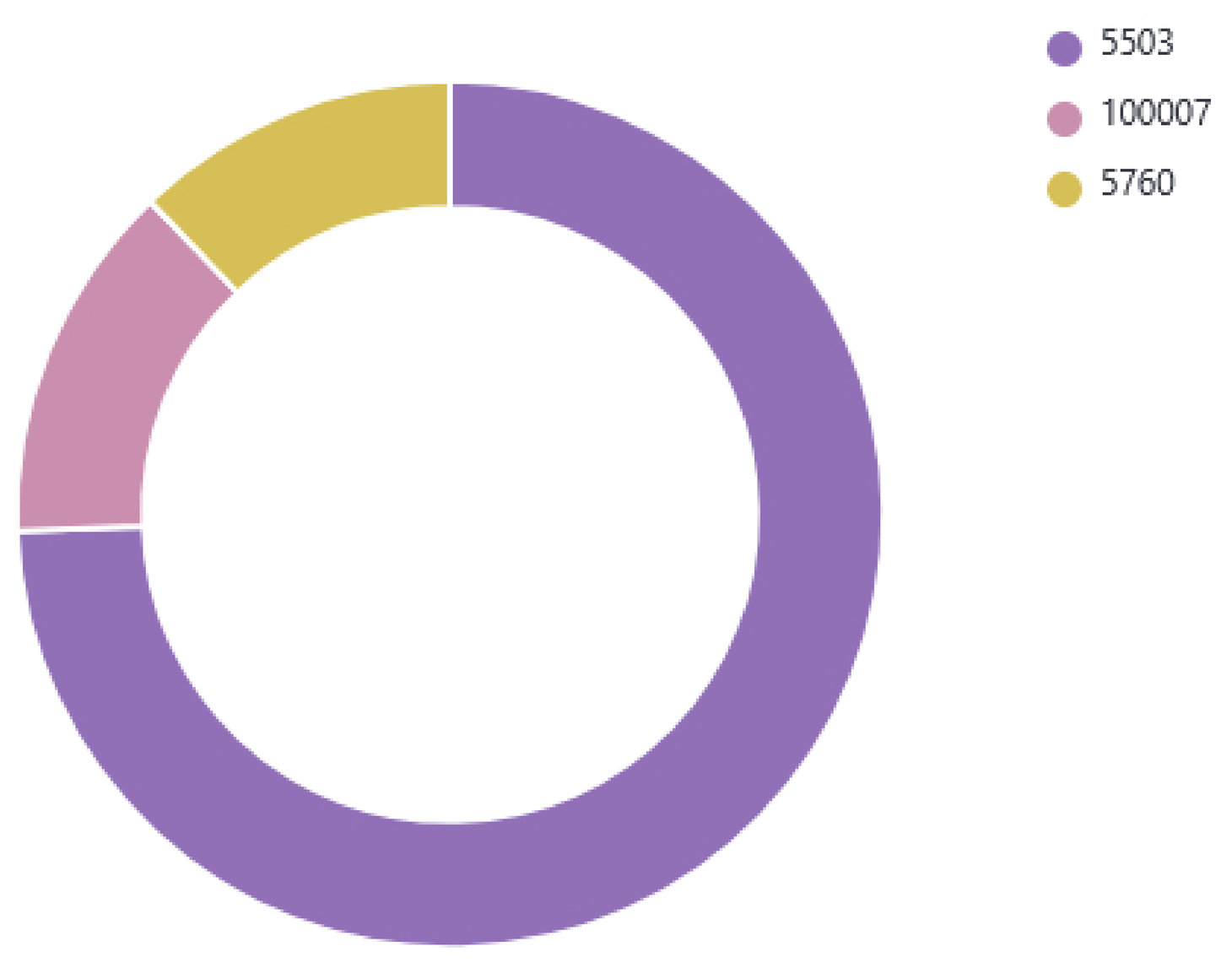
Total Suspicious Login Events

1,040
Suspicious Login Events

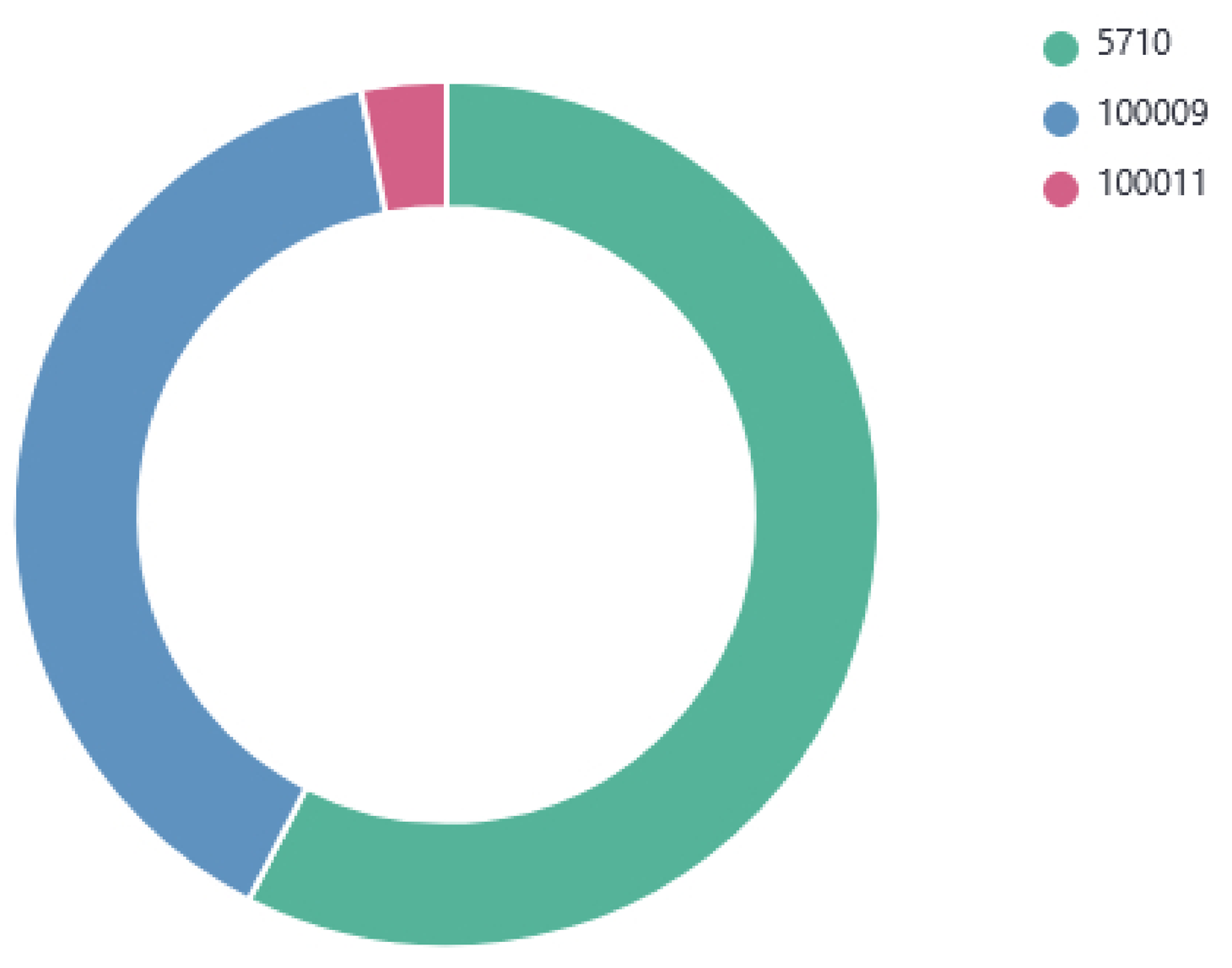
Successful Logins Chart by Rule ID



Failed Logins Chart by Rule ID



Suspicious Logins Chart by Rule ID



Linux Events

Linux Events

Windows Events

Windows Events

Successful Logins - Linux

Rule ID	Rule Description	Agent	User (Source)	User (Dest.)
5715	sshd: authentication success.	wazuh01	N/A	[redacted]
100008	Linux: Successful SSH login detected for [redacted] from	wazuh01	[redacted]	root(uid=0)
100008	Linux: Successful SSH login detected for [redacted] from	wazuh01	[redacted]	[redacted](uid=1000)
100008	Linux: Successful SSH login detected for [redacted] from	wazuh01	[redacted]	root(uid=0)

Successful Logins - Windows

Rule ID	Rule Description	Agent	User (Source)	User (Dest.)
60106	Windows Logon Success	wazuh03	N/A	N/A

Failed Logins - Linux

Rule ID	Rule Description	Agent	User (So...	User (De...
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root
5760	sshd: authentication failed.	wazuh04	N/A	root

Failed Logins - Windows

Rule ID	Rule Description	Agent	User (So...	IP	User (I
60122	Logon Failure - Unknown user or bad password	wazuh03	N/A	N/A	N/A
100013	Windows: Failed login attempt from user [redacted] on wazuh(	wazuh03	N/A	N/A	N/A
100013	Windows: Failed login attempt from user Test on wazuh03	wazuh03	N/A	N/A	N/A
100013	Windows: Failed login attempt from user NOUSER on wazuh(	wazuh03	N/A	N/A	N/A
100013	Windows: Failed login attempt from user Administrator on w	wazuh03	N/A	N/A	N/A

Suspicious Login Attempts - Linux

Rule ID	Rule Description	Agent	User	Use
5710	sshd: Attempt to login using a non-existent user	wazuh04	worker	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	webserver	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	webserver	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	webserver	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	webdev	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	webdev	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	webdev	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	webdev	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	vncuser	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	vinay	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	vastbase	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	userroot	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	userroot	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	user_01	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	user1	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	user01	N/
5710	sshd: Attempt to login using a non-existent user	wazuh04	user01	N/

2 3 4 5 >

Suspicious Login Attempts - Windows

Rule ID	Rule Description	Agent	User	User (...	IP
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A
100011	Windows Firewall: Blocked inbound SSH (port 22) from (	wazuh03	N/A	N/A	N/A

Reference List of Rules - Linux

Reference List of Rules

Linux

Successful

Rule ID	Rule Description
5501	PAM: Login session opened.
5715	sshd: authentication success.
100008	Linux: Successful SSH login detected for srcuser from srcip

Failed

Rule ID	Rule Description
5716	sshd: authentication failed.
5733	sshd: User entered incorrect password.
5741	sshd: connection refused
5760	sshd: authentication failed.
100007	Linux: Failed SSH login attempt for dstuser from srcip

Suspicious

Rule ID	Rule Description
5504	PAM: Attempt to login with an invalid user.
5710	sshd: Attempt to login using a non-existent user
5711	sshd: Useless/Duplicated SSHD message without a user/ip.
5718	sshd: Attempt to login using a denied user.
5723	sshd: key error.
5724	sshd: key error.
5726	sshd: Unknown PAM module, PAM misconfiguration.
5753	sshd: could not negotiate with client, no matching cipher.
5755	sshd: Authentication refused due to owner/permissions of authorized_keys.
5758	Maximum authentication attempts exceeded.
100009	SSH login attempt for invalid user "user" from "ip"

Reference List of Rules - Windows

Reference List of Rules

Windows

Successful

Rule ID	Rule Description
60106	Windows Logon Success
60118	Windows Workstation Logon Success

Failed

Rule ID	Rule Description
60105	Windows Logon Failure
60122	Logon Failure - Unknown user or bad password
60128	Logon Failure - Account's password expired
60130	Logon Failure - Account locked out
60131	Windows DC Logon Failure

Suspicious

Rule ID	Rule Description
10007	Windows Firewall blocked SSH connection attempt
60115	Windows: User account locked out (multiple login errors).
60204	Multiple Windows Logon Failures
100011	Windows Firewall: Blocked inbound SSH (port 22) from (win.eventdata.sourceAddress) on (win.system.computer)