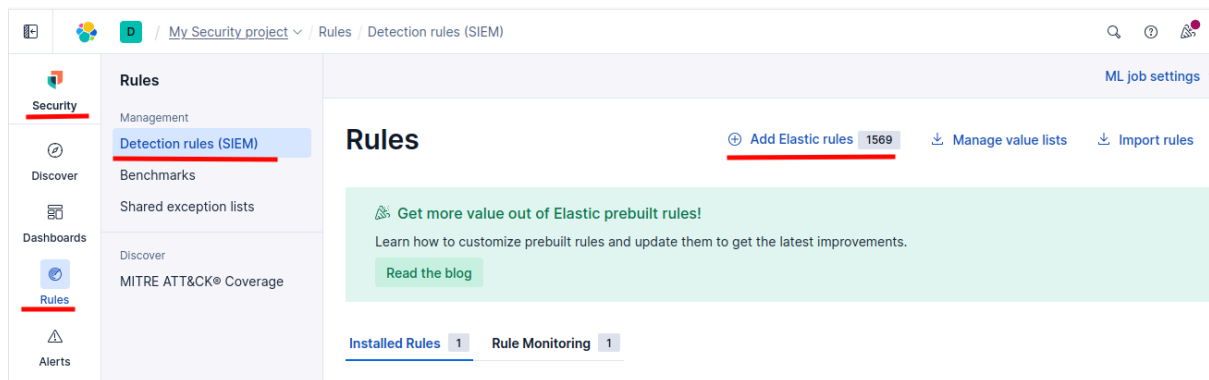


In this lab we have to continue to enhance its Security Information and Event Management (SIEM) capabilities, your team has been tasked with enabling, testing, and analyzing security alerts within Elastic SIEM using the MITRE ATT&CK framework.

In this part we have to enable security rules in elastic SIEM.



Here, we are seeing the elastic cloud, so, we have to go into security, rules, detection rules(SIEM) and add elastic rules, because we need to add two new rules.

Potential Network Scan Detected

×

[Overview](#) [Investigation guide](#)

▼ About

This rule identifies a potential port scan. A port scan is a method utilized by attackers to systematically scan a target system or network for open ports, allowing them to identify available services and potential vulnerabilities. By mapping out the open ports, attackers can gather critical information to plan and execute targeted attacks, gaining unauthorized access, compromising security, and potentially leading to data breaches, unauthorized control, or further exploitation of the targeted system or network. This rule defines a threshold-based approach to detect connection attempts from a single source to a wide range of destination ports.

Author	Elastic
Severity	● Low
Risk score	21
License	Elastic License v2
MITRE ATT&CK™	Discovery (TA0007) ↗ <ul style="list-style-type: none">Network Service Discovery (T1046) Reconnaissance (TA0043) ↗<ul style="list-style-type: none">Active Scanning (T1595)Scanning IP Blocks (T1595.001)

Timestamp override event.ingested

Max alerts per run 5

Tags Domain: Network Tactic: Discovery Tactic: Reconnaissance Use Case: Network Security Monitoring

[Dismiss](#)

[Install without enabling](#)

[Install and enable](#)

That's the first rule that we need to install.

Multiple Logon Failure from the same Source Address

×

[Overview](#) [Investigation guide](#)

▼ About

Identifies multiple consecutive logon failures from the same source address and within a short time interval. Adversaries will often brute force login attempts across multiple users with a common or known password, in an attempt to gain access to accounts.

Author	Elastic
Severity	● Medium
Risk score	47
Reference URLs	<ul style="list-style-type: none">https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625 ↗https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624 ↗https://social.technet.microsoft.com/Forums/ie/en-US/c82ac4f3-a235-472c-9fd3-53aa646cfcfd/network-information-missing-in-event-id-4624?forum=winserversecurity ↗https://serverfault.com/questions/379092/remote-desktop-failed-logon-event-4625-not-logging-ip-address-on-2008-terminal-s/403638#403638 ↗
License	Elastic License v2
MITRE ATT&CK™	Credential Access (TA0006) ↗ <ul style="list-style-type: none">Brute Force (T1110)Password Guessing (T1110.001)Password Spraying (T1110.003)

Max alerts per run 100

Tags Domain: Endpoint OS: Windows Use Case: Threat Detection Tactic: Credential Access

[Dismiss](#)

[Install without enabling](#)

[Install and enable](#)

And this rule.

Now, let's open the MITRE ATT&CK techniques to confirm if the rules are enabled.

The screenshot displays the 'MITRE ATT&CK Coverage' dashboard. The left sidebar contains a navigation menu with 'Rules' selected. The main content area shows a grid of MITRE ATT&CK techniques. The 'Active Scanning' sub-technique is highlighted, showing a rule named 'Potential Network Scan Detected' is enabled. The dashboard also includes filters for 'Installed rule status' and 'Installed rule type', a search bar, and a legend for rule counts.

Tactic	Sub-technique	Rules	Enabled Rules
Reconnaissance	Active Scanning	1/10 techniques	1
Reconnaissance	Gather Victim Host Information	0/4	0
Reconnaissance	Gather Victim Identity Information	0/3	0
Active Scanning	Potential Network Scan Detected	1	1
Persistence	Account Manipulation	0/23 techniques	0
Persistence	BITS Jobs	0/0	0
Persistence	Boot or Logon Autostart Execution	0/14	0

Here we can check that our rule Potential Network Scan Detected is in reconnaissance tactic, and is inside of Active Scanning techniques, let's check the clothes to see more.

Rules

Management

Detection rules (SIEM)

Benchmarks

Shared exception lists

Discover

MITRE ATT&CK® Coverage

MITRE ATT&CK® coverage

Your current coverage of MITRE ATT&CK® tactics and techniques, based on installed rules. Click a cell to view and enable a technique to the MITRE ATT&CK® framework to be displayed. [Learn more.](#)

Installed rule status 1

Installed rule type 2

Search for the tactic, technique (e.g., "Defense Evasion")

Collapse cells

Expand cells

Legend (count will increase)

>10 rules

1-3 rules

	<div>Defense Evasion</div> <div>0/45 techniques</div> <div>0</div> <div>0</div>	<div>Credential Access</div> <div>1/17 techniques</div> <div>0</div> <div>1</div>	<div>Discovery</div> <div>1/33 techniques</div> <div>0</div> <div>0</div>	<div>Lateral Movement</div> <div>0/9 techniques</div> <div>0</div> <div>0</div>	<div>Collection</div> <div>0/17 techniques</div> <div>0</div> <div>0</div>
<div>Control</div> <div>0/6</div>	<div>Abuse Elevation Control Mechanism</div> <div>Sub-techniques 0/6</div> <div>0</div> <div>0</div>	<div>Adversary-In-the-Middle</div> <div>Sub-techniques 0/4</div> <div>0</div> <div>0</div>			
	<div>Access Token Manipulation</div> <div>Sub-techniques 0/5</div> <div>0</div> <div>0</div>	<div>Brute Force</div> <div>Sub-techniques 2/4</div> <div>0</div> <div>0</div>			
<div>Authentication</div> <div>0/7</div>	<div>BITS Jobs</div> <div>Sub-techniques 0/0</div> <div>0</div> <div>0</div>	<div>Credentials from Password Stores</div> <div>Sub-techniques 0/6</div> <div>0</div> <div>0</div>			

Brute Force

Sub-techniques 2/4

Enabled rules 1

Multiple Logon Failure from the same Source Address

Disabled rules 0

Enable all disabled

Here we can check that our Multiple Logon Failure from the same Source Address is in Credentials access tactic, and inside of brute force techniques.

Rules

Management
Detection rules (SIEM)
Benchmarks
Shared exception lists

Discover

MITRE ATT&CK® Coverage

MITRE ATT&CK® coverage

Your current coverage of MITRE ATT&CK® tactics and techniques, based on installed rules. Click a cell to view and enter to the MITRE ATT&CK® framework to be displayed. [Learn more.](#)

Installed rule status 1

Installed rule type 2

Collapse cells

Expand cells

Legend

>10 ru

1-3 ru

<div>Defense Evasion</div> <div>0/45 techniques</div> <div>Disabled Rules: 0</div> <div>Enabled Rules: 0</div>	<div>Credential Access</div> <div>1/17 techniques</div> <div>Disabled Rules: 0</div> <div>Enabled Rules: 1</div>	<div>Discovery</div> <div>1/33 techniques</div> <div>Disabled Rules: 0</div> <div>Enabled Rules: 1</div>	<div>Lateral Movement</div> <div>0/9 techniques</div> <div>Disabled Rules: 0</div> <div>Enabled Rules: 0</div>
<div>Abuse Elevation Control Mechanism</div> <div>Sub-techniques 0/6</div>	<div>Adversary-in-the-Middle</div> <div>Sub-techniques 0/4</div>	<div>Account Discovery</div> <div>Sub-techniques 0/4</div>	<div>Exploitation of Remote Services</div> <div>Sub-techniques 0/0</div>
<div>Access Token Manipulation</div> <div>Sub-techniques 0/5</div>	<div>Brute Force</div> <div>Sub-techniques 2/4</div>	<div>Application Window Discovery</div> <div>Sub-techniques 0/0</div>	<div>Internal Spearphishing</div> <div>Sub-techniques 0/0</div>
<div>BITS Jobs</div> <div>Sub-techniques 0/0</div>	<div>Credentials from Password Stores</div> <div>Sub-techniques 0/6</div>	<div>Browser Information Discovery</div> <div>Sub-techniques 0/0</div>	<div>Lateral Tool Transfer</div> <div>Sub-techniques 0/0</div>
		<div>Remote Service Session</div>	

0/12

Permissions Modification

Sub-techniques 0/2

0/5

Hide Artifacts

Sub-techniques 0/14

0/4

Hijack Execution Flow

Sub-techniques 0/12

0/11

Impair Defenses

Sub-techniques 0/11

0/0

Impersonation

Sub-techniques 0/0

0/10

Indicator Removal

Sub-techniques 0/10

0/8

Steal Application Access Token

Sub-techniques 0/0

0/0

Steal Web Session Cookie

Sub-techniques 0/0

0/0

Steal or Forge Authentication Certificates

Sub-techniques 0/0

0/5

Steal or Forge Kerberos Tickets

Sub-techniques 0/5

0/0

Unsecured Credentials

0/0

Group Policy Discovery

Sub-techniques 0/0

0/0

Log Enumeration

Sub-techniques 0/0

0/0

Network Service Discovery

Sub-techniques 0/0

0/0

Network Share Discovery

Sub-techniques 0/0

0/0

Network Sniffing

Sub-techniques 0/0

0/0

Password Policy Discovery

Network Service Discovery

Sub-techniques 0/0

Enabled rules 1

Potential Network Scan Detected

Disabled rules 0

Enable all disabled

Here in Discovery tactic we can check that inside of Network Service Discovery, we can find the Potential Network Scan Detected rule enabled also.

Untitled

Data view logs-*

Search field names

Auto Interval No breakdown

event.code : "4625" and user.name : "brandon gracy"

Selected fields 8

- @timestamp
- message
- event.category
- event.action
- host.name
- source.ip
- destination.ip
- user.name

Available fields 313

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- data_stream.dataset
- data_stream.namespace
- data_stream.type
- dataset.name
- dataset.namespace

Documents (5) Patterns Field statistics

@timestamp message event.category event.action

Dec 17, 2025 @ 23:06:00.474

Conta: BRANDON ID de Início de Sessão: 0x88770 Tipo de Início de Sessão: 2 Conta cujo Início de Sessão Falhou: ID de Segurança: S-1-0-0 Nome da Conta: brandon gracy Domínio da Conta: BRANDON

Dec 17, 2025 @ 23:05:56.654

Informações da Falha: Motivo da Falha: Nome de utilizador desconhecido ou palavra-passe incorreta. Estado: 0xC000006D Sub-estado: 0xC0000064

Dec 17, 2025 @ 23:05:54.674

Informações do Processo: ID do Processo Chamador: 0x2ff4 Nome do Processo Chamador: C:\Windows\System32\svchost.exe

Dec 17, 2025 @ 23:05:51.515

Informações da Rede: Nome da Estação de Trabalho: BRANDON Endereço de Rede de Origem: ::1 Porta de Origem: 0

Dec 17, 2025 @ 23:05:48.529

Informações de Autenticação Detalhadas: Processo de Início de Sessão: seclogo Pacote

Here, we can check what the issue is.

Security

Filter your data using KQL syntax

ML Job settings Add Integrations Data view Security solution default

Today < > Refresh

Status Severity User brand Host brandon

Summary Trend Counts Treemap

Severity levels

Levels Count

Medium 2

2 alerts

Alerts by name

Rule name Count

newnew 2

Top alerts by

host.name

brandon 100%

kibana.alert.reason authentication, session event with process svchost.exe, source ::1:0, by brand on brandon created medium alert newnew.

Columns 18 Sort fields 1 2 alerts Fields

Assignees	Severity	Risk Score	Reason	host.name	user.name	Host Risk Level	User
	medium	47	authentication, session event with process svchost.exe, source ::1:0, by br...	brandon	brand	—	—
	medium	47	authentication, session event with process svchost.exe, source ::1:0, by br...	brandon	brand	—	—

Updated 1 minute ago Grid view Additional filters Group alerts by: None

If we go to alerts, we can check the alert about the attempt of login.

