

SIEM Rules Detection Task

Yehia A. Mostafa

1) Task Description

Create detection rules for:

1. **User account and group enumeration**

Example: `net user` , `net group` , `whoami /groups`

2. **User account creation using net command**

Example: `net user attacker Passw0rd! /add`

3. **Privilege escalation by adding a new user to the Administrators group**

Example: `net localgroup administrators attacker /add`

4. **Credential dumping by extracting the Security Account Manager (SAM)**

Example: `reg save HKLM\SAM` or tools that attempt SAM database access

Bonus (Optional)

Create a **correlation rule** (EQL) to detect a brute force attack by correlating **multiple failed logons** followed by a **successful logon** from the same account and source within a short timeframe.

Reference

- <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>

2) Environment & Prep

- Increased **Ubuntu Server RAM to 8 GB** (Server was irresponsive due to lack of resources).
- Installed **Sysmon** to capture process details (e.g., `process.args`) and ship them to Elastic:
 1. Downloaded **Sysmon64**

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

2. Downloaded **Sysmon config** (XML) from GitHub (repo with exported config).
3. Installed with:

```
.\Sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

4. Verified service:

```
Get-Service Sysmon64
```

5. In **Kibana** → **Fleet** → **Agents** → **Edit policy** → **Add Windows integration** → **Activate Sysmon logging**.

3) Practice Task discussed in session:

Created this PS Script

```
$TestUser = "elasticTestUser"
$Password = ConvertTo-SecureString "P@ssw0rd123!" -AsPlainText -Force

Write-Host "=== Task 1: Generating Windows Admin Events for Elastic ==="

# 1. User Creation
Write-Host "[+] Creating test user: $TestUser"
New-LocalUser -Name $TestUser -Password $Password -FullName "Elastic Test User" -Description "Test user for Elastic log events"

# 2. User Deletion (create another temp user then delete)
$TempUser = "tempDeleteUser"
Write-Host "[+] Creating and deleting user: $TempUser"
New-LocalUser -Name $TempUser -Password $Password -FullName "Temp Delete User" -Description "User to be deleted"
Remove-LocalUser -Name $TempUser
```

```
# 3. Lockout User (simulate failed logon attempts if policy allows)
Write-Host "[+] Simulating failed logins to lock out user: $TestUser"
for ($i=0; $i -lt 10; $i++) {
    Start-Process "powershell.exe" -ArgumentList "net use \\localhost\IPC$ /user:$env:COMPUTERNAME\$TestUser WrongPassword!" -WindowStyle Hidden
    Start-Sleep -Seconds 2
}

# 4. Privilege Escalation (add user to Administrators)
Write-Host "[+] Adding $TestUser to Administrators group"
Add-LocalGroupMember -Group "Administrators" -Member $TestUser

# 5. Disable User
Write-Host "[+] Disabling $TestUser"
Disable-LocalUser -Name $TestUser

# 6. Add New Policy (audit policy change as example)
Write-Host "[+] Modifying audit policy"
auditpol.exe /set /subcategory:"Logoff" /success:enable
```

4) Test Activity Scripts (to trigger all detections)

4.1 AdminActions.ps1 (initial user/admin events script)

If you see errors when running, you can use:

```
powershell -ExecutionPolicy Bypass -File "C:\Users\yehia
mostafa\OneDrive\Desktop\AdminActions.ps1"
```

```
$TestUser = "elasticTestUser"
$Password = ConvertTo-SecureString "P@ssw0rd123!" -AsPlainText -Force
```

Write-Host "=== Task 1: Generating Windows Admin Events for Elastic ==="

1. User Creation

Write-Host "[+] Creating test user: \$TestUser"

New-LocalUser -Name \$TestUser -Password \$Password -FullName "Elastic Test User" -Description "Test user for Elastic log events"

2. User Deletion (create another temp user then delete)

\$TempUser = "tempDeleteUser"

Write-Host "[+] Creating and deleting user: \$TempUser"

New-LocalUser -Name \$TempUser -Password \$Password -FullName "Temp Delete User" -Description "User to be deleted"

Remove-LocalUser -Name \$TempUser

3. Lockout User (simulate failed logon attempts if policy allows)

Write-Host "[+] Simulating failed logins to lock out user: \$TestUser"

for (\$i=0; \$i -lt 10; \$i++) {

 Start-Process "powershell.exe" -ArgumentList "net use \\localhost\IPC\$ /user:\$env:COMPUTERNAME\\$TestUser WrongPassword!" -WindowStyle Hidden

 Start-Sleep -Seconds 2

}

4. Privilege Escalation (add user to Administrators)

Write-Host "[+] Adding \$TestUser to Administrators group"

Add-LocalGroupMember -Group "Administrators" -Member \$TestUser

5. Disable User

Write-Host "[+] Disabling \$TestUser"

Disable-LocalUser -Name \$TestUser

6. Add New Policy (audit policy change as example)

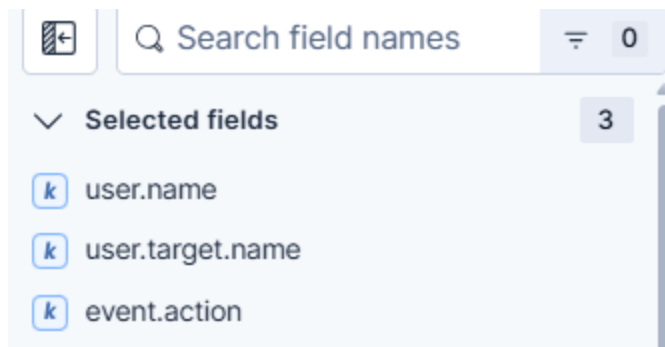
Write-Host "[+] Modifying audit policy"

auditpol.exe /set /subcategory:"Logoff" /success:enable

```
PS C:\Users\yehia mostafa\OneDrive\Desktop> powershell -ExecutionPolicy Bypass -File "C:\Users\yehia mostafa\OneDrive\Desktop\AdminActions.ps1"
=== Task 1: Generating Windows Admin Events for Elastic ===
[*] Creating test user: elasticTestUser
[*] Creating and deleting user: tempDeleteUser
[*] Simulating failed logins to lock out user: elasticTestUser
[*] Adding elasticTestUser to Administrators group
[*] Disabling elasticTestUser
[*] Modifying audit policy
The command was successfully executed.
```

- **Kibana → Discover** → selected relevant fields for visibility and filtering.
- Excluded empty rows for `user.name` or `user.target.name` (hover field → **minus**).
- Filtered by the created test user `elasticTestUser` using:

`user.target.name: elastic*`



@timestamp	user.name	user.target.name	event.action
Aug 16, 2025 @ 14:24:24.311	DESKTOP-C1JD759S	elasticTestUser	group-membership-enumerated
Aug 16, 2025 @ 14:24:24.396	DESKTOP-C1JD759S	elasticTestUser	group-membership-enumerated
Aug 16, 2025 @ 14:24:24.298	DESKTOP-C1JD759S	elasticTestUser	group-membership-enumerated
Aug 16, 2025 @ 14:24:24.291	DESKTOP-C1JD759S	elasticTestUser	group-membership-enumerated
Aug 16, 2025 @ 14:22:16.037	Yehia Mostafa	elasticTestUser	modified-user-account
Aug 16, 2025 @ 14:22:16.037	Yehia Mostafa	elasticTestUser	disabled-user-account
Aug 16, 2025 @ 14:21:55.562	Yehia Mostafa	elasticTestUser	reset-password
Aug 16, 2025 @ 14:21:55.562	Yehia Mostafa	elasticTestUser	modified-user-account
Aug 16, 2025 @ 14:21:55.534	Yehia Mostafa	elasticTestUser	modified-user-account
Aug 16, 2025 @ 14:21:55.534	Yehia Mostafa	elasticTestUser	enabled-user-account

success — events visible and attributable.

4.2 AdminActionsTest.ps1 (bulk trigger for the 4 rules + cleanup)

```

# =====
# AdminActionsTest.ps1
# Script to trigger detection rules in Elastic via Windows Security Events
# =====

Write-Host ">>> Starting detection trigger script..." -ForegroundColor Cyan

# 1. Recon / Enumeration (net.exe + whoami.exe)
Write-Host ">>> Running enumeration commands..." -ForegroundColor Yellow
W
Start-Process -FilePath "net.exe" -ArgumentList "user" -NoNewWindow -Wait
Start-Process -FilePath "net.exe" -ArgumentList "group" -NoNewWindow -Wait
Start-Process -FilePath "whoami.exe" -ArgumentList "/groups" -NoNewWindow -Wait

# 2. User Creation (Event ID 4720)
Write-Host ">>> Creating test user 'elasticTestUser'..." -ForegroundColor Yellow
net user elasticTestUser Password! /add

# 3. Privilege Escalation (Add to Administrators group, Event ID 4732)
Write-Host ">>> Adding test user 'elasticTestUser' to Administrators group..." -ForegroundColor Yellow
net localgroup Administrators elasticTestUser /add

# 4. Credential Dumping Attempt (reg.exe saving SAM hive)
Write-Host ">>> Attempting to dump SAM hive (this may be blocked)..." -ForegroundColor Yellow
try {
    Start-Process -FilePath "reg.exe" -ArgumentList "save HKLM\SAM C:\Temp\SAM_dump.save" -NoNewWindow -Wait
} catch {
    Write-Host ">>> Failed to dump SAM hive (expected if no permissions)." -ForegroundColor Red
}

```

```
}
```

```
# =====
```

```
# CLEANUP SECTION
```

```
# =====
```

Write-Host ">>> Cleaning up test user and reverting changes..." -ForegroundColor Cyan

```
# Remove user from Administrators group
```

```
net localgroup Administrators elasticTestUser /delete
```

```
# Delete user account
```

```
net user elasticTestUser /delete
```

```
# Remove dump file if it exists
```

```
if (Test-Path "C:\Temp\SAM_dump.save") {
```

```
    Remove-Item "C:\Temp\SAM_dump.save" -Force
```

```
    Write-Host ">>> Removed SAM hive dump file." -ForegroundColor Yellow
```

```
}
```

Write-Host ">>> Cleanup complete. Test finished." -ForegroundColor Green

Columns 12 Sort fields 1 19 alerts Fields										Updated 10 seconds ago		Grid view Additional filters		Group alerts by: None			
Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason	host.name	ut									
  	Aug 17, 2025 @ 11:07:47.855	Privilege Escalation (add to...		medium	47	iam event by Yehia Mostafa on desktop-c1jd759 created medium alert Priv...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.850	Privilege Escalation (add to...		medium	47	iam event by Yehia Mostafa on desktop-c1jd759 created medium alert Priv...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.737	User Creation Detection		low	21	event on desktop-c1jd759 created low alert User Creation Detection.	desktop-c1jd759	—									
  	Aug 17, 2025 @ 11:07:47.730	User Creation Detection		low	21	iam event by Yehia Mostafa on desktop-c1jd759 created low alert User Cr...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.717	Recon (Enumeration)		medium	47	process event with process whoami.exe, parent process powershell.exe, by...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.715	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.710	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.706	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.702	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.698	Recon (Enumeration)		medium	47	process event with process whoami.exe, parent process powershell.exe, by...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.694	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.690	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 11:07:47.635	Credential Dumping (SAM ...		high	73	process event with process reg.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
  	Aug 17, 2025 @ 10:58:17.816	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
	Aug 17, 2025 @ 10:58:17.814	Recon (Enumeration)		medium	47	process event with process whoami.exe, parent process powershell.exe, by...	desktop-c1jd759	Yi									
	Aug 17, 2025 @ 10:58:17.811	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
	Aug 17, 2025 @ 10:58:17.808	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
	Aug 17, 2025 @ 10:58:17.784	Credential Dumping (SAM ...		high	73	process event with process reg.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi									
	Aug 17, 2025 @ 10:56:47.598	Recon (Enumeration)		medium	47	process event with process net.exe, parent process cmd.exe, by Yehia Mos...	desktop-c1jd759	Yi									

5) Detection Use Cases (Rules)

5.1 User Account Creation (net user)

Rule Name

Windows – User Account Created

Detection Logic (KQL)

```
event.action: "user-account-created" or event.code: "4720"
```

Name

User Creation Detection

Description

This detection rule identifies the creation of new user accounts on Windows systems by monitoring for Security Event ID 4720 or the normalized field event.action: "user-account-created". Adversaries often create new local or domain accounts to establish persistence, elevate privileges, or maintain long-term access within a compromised environment.

Default severity

Select a severity level for all alerts generated by this rule.

☒ Low

☐ Severity override

Use source event values to override the default severity.

Default risk score

Select a risk score for all alerts generated by this rule.

0 25 50 75 100 21

☐ Risk score override

Use a source event value to override the default risk score.

Tags

Optional

Type one or more custom identifying tags for this rule. Press enter after each tag to begin a new one.

▼ [Advanced settings](#)

MITRE ATT&CK™ threats
Optional

MITRE ATT&CK™ tactic
Persistence (TA0003)
MITRE ATT&CK™ technique
Create Account (T1136)
Add subtechnique
Add technique
Add tactic

Custom highlighted fields
Optional

user.target.name
user.name

Setup guide
Optional

B I [list icons] [quote icon] [code icon] [link icon] [comment icon]
Preview
Prerequisites

- Windows Event Logging must be enabled
- Elastic Agent with Windows integration installed

Provide instructions on rule prerequisites such as required integrations, configuration steps, and anything else needed for the rule to work correctly.

Investigation guide
Optional

B I [list icons] [quote icon] [code icon] [link icon] [comment icon] [share icon] [refresh icon]
Preview
Check if the creator (SubjectUserName) is a known admin account (e.g., IT helpdesk).
3. Escalate if Suspicious
Flag as suspicious if:

- Created by a non-admin user.
- Created outside business hours.
- Account name looks suspicious (e.g., admin2, temp, backupuser).

Author
Optional

Yehia Mostafa - Zerosplit

Type one or more authors for this rule. Press enter after each author to add a new one.

License
Optional
Add a license name

Elastic Endpoint exceptions
☐ Add existing Endpoint exceptions to the rule

Building block
☐ Mark all generated alerts as "building block" alerts

Max alerts per run
Optional

49

The maximum number of alerts the rule will create each time it runs. Default is 100.

The lookback time is the time it rewinds and starts checking since.

Definition About **Schedule** Actions

Schedule

Runs every

30

Seconds

Rules run periodically and detect alerts within the specified time frame.

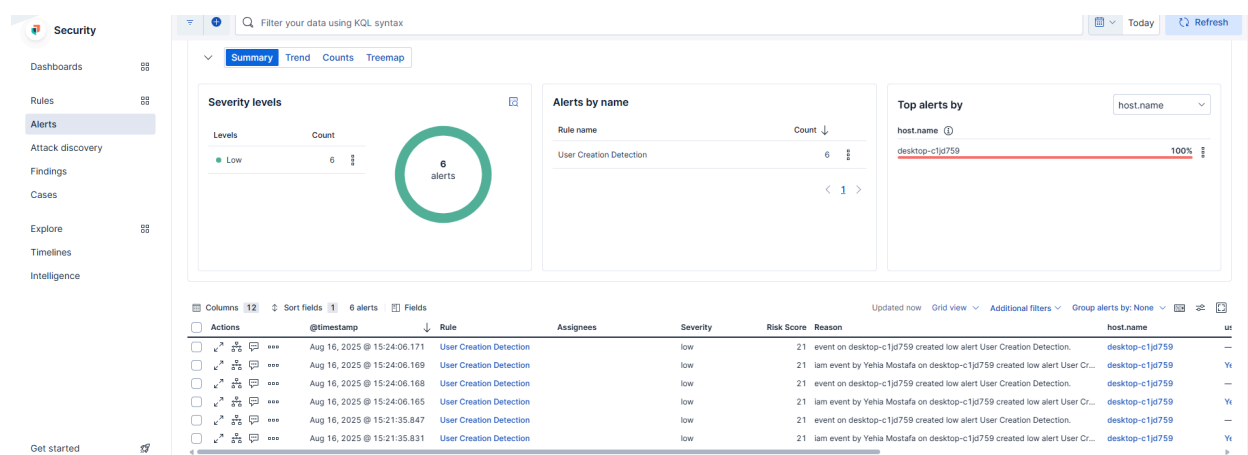
Additional look-back time

3

Hours

Adds time to the look-back period to prevent missed alerts.

Security → Alerts



success.

5.2 User Account & Group Enumeration (Recon)

Using Same Configurations as mentioned above.

Detection Logic (KQL)

```
process.name:("net.exe" or "whoami.exe") and process.args:("user" or "grou
```

p" or "/groups")

5.3 Privilege Escalation (added to Administrators)

Detection Logic (KQL)

event.action: "added-to-group" or event.code: "4732"

5.4 Credential Dumping Attempt (SAM)

Detection Logic (KQL)

process.name: "reg.exe"
and process.args: ("save" and "HKLM\\SAM")

Results for the bulk test:

Columns 12 Sort fields 1 19 alerts Fields											
Updated 10 seconds ago Grid view Additional filters Group alerts by: None											
Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason	host.name	ut			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.855	Privilege Escalation (add to...		medium	47	iam event by Yehia Mostafa on desktop-c1jd759 created medium alert Priv...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.850	Privilege Escalation (add to...		medium	47	iam event by Yehia Mostafa on desktop-c1jd759 created medium alert Priv...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.737	User Creation Detection		low	21	event on desktop-c1jd759 created low alert User Creation Detection.	desktop-c1jd759	—			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.730	User Creation Detection		low	21	iam event by Yehia Mostafa on desktop-c1jd759 created low alert User Cr...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.717	Recon (Enumeration)		medium	47	process event with process whoami.exe, parent process powershell.exe, by...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.715	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.710	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.706	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.702	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.698	Recon (Enumeration)		medium	47	process event with process whoami.exe, parent process powershell.exe, by...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.694	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.690	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 11:07:47.635	Credential Dumping (SAM ...		high	73	process event with process reg.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 10:58:17.816	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 10:58:17.814	Recon (Enumeration)		medium	47	process event with process whoami.exe, parent process powershell.exe, by...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 10:58:17.811	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 10:58:17.808	Recon (Enumeration)		medium	47	process event with process net.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 10:58:17.784	Credential Dumping (SAM ...		high	73	process event with process reg.exe, parent process powershell.exe, by Yeh...	desktop-c1jd759	Yi			
<input type="checkbox"/>	Aug 17, 2025 @ 10:56:47.598	Recon (Enumeration)		medium	47	process event with process net.exe, parent process cmd.exe, by Yehia Mos...	desktop-c1jd759	Yi			

success.

6) Bonus: Brute Force Detection (Correlation)

According to CrowdStrike, ***typical brute force attacks can attempt many guesses per second.***

Implemented detection focuses on clear failed-attempt bursts.

Correlation Rule (EQL)

```
sequence by host.id, source.ip, user.name with maxspan=300s  
[authentication where winlog.event_id == "4625" and event.outcome == "failure"] with runs=10
```

- **Meaning:** For the same `host.id` + `source.ip` + `user.name`, alert when there are ≥ 10 failed logons (`4625`) within **300s**.

8) Hydra Test Setup (Windows SSH & Firewall)

To brute force against the Windows host via SSH:

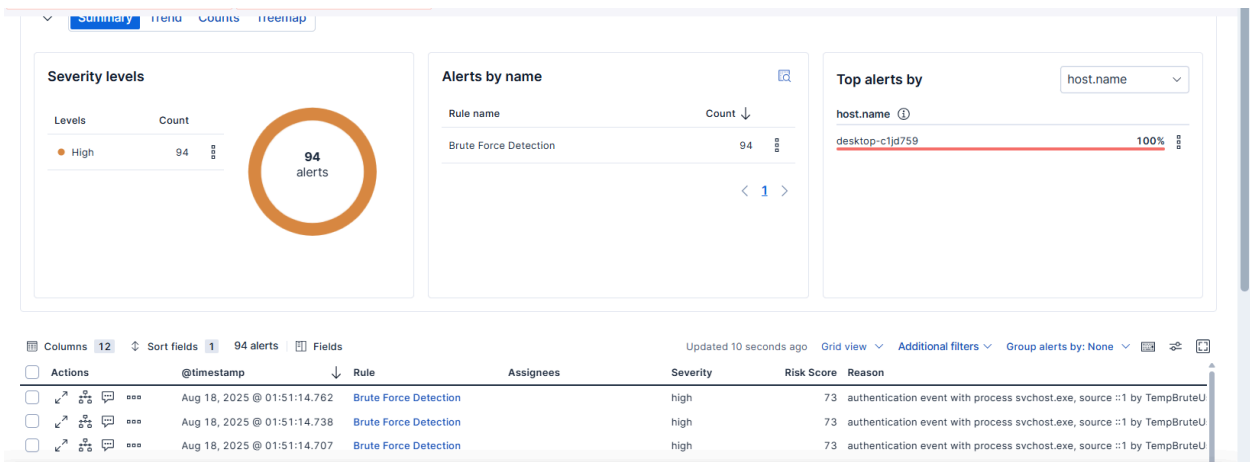
Install OpenSSH Server on Windows host

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0  
  
# Start the service  
Start-Service sshd  
  
# Start on boot  
Set-Service -Name sshd -StartupType 'Automatic'  
  
# Allow SSH in the firewall  
New-NetFirewallRule -Name sshd -DisplayName "OpenSSH Server" -Protocol  
TCP -LocalPort 22 -Action Allow -Direction Inbound
```

Hydra command (from Kali/Ubuntu)

hydra -l "Yehia Mostafa" -P /usr/share/wordlists/rockyou.txt ssh://192.168.138.1 -t 1 -V

```
File Actions Edit View Help
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "boogie2" - 45257 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bondoc" - 45258 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bombar" - 45259 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bobobobo" - 45260 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bob1234" - 45261 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "boarding" - 45262 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bme225" - 45263 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bluelover" - 45264 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bluecar" - 45265 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bluebells" - 45266 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "blue94" - 45267 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "blowme69" - 45268 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bloode5" - 45269 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "blanchard" - 45270 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "black15" - 45271 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "birds" - 45272 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "birdman" - 45273 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "billy69" - 45274 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "biglips" - 45275 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bigjoe" - 45276 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bigbear1" - 45277 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "betita" - 45278 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bestfriendsforever" - 45279 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bellydance" - 45280 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bellylove" - 45281 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bellababy" - 45282 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "belive" - 45283 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bekah" - 45284 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "beijos" - 45285 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bebot" - 45286 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bebeem" - 45287 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "beaufort" - 45288 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "beatriz1" - 45289 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "beatrice1" - 45290 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bball30" - 45291 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "basketball10" - 45292 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "baschet" - 45293 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "barney2" - 45294 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "barefoot" - 45295 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bangag" - 45296 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bandit01" - 45297 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "barana7" - 45298 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bamboo4" - 45299 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "balderas" - 45300 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "balley02" - 45301 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "bagheera" - 45302 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "badangel" - 45303 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babysam" - 45304 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babyim" - 45305 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babygirl09" - 45306 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babygirl02" - 45307 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babybaya" - 45308 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babyboom" - 45309 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babybooi3" - 45310 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "babigr1" - 45311 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "azriel" - 45312 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "awesomeness" - 45313 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "awawaw" - 45314 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "austin21" - 45315 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.138.1 - login "Yehia Mostafa" - pass "aurica" - 45316 of 14344399 [child 0] (0/0)
```



success.

9) EQL Field Mapping Conflict – Problem & Workaround

Observed error:

Found 2 problems line 2:25: Cannot use field [winlog.event_id] due to ambiguities being mapped as

[2] incompatible types: [text] in [winlogbeat-2025.08.14, winlogbeat-2025.08.16, winlogbeat-2025.08.17],

[keyword] in [.ds-logs-system.application-default-2025.08.11-000001, .ds-logs-system.security-default-2025.08.11-000001,

.ds-logs-system.system-default-2025.08.11-000001, .ds-logs-windows.powershell-default-2025.08.17-000001,

.ds-logs-windows.powershell_operational-default-2025.08.17-000001, .ds-logs-windows.sysmon_operational-default-2025.08.17-000001] line 2:55:

Cannot use field [event.outcome] due to ambiguities being mapped as [2] in compatible types:

[text] in [winlogbeat-2025.08.14, winlogbeat-2025.08.16, winlogbeat-2025.08.17], [keyword] in [.ds-logs-system.auth-default-2025.08.11-000001, .ds-logs-system.security-default-2025.08.11-000001,

.ds-logs-windows.powershell-default-2025.08.17-000001, .ds-logs-windows.powershell_operational-default-2025.08.17-000001, .ds-logs-windows.sysmon_operational-default-2025.08.17-000001]

Root cause

- Mixed mappings across indices: some map `winlog.event_id` / `event.outcome` as **text**, others as **keyword**. EQL needs consistency.

Temporary workaround applied

- **Unlinked** problematic indices from the rule so the query runs only against indices with consistent (keyword) mappings.

Index patterns

apm-*-transaction*	auditbeat-*	endgame-*
filebeat-*	logs-*	packetbeat-*
-*elastic-cloud-logs-*		

What “unlinking” did

- Rule stopped querying the broken index pattern → **errors disappeared**.

- **Trade-off:** events in unlinked indices are **ignored** (no detections from them).

Future correct approach (planned)

1. Reindex into a new index (e.g., `winlogbeat-fixed`) with **proper mappings** (`keyword` for `winlog.event_id` , `event.outcome` , etc.).
 2. Delete or stop using the broken index (`winlogbeat-2025.08.17`).
 3. Point rules only at the **fixed index** or a pattern including only fixed indices.
-

10) Cleanup & System State

- Removed temporary test users and group membership changes in the script (cleanup section).
 - Verified only intended local users remain (kept system accounts disabled).
-