🔴 Week 4 – Threat Simulation (Ransomware) using Atomic Red Team

🎯 Objective

- Simulate **ransomware-like behavior**
- Focus on **T1490 – Delete Shadow Volume Copies**
- Detect activity in **Wazuh**
- Map alerts to **MITRE ATT&CK**
- Visualize the **Kill Chain** in **OpenSearch / Kibana**

🧱 Lab Architecture (Assumed)

Component	Role
Kali / Ubuntu	Attacker / Atomic Red Team
Windows 10 / Server	Victim (Wazuh Agent installed)
Wazuh Manager	SIEM
OpenSearch Dashboard	Visualization

🧩 MITRE ATT&CK Mapping (Used)

Kill Chain Phase	Technique
Initial Access	T1059 (Command Execution)
Execution	T1059.003 (PowerShell)
Impact	**T1490 – Inhibit System Recovery**

🟢 STEP 1: Prepare the Windows Target (Victim)

1.1 Verify Wazuh Agent is Running

Get-Service Wazuh*

Status must be **Running**

1.2 Enable Command & PowerShell Logging

Enable PowerShell Script Block Logging

gpedit.msc

Navigate:

Computer Configuration

→ Administrative Templates

→ Windows Components

→ Windows PowerShell

Enable:

- ✅ Turn on PowerShell Script Block Logging
- ✅ Turn on **PowerShell Transcription(For maximum detection visibility)**
- ✅ Turn on Module Logging

**For turn on Module logging you need to add modules:

Step 1: Enable the policy

- Select **Enabled** ✅

Step 2: Click Show… (IMPORTANT)

Under **Options**, click:
Module Names → Show…
👉 This opens a **new list window**
This is the step most people miss.

Step 3: Add module entries (MANDATORY)

In the new window:

1. Click **Add**
2. In **Value name**, enter:
   Microsoft.PowerShell.*
3. Click **OK**
   (Optional but recommended – add second entry)
   Microsoft.WSMan.Management
   ✅ You should now see entries in the list

Step 4: Save

- Click **OK** (close list)
- Click **Apply**
- Click **OK**

  ❌ Do NOT click OK unless the list contains entries

🎯 Why this policy behaves this way

- Module Logging **only logs modules you explicitly specify**
- If the list is empty → policy is invalid → error shown

1.3 Enable Audit Process Creation

auditpol /set /subcategory:"Process Creation" /success:enable /failure:enable

---

🟢 STEP 2: Install Atomic Red Team (On Windows)

2.1 Open PowerShell as Administrator

Set-ExecutionPolicy Bypass -Scope Process -Force

2.2 Install Atomic Red Team

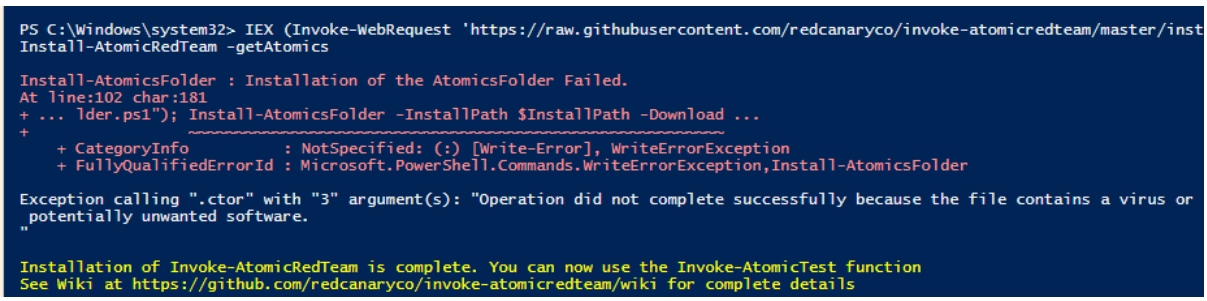
IEX (Invoke-WebRequest 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing)

Install-AtomicRedTeam -getAtomics

Verify:

Get-AtomicTechnique

- If this error occurs:



**Root Cause

This line is the key:

“Operation did not complete successfully because the file contains a virus or potentially unwanted software.”

⚠️ **This is EXPECTED behavior**
Atomic Red Team **contains real malware-like scripts** (by design), so:

- Windows Defender detects them as **PUA / malware**
- The **Atomics folder download is blocked**
- Invoke-AtomicRedTeam module installs ✅
- **Atomic test files do NOT** ❌

Step 1: Open PowerShell as Administrator

Step 2: Create a safe lab directory

mkdir C:\AtomicRedTeam

Step 3: Add Defender Exclusion (REQUIRED)

Add-MpPreference -ExclusionPath "C:\AtomicRedTeam"

Verify:

Get-MpPreference | Select-Object -ExpandProperty ExclusionPath

Step 4: Reinstall Atomics folder

Install-AtomicRedTeam -InstallPath C:\AtomicRedTeam -GetAtomics -Force

You should now see **NO virus error**.

```
PS C:\Windows\system32> Install-AtomicRedTeam -InstallPath C:\AtomicRedTeam -GetAtomics -Force

Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details

PS C:\Windows\system32> Test-Path C:\AtomicRedTeam\atomics

True
```

🟢 **STEP 3: Simulate Ransomware Behavior (T1490)**

3.1 Technique Overview

T1490 – Inhibit System Recovery

Ransomware deletes Shadow Copies to prevent recovery.

3.2 Run Atomic Test for T1490

Invoke-AtomicTest T1490

🔴 This executes:

vssadmin delete shadows /all /quiet

```
PS C:\Windows\system32> Invoke-AtomicTest T1490

PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1490-1 Windows - Delete Volume Shadow Copies
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
No items found that satisfy the query.
Exit code: 1
Done executing test: T1490-1 Windows - Delete Volume Shadow Copies
Executing test: T1490-2 Windows - Delete Volume Shadow Copies via WMI
No Instance(s) Available.
Exit code: 0
Done executing test: T1490-2 Windows - Delete Volume Shadow Copies via WMI
Executing test: T1490-3 Windows - wbadmin Delete Windows Backup Catalog
Process Timed out after 120 seconds, use '-TimeoutSeconds' to specify a different timeout
Exit code: -1
Done executing test: T1490-3 Windows - wbadmin Delete Windows Backup Catalog
Executing test: T1490-4 Windows - Disable Windows Recovery Console Repair
The operation completed successfully.
The operation completed successfully.
Exit code: 0
Done executing test: T1490-4 Windows - Disable Windows Recovery Console Repair
Executing test: T1490-5 Windows - Delete Volume Shadow Copies via WMI with PowerShell
Exit code: 0
Done executing test: T1490-5 Windows - Delete Volume Shadow Copies via WMI with PowerShell
Executing test: T1490-6 Windows - Delete Backup Files
```

🟢 STEP 4: Confirm Alerts in Wazuh

4.1 On Wazuh Manager

****first we need to configure rule here:**

sudo nano /var/ossec/etc/rules/local_rules.xml

```
<!-- ============ ADD CUSTOM T1490 RULE ================== -->
<rule id="100200" level="12">
  <if_sid>60602</if_sid>
  <field name="win.system.providerName">VSS</field>
  <!-- <field name="win.eventdata.binary">vssadmin.exe</field>-->
  <description>Atomic Red Team: Shadow Volume Copies deletion detected (T1490)</description>
  <mitre>
    <id>T1490</id>
```

</mitre>

<group>windows,impact,ransomware</group>

</rule>

```
 GNU nano 6.2                                                    /var/ossec/etc/rules/local_rules.xml
<group name="custom_rules,local">

  <!-- ================ SSH FAILED LOGIN ================ -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1</description>
    <group>linux,authentication_failed,sshd</group>
  </rule>

  <!-- ============ WINDOWS BRUTE FORCE ================== -->
  <rule id="100002" level="5">
    <if_matched_sid>18107</if_matched_sid>
    <description>Windows brute-force detected</description>
    <mitre>
      <id>T1110</id>
    </mitre>
    <group>windows,authentication,bruteforce</group>
  </rule>

  <!-- ============ ADD CUSTOM T1490 RULE ================== -->
  <rule id="100200" level="12">
    <if_sid>60602</if_sid>
    <field name="win.system.providerName">VSS</field>
   <!-- <field name="win.eventdata.binary">vssadmin.exe</field>-->
    <description>Atomic Red Team: Shadow Volume Copies deletion detected (T1490)</description>
    <mitre>
      <id>T1490</id>
    </mitre>
    <group>windows,impact,ransomware</group>
  </rule>

</group>
```

Then:

sudo /var/ossec/bin/wazuh-analysisd -t

sudo systemctl restart wazuh-manager

sudo tail -f /var/ossec/logs/alerts/alerts.json

4.2 Expected Alerts

You should see alerts like:

- Process created: vssadmin.exe
- Suspicious PowerShell execution
- MITRE: T1490

Example fields:

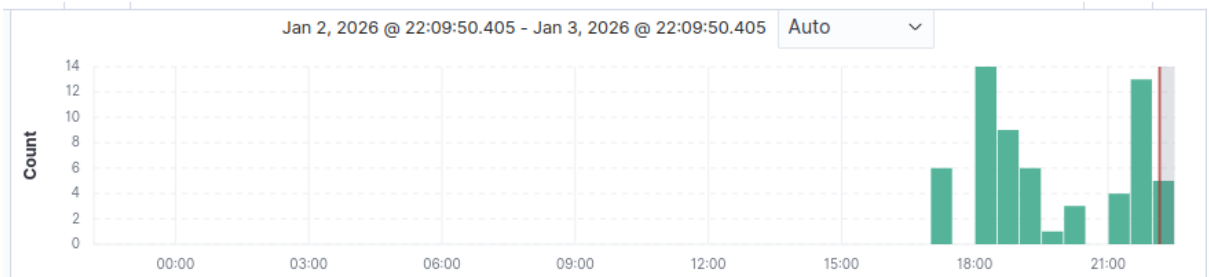
"mitre": {

"id": ["T1490"],

"tactic": ["impact"],

"technique": ["Inhibit System Recovery"]

}



Time	agent.name	rule.description	rule.level	rule.id
Jan 3, 2026 @ 22:08:08.905	WIN-TAHL77SR7PP	Atomic Red Team: Shadow Volume Copies deletion detected (T1490)	12	100200
Jan 3, 2026 @ 22:08:08.864	WIN-TAHL77SR7PP	Atomic Red Team: Shadow Volume Copies deletion detected (T1490)	12	100200
Jan 3, 2026 @ 22:04:00.779	WIN-TAHL77SR7PP	Atomic Red Team: Shadow Volume Copies deletion detected (T1490)	12	100200
Jan 3, 2026 @ 22:01:52.011	WIN-TAHL77SR7PP	Windows logon success.	3	60106
Jan 3, 2026 @ 22:01:24.153	WIN-TAHL77SR7PP	Atomic Red Team: Shadow Volume Copies deletion detected (T1490)	12	100200
Jan 3, 2026 @ 21:58:29.459	WIN-TAHL77SR7PP	Windows application error event.	9	60602
Jan 3, 2026 @ 21:58:29.417	WIN-TAHL77SR7PP	Windows application error event.	9	60602
Jan 3, 2026 @ 21:57:54.744	WIN-TAHL77SR7PP	Name resolution for the name time.windows.com timed out	5	61109
Jan 3, 2026 @ 21:56:18.580	WIN-TAHL77SR7PP	Windows application error event.	9	60602
Jan 3, 2026 @ 21:53:42.571	WIN-TAHL77SR7PP	Windows logon success.	3	60106
Jan 3, 2026 @ 21:49:42.213	WIN-TAHL77SR7P	Windows application error event.	9	60602

🟢 STEP 5: Map Alerts to the Kill Chain

Kill Chain Sequence for This Attack

Initial Access → Execution → Impact

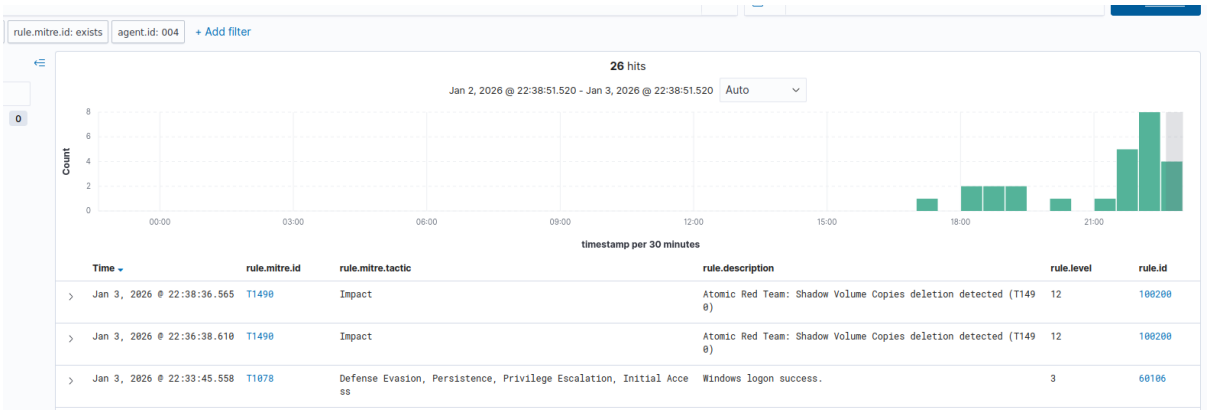
Order	Event Observed	Evidence (Your Logs)	MITRE Technique
1	Valid account logon	Windows Event **4624** (SYSTEM / Elevated Token)	**T1078 – Valid Accounts**
2	Command execution via PowerShell	Invoke-AtomicTest T1490	**T1059 – Command and Scripting Interpreter**

3	OS utility execution	vssadmin.exe delete shadows /all /quiet	**T1059.003 – Windows Command Shell**
4	Shadow copy deletion attempt	VSS Event **ID 13**	**T1490 – Inhibit System Recovery**

```
PS C:\Windows\system32> Invoke-AtomicTest T1490 -TestNumbers 1

PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1490-1 Windows - Delete Volume Shadow Copies
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
Error: You don't have the correct permissions to run this command.  Please run this utility from a command
window that has elevated administrator privileges.
Exit code: 2
Done executing test: T1490-1 Windows - Delete Volume Shadow Copies
```



**NOTE: If this error occur

```
PS C:\Windows\system32> Invoke-AtomicTest T1490 -WhatIf

Invoke-AtomicTest : The term 'Invoke-AtomicTest' is not recognized as the name of a cmdlet, function, script file,
At line:1 char:1
+ Invoke-AtomicTest T1490 -WhatIf
+ ~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Invoke-AtomicTest:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

Then follow below steps:

Step 1: Open PowerShell as Administrator

(This is mandatory for T1490)

Step 2: Check if Atomic Red Team Exists

Test-Path C:\AtomicRedTeam

If False, install it:

cd C:\

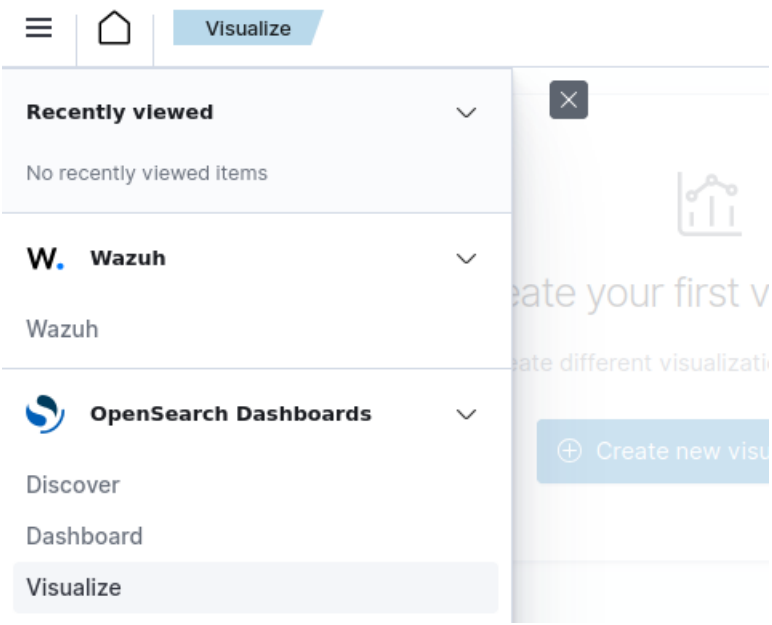
git clone https://github.com/redcanaryco/atomic-red-team.git

Step 3: Import Atomic Module

Import-Module C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1 -Force
Verify:
Get-Command Invoke-AtomicTest

🟢 STEP 6: Visualize Kill Chain in OpenSearch

6.1 Open on your host machine Wazuh Dashboard



6.2 Create a Custom Kill Chain Visualization

Go to:

Dashboard → Visualize → Create Visualization

Choose:

- 📊 **Vertical Bar Chart** (or Timeline)

6.3 Configure Data Source

- Index Pattern:
- wazuh-alerts-*

6.4 Buckets Configuration

X-Axis (Kill Chain Order)

- Aggregation: **Terms**
- Field:
- rule.mitre.tactic

Y-Axis

- Aggregation: **Count**

6.5 Add Filter (Only Attack Simulation)

rule.mitre.id : T1490 OR T1059*

6.6 Resulting Visualization

You should see:

Execution → Impact

With timestamps showing **sequence progression**

🟢 **STEP 7: Create Kill Chain Dashboard (Gate Check)**

7.1 Create Dashboard

Dashboard → Create new

Add:

- 📈 Kill Chain Bar Chart
- 📋 Alerts Table
- ⏱️ Timeline of events

7.2 Alerts Table Columns

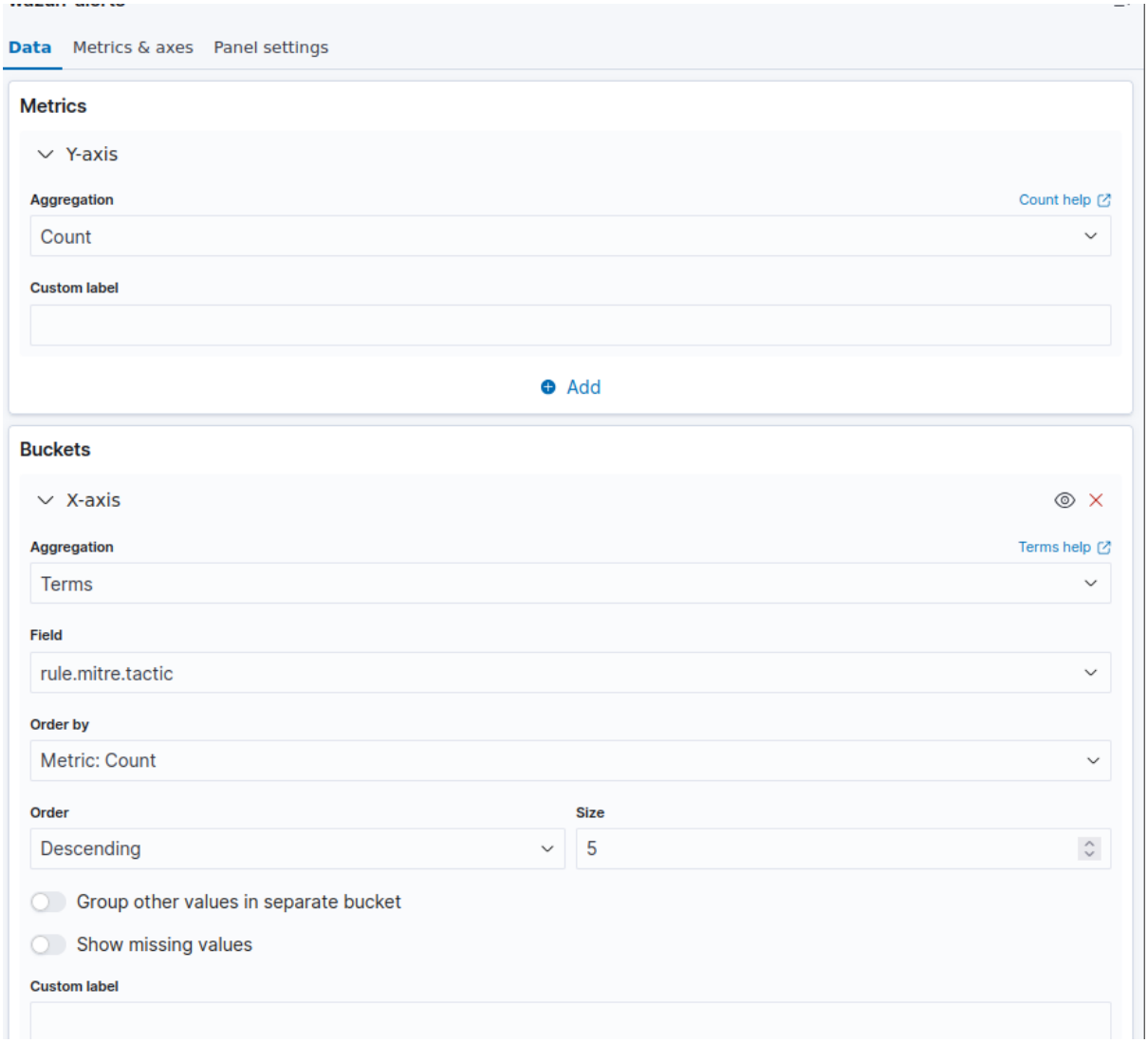
Add:

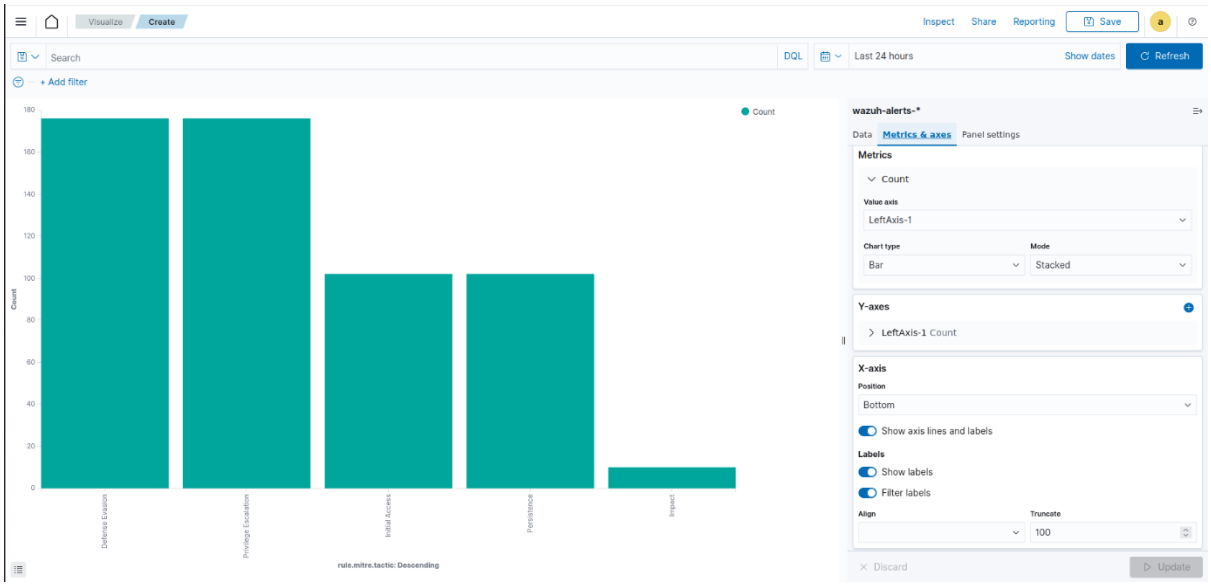
- @timestamp
- agent.name

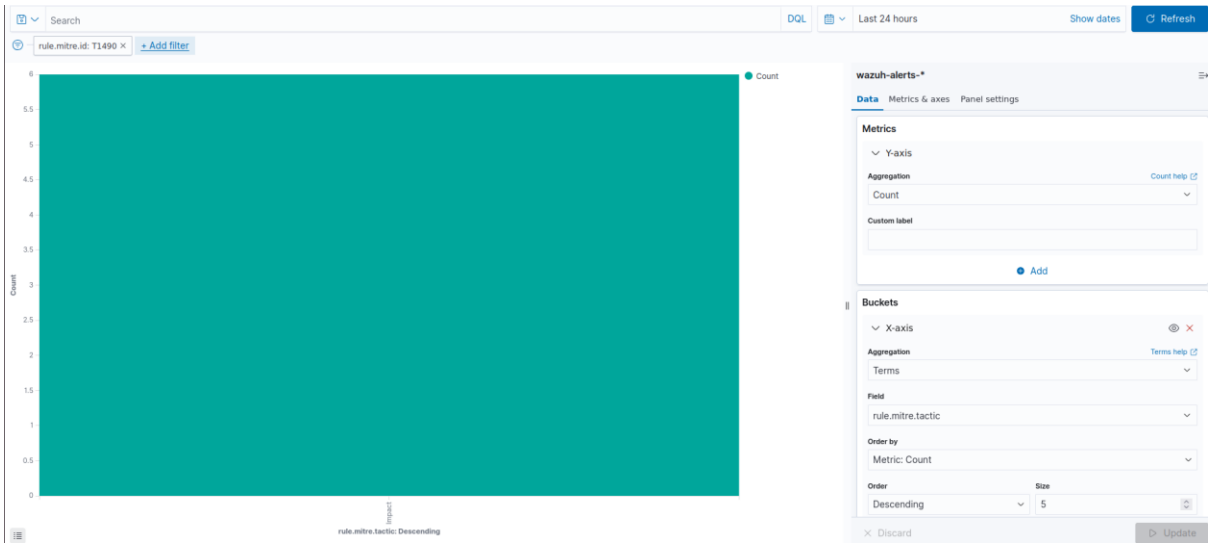
- rule.description
- rule.mitre.id
- rule.mitre.tactic
- process.name

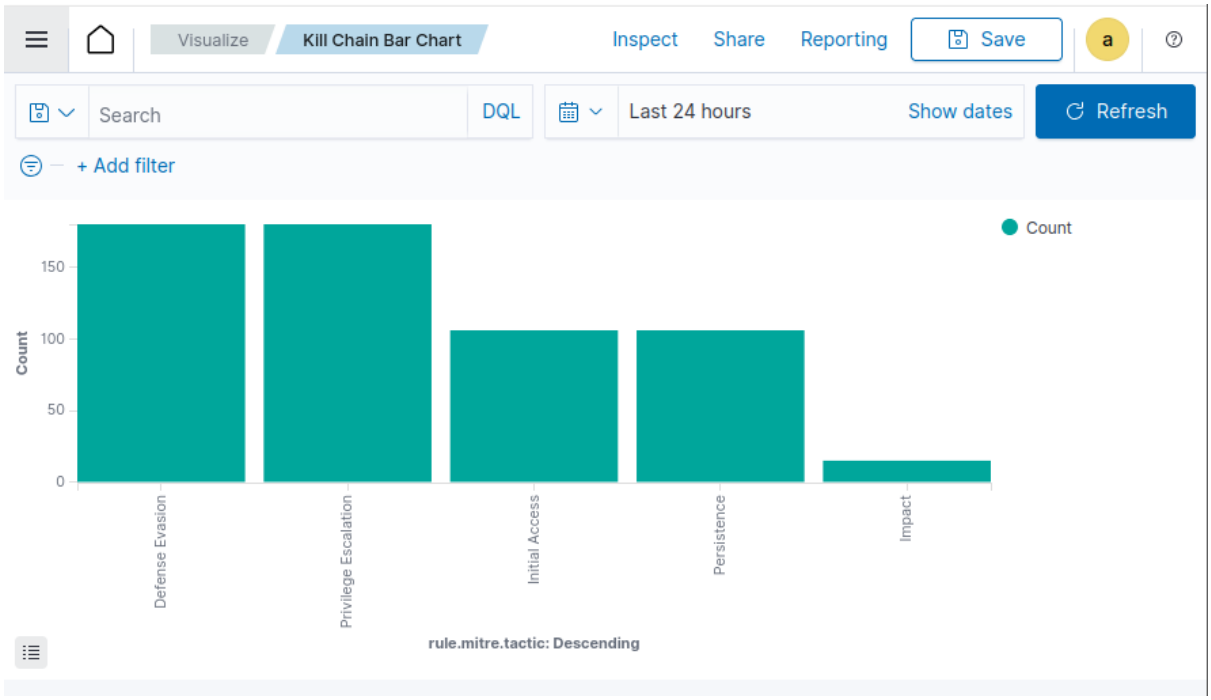
🟢 STEP 8: Gate Check – What to Present

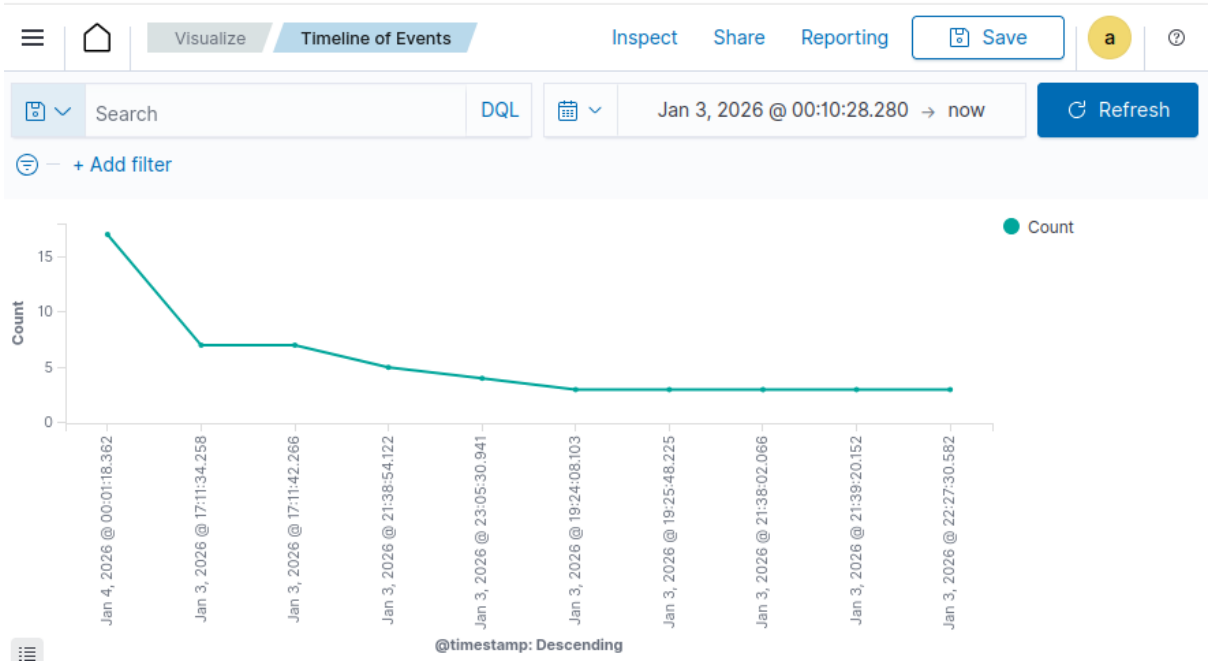
✅ Atomic Red Team command used
✅ Detection in Wazuh alerts
✅ MITRE mapping (T1490)
✅ Kill Chain visualization
✅ Timeline showing attack flow

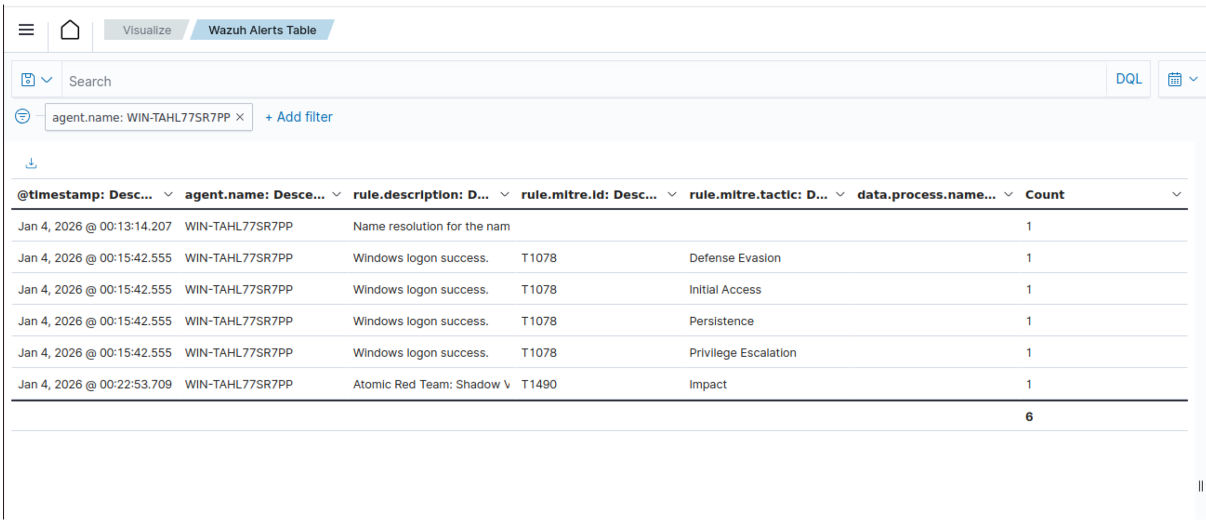


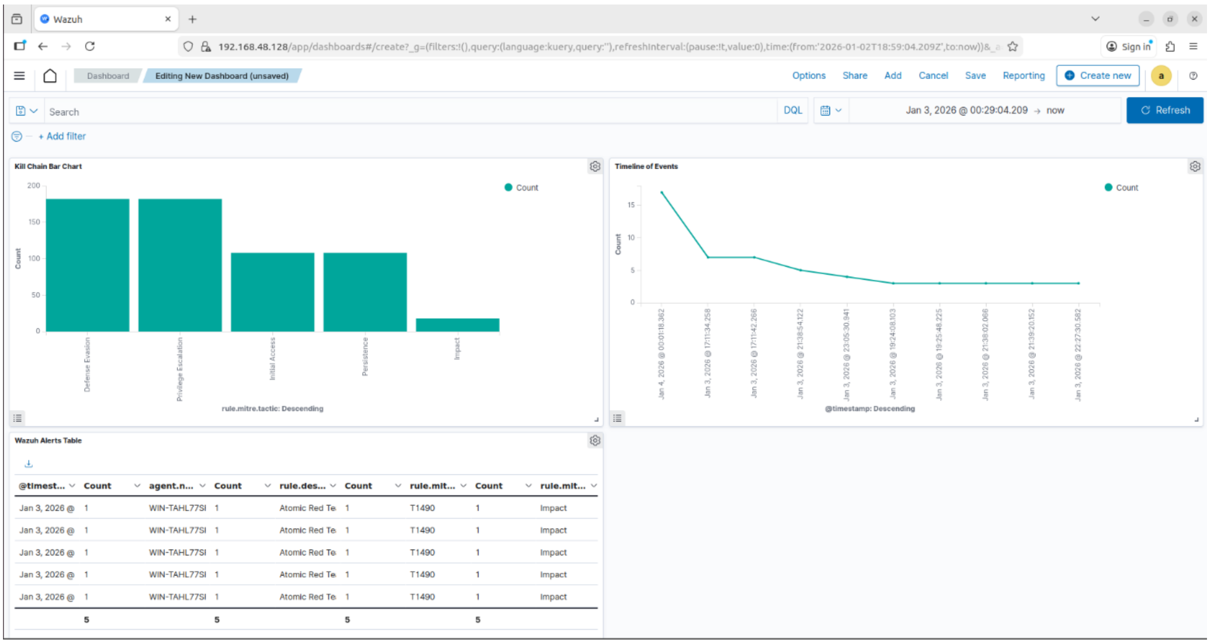

Visualize
Create
Inspect
Share
Reporting
Save
Search
DQL
Last 24 hours
Show dates
Refresh
+ Add filter
Count
Defense Evasion
Privilege Escalation
Initial Access
Persistence
Impact
rule.mitre.tactic: Descending
wazuh-alerts-*
Data
Metrics & axes
Panel settings
Metrics
Count
Value axis
LeftAxis-1
Chart type
Bar
Mode
Stacked
Y-axes
LeftAxis-1 Count
X-axis
Position
Bottom
Show axis lines and labels
Labels
Show labels
Filter labels
Align
Truncate
100
Discard
Update


Search
DQL
Last 24 hours
Show dates
Refresh
rule.mitre.id: T1490
+ Add filter
Count
Impact
rule.mitre.tactic: Descending
wazuh-alerts-*
Data
Metrics & axes
Panel settings
Metrics
Y-axis
Aggregation
Count help
Count
Custom label
Add
Buckets
X-axis
Aggregation
Terms help
Terms
Field
rule.mitre.tactic
Order by
Metric: Count
Order
Descending
Size
5
Discard
Update


Visualize
Kill Chain Bar Chart
Inspect
Share
Reporting
Save
a
Search
DQL
Last 24 hours
Show dates
Refresh
+ Add filter
Count
150
100
50
0
Count
Defense Evasion
Privilege Escalation
Initial Access
Persistence
Impact
rule.mitre.tactic: Descending


Visualize
Timeline of Events
Inspect
Share
Reporting
Save
a
Search
DQL
Jan 3, 2026 @ 00:10:28.280 → now
Refresh
+ Add filter
Count
15
10
5
0
Count
Jan 4, 2026 @ 00:01:18.362
Jan 3, 2026 @ 17:11:34.258
Jan 3, 2026 @ 17:11:42.266
Jan 3, 2026 @ 21:38:54.122
Jan 3, 2026 @ 23:05:30.941
Jan 3, 2026 @ 19:24:08.103
Jan 3, 2026 @ 19:25:48.225
Jan 3, 2026 @ 21:38:02.066
Jan 3, 2026 @ 21:39:20.152
Jan 3, 2026 @ 22:27:30.582
@timestamp: Descending





STEP 9: Cleanup (Optional)

Remove-Item -Recurse -Force C:\AtomicRedTeam