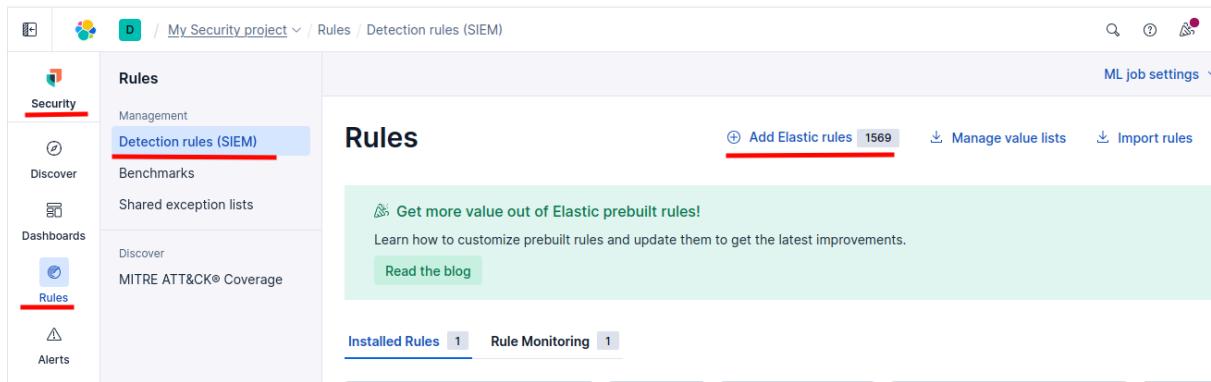


In this lab we have to continues to enhance its Security Information and Event Management (SIEM) capabilities, your team has been tasked with enabling, testing, and analyzing security alerts within Elastic SIEM using the MITRE ATT&CK framework.

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



The screenshot shows the Elastic Cloud interface with the following details:

- Project:** My Security project
- Section:** Rules / Detection rules (SIEM)
- Left Sidebar (Selected):** Rules
- Left Sidebar Options:** Security, Discover, Dashboards, Rules (selected), Alerts
- Main Content:** Rules page with a red box highlighting the "Add Elastic rules" button.
- Buttons on Main Content:** Add Elastic rules (1569), Manage value lists, Import rules
- Callout on Main Content:** Get more value out of Elastic prebuilt rules! (with a "Read the blog" link)
- Bottom Navigation:** Installed Rules (1), Rule Monitoring (1)

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

X

[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™	<a href="#">Discovery (TA0007)</a> ↗ └ <a href="#">Network Service Discovery (T1046)</a>
	<a href="#">Reconnaissance (TA0043)</a> ↗ └ <a href="#">Active Scanning (T1595)</a> └ <a href="#">Scanning IP Blocks (T1595.001)</a>
Timestamp override	event.ingested
Max alerts per run	5
Tags	<a href="#">Domain: Network</a> <a href="#">Tactic: Discovery</a> <a href="#">Tactic: Reconnaissance</a> <a href="#">Use Case: Network Security Monitoring</a>
Dismiss	<a href="#">Install without enabling</a> <a href="#">Install and enable</a>

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

## Multiple Logon Failure from the same Source Address

X

[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"><li><a href="https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625">https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625</a> ↗</li><li><a href="https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624">https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624</a> ↗</li><li><a href="https://social.technet.microsoft.com/Forums/ie/en-US/c82ac4f3-a235-472c-9fd3-53aa646cfcd/network-information-missing-in-event-id-4624?forum=winserversecurity">https://social.technet.microsoft.com/Forums/ie/en-US/c82ac4f3-a235-472c-9fd3-53aa646cfcd/network-information-missing-in-event-id-4624?forum=winserversecurity</a> ↗</li><li><a href="https://serverfault.com/questions/379092/remote-desktop-failed-logon-event-4625-not-logging-ip-address-on-2008-terminal-s/403638#403638">https://serverfault.com/questions/379092/remote-desktop-failed-logon-event-4625-not-logging-ip-address-on-2008-terminal-s/403638#403638</a> ↗</li></ul>
License	Elastic License v2
MITRE ATT&CK™	<a href="#">Credential Access (TA0006)</a> ↗ └ <a href="#">Brute Force (T1110)</a> └ <a href="#">Password Guessing (T1110.001)</a> └ <a href="#">Password Spraying (T1110.003)</a>
Max alerts per run	100
Tags	<a href="#">Domain: Endpoint</a> <a href="#">OS: Windows</a> <a href="#">Use Case: Threat Detection</a> <a href="#">Tactic: Credential Access</a>
Dismiss	<a href="#">Install without enabling</a> <a href="#">Install and enable</a>

And this rule.

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

The screenshot shows a security management interface with a sidebar navigation menu. The menu includes options like Security, Discover, Dashboards, Rules (which is selected), Alerts, Attack discovery, and More. The main content area is titled "MITRE ATT&CK® coverage". It displays a legend indicating rule counts: >10 rules (dark green), 7-10 rules (medium green), 1-3 rules (light green), and 0 rules (yellow). A search bar and filters for "Installed rule status" (1) and "Installed rule type" (2) are present. The main grid shows various technique categories with their sub-techniques and rule counts. A specific row for "Potential Network Scan Detected" under "Active Scanning" is highlighted in red, showing 1 enabled rule. A button labeled "Enable all disabled" is visible at the bottom of this row.

Technique Category	Sub-technique	Enabled Rules	Disabled Rules
Reconnaissance	1/10 techniques	1	0
	Gather Victim Host Information	0/4	0
	Gather Victim Identity Information	0/3	0
	Sub-techniques	1/3	0
Active Scanning	Potential Network Scan Detected	1	0
	Gather Victim Host Information	0/4	0
	Gather Victim Identity Information	0/3	0
	Sub-techniques	1/3	0
Persistence	Establish Persistence	0	0
	Exploit Known Vulnerabilities	0	0
	Impersonate User Accounts	0	0
	Sub-techniques	0/12	0
Privilege Escalation	Compromise Infrastructure	0	0
	External Remote	0	0
	Internal	0	0
	Sub-techniques	0/14	0
Account Manipulation	Change User Logon	0	0
	Change User Logon	0	0
	Change User Logon	0	0
	Sub-techniques	0/7	0
BITS Jobs	BITS Jobs	0	0
	BITS Jobs	0	0
	BITS Jobs	0	0
	Sub-techniques	0/0	0
Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	0	0
	Boot or Logon Autostart Execution	0	0
	Boot or Logon Autostart Execution	0	0
	Sub-techniques	0/14	0
Boot or Logon	Boot or Logon	0	0
	Boot or Logon	0	0
	Boot or Logon	0	0
	Sub-techniques	0/0	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**

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 when expanded)
 

- >10 rules
- 1-3 rules
- 0 rules

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

**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**

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

Installed rule status: 1 / 1

Installed rule type: 2 / 2

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

Collapse cells | Expand cells

Legend: >10 ru (dark green) | 1-3 ru (light green)

Tactic	Defense Evasion	Credential Access	Discovery	Lateral Movement
0/45 techniques	0/17 techniques	1/33 techniques	0/9 techniques	
Disabled Rules: 0 Enabled Rules: 0	Disabled Rules: 0 Enabled Rules: 1	Disabled Rules: 0 Enabled Rules: 1	Disabled Rules: 0 Enabled Rules: 0	
Abuse Elevation Control Mechanism Sub-techniques 0/6	Adversary-In-the-Middle Sub-techniques 0/4	Account Discovery Sub-techniques 0/4	Exploitation of Remote Services Sub-techniques 0/0	
Access Token Manipulation Sub-techniques 0/5	Brute Force Sub-techniques 2/4	Application Window Discovery Sub-techniques 0/0	Internal Spearphishing Sub-techniques 0/0	
BITs Jobs Sub-techniques 0/7	Credentials from Password Stores Sub-techniques 0/6	Browser Information Discovery Sub-techniques 0/0	Lateral Tool Transfer Sub-techniques 0/0	
			Remote Service Session	

0/12

Job 0/5

0/4

Discovery	Permissions Modification	Sub-techniques	Group Policy Discovery	Network Service Discovery	Network Share Discovery	Network Sniffing	Unsecured Credentials
Sub-techniques 0/8	Sub-techniques 0/2	0/8	Sub-techniques 0/0	Sub-techniques 0/0	Sub-techniques 0/0	Sub-techniques 0/0	Sub-techniques 0/0
Steal Application Access Token Sub-techniques 0/0	Steal Web Session Cookie Sub-techniques 0/0		Log Enumeration Sub-techniques 0/0	Network Service Discovery Sub-techniques 0/0	Network Share Discovery Sub-techniques 0/0	Network Sniffing Sub-techniques 0/0	Unsecured Credentials
Hijack Execution Flow Sub-techniques 0/12	Impair Defenses Sub-techniques 0/11		Steal or Forge Authentication Certificates Sub-techniques 0/0				
Hide Artifacts Sub-techniques 0/14	Impersonation Sub-techniques 0/0		Steal or Forge Kerberos Tickets Sub-techniques 0/5				
Indicator Removal Sub-techniques 0/10			Unsecured Credentials				

**Network Service Discovery**

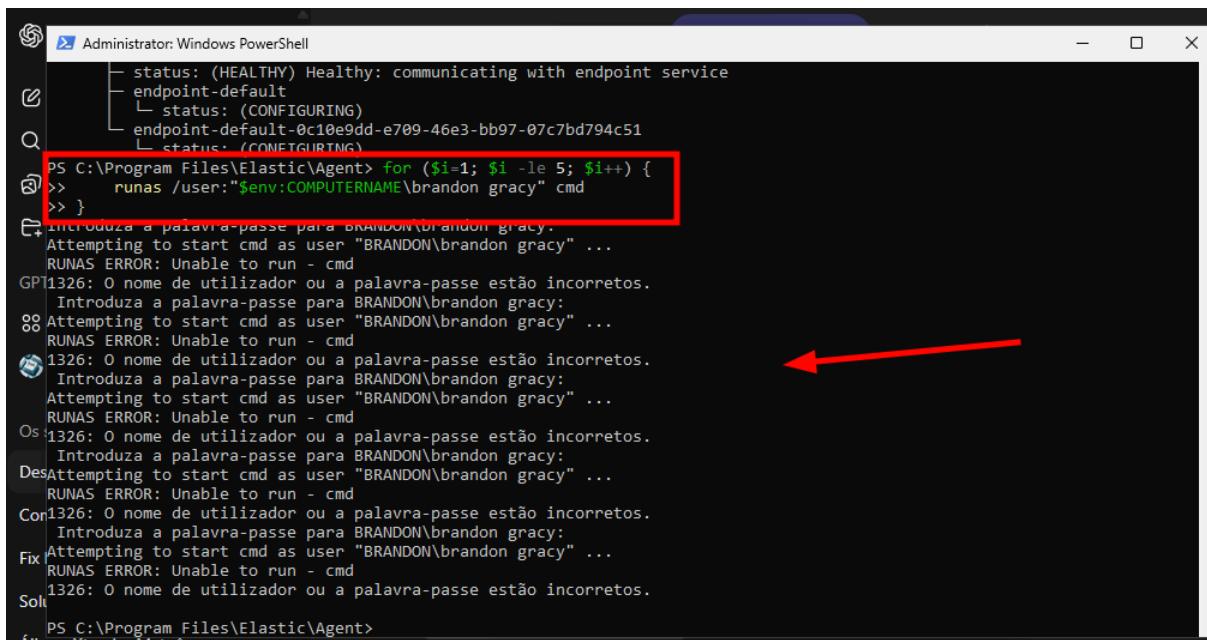
Sub-techniques 0/0

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.



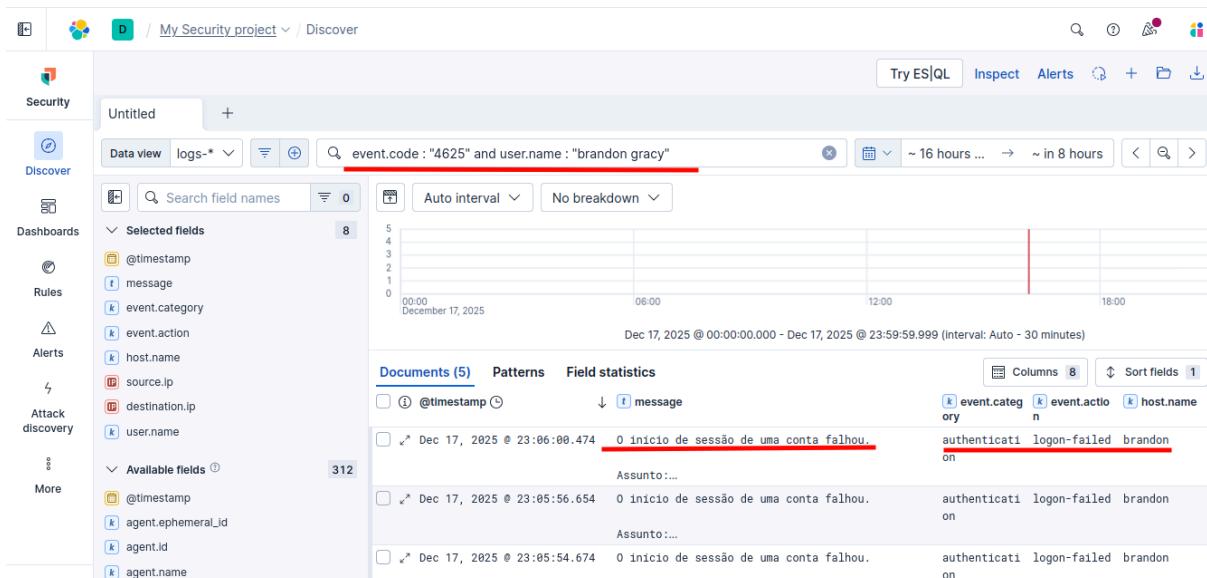
```

Administrator: Windows PowerShell
PS C:\Program Files\Elastic\Agent> for ($i=1; $i -le 5; $i++) {
>>   runas /user:"$env:COMPUTERNAME\brandon gracy" cmd
>> }

+ Introduza a palavra-passe para BRANDON\brandon gracy.
Attempting to start cmd as user "BRANDON\brandon gracy" ...
RUNAS ERROR: Unable to run - cmd
GPT1326: O nome de utilizador ou a palavra-passe estão incorretos.
Introduza a palavra-passe para BRANDON\brandon gracy:
88 Attempting to start cmd as user "BRANDON\brandon gracy" ...
RUNAS ERROR: Unable to run - cmd
1326: O nome de utilizador ou a palavra-passe estão incorretos.
Introduza a palavra-passe para BRANDON\brandon gracy:
Attempting to start cmd as user "BRANDON\brandon gracy" ...
RUNAS ERROR: Unable to run - cmd
Os1326: O nome de utilizador ou a palavra-passe estão incorretos.
Introduza a palavra-passe para BRANDON\brandon gracy:
DesAttempting to start cmd as user "BRANDON\brandon gracy" ...
RUNAS ERROR: Unable to run - cmd
Com1326: O nome de utilizador ou a palavra-passe estão incorretos.
Introduza a palavra-passe para BRANDON\brandon gracy:
FixAttempting to start cmd as user "BRANDON\brandon gracy" ...
RUNAS ERROR: Unable to run - cmd
1326: O nome de utilizador ou a palavra-passe estão incorretos.
Solt
PS C:\Program Files\Elastic\Agent>

```

Now, in the windows vm, we run a command to fail the password authentication to see in the elastic the error.



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

Document	Time	Message
Dec 17, 2025 @ 23:06:00.474	Dec 17, 2025 @ 23:06:00.474	0 inicio de sessão de uma conta falhou.
Dec 17, 2025 @ 23:05:56.654	Dec 17, 2025 @ 23:05:56.654	0 inicio de sessão de uma conta falhou.
Dec 17, 2025 @ 23:05:54.674	Dec 17, 2025 @ 23:05:54.674	0 inicio de sessão de uma conta falhou.

Here we can check if the attempt failed to login.

The screenshot shows a Kibana Data View interface with the following details:

- Selected fields:** @timestamp, message, event.category, event.action, host.name, source.ip, destination.ip, user.name.
- Available fields:** @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.
- Time Range:** December 17, 2025 @ 00:00:00.000 - Dec 17, 2025 @ 23:59:59.999 (interval: Auto - 30 min).
- Documents (5) Patterns Field statistics:**
  - Filter: @timestamp < Dec 17, 2025 @ 23:06:00.474
  - Sort by: message
  - Results:
    - Dec 17, 2025 @ 23:05:56.654: Conta: BRANDON ID de Inicio 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 @ 23:05:54.674: Informações da Falha: Motivo da Falha: Nome de utilizador desconhecido ou palavra-passe incorreta. Estado: 0xC000006D Sub-estado: 0xC0000064
    - Dec 17, 2025 @ 23:05:51.515: Informações do Processo: ID do Processo Chamador: 0x2ff4 Nome do Processo Chamador: C:\Windows\System32\svchost.exe
    - Dec 17, 2025 @ 23:05:48.529: Informações da Rede: Nome da Estação de Trabalho: BRANDON Endereço de Rede de Origem: ::1 Porta de Origem: 0 Informações de Autenticação Detalhadas: Processo de Início de Sessão: seelogon Pacote

Here, we can check what the issue is.

The screenshot shows the Splunk Security Cloud Alerts page with the following details:

- Left sidebar:** Security, Discover, Dashboards, Rules, **Alerts**, Attack discovery, Findings, Cases, More.
- Top navigation:** ML Job settings, Add integrations, Data view, Security solution default, Today, Refresh.
- Alert summary:**
  - Status: Severity
  - User: brandon
  - Host: brandon
- Summary section:**
  - Severity levels: Medium (2 alerts)
  - Alerts by name: newnew (2 alerts)
  - Top alerts by host.name: brandon (100%)
- Alert details table:**

Assignee	Severity	Risk Score	Reason
	medium	47	authentication, session event with process svchost.exe, source ::1:0, by brandon created medium alert newnew.
	medium	47	authentication, session event with process svchost.exe, source ::1:0, by brandon

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

