Completion Summary of the Sentinel Project: Honeypot and Incident Detection & Response (Microsoft Sentinel)

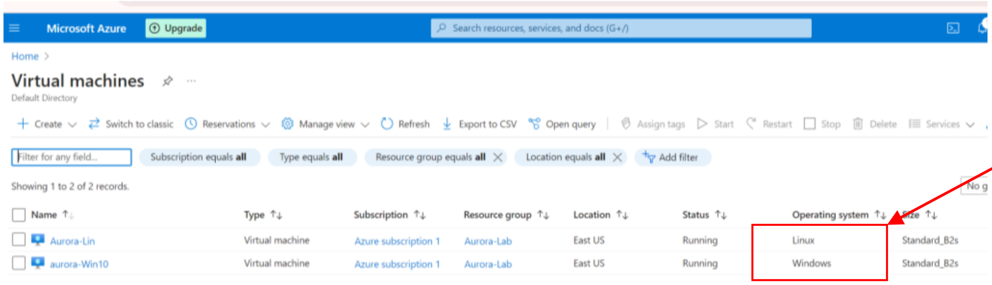
Project Overview

The Sentinel project aimed to enhance threat detection and incident response capabilities by deploying a honeypot in the cloud, monitoring for malicious activity, and implementing robust security measures. The project involved creating open firewall rules to attract public traffic, capturing and analyzing brute force attempts, mapping adversary locations, and developing analytic rules and incident response playbooks. Finally, we secured the environment in line with NIST 800-53 SC-7 (Boundary Protection) and verified the effectiveness of the security measures.

Step-by-Step Summary

1. Honeypot Deployment and Firewall Configuration

a) **Created Honeypot in the Cloud**:
   - ○ Deployed a vulnerable virtual machine (VMs) as a honeypot to attract malicious activities. Windows 10 and Ubuntu 20.0.4 Linux VM.

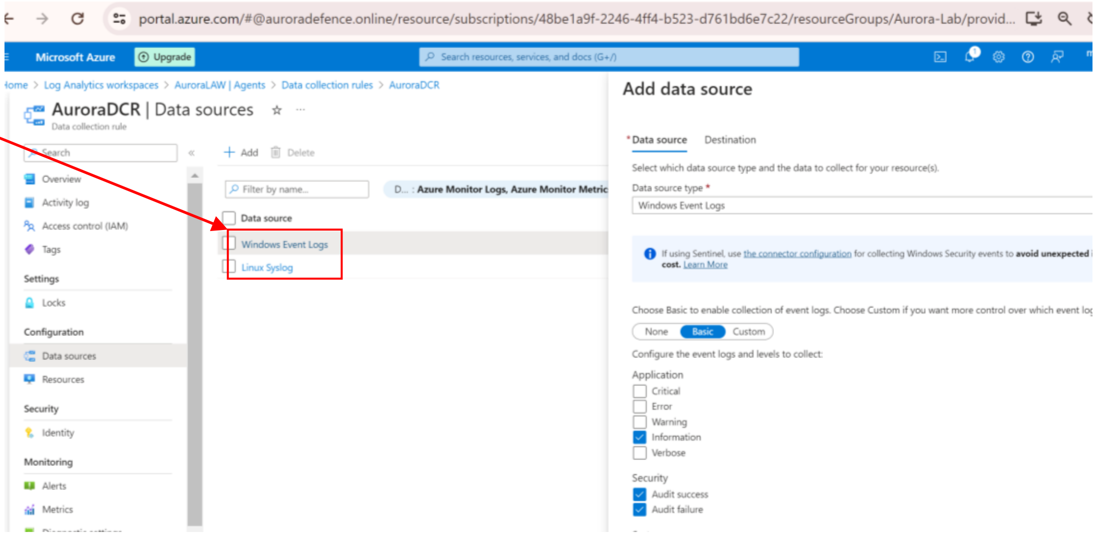


Showing 1 to 2 of 2 records.

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size
Aurora-Lin	Virtual machine	Azure subscription 1	Aurora-Lab	East US	Running	Linux	Standard_B2s
aurora-Win10	Virtual machine	Azure subscription 1	Aurora-Lab	East US	Running	Windows	Standard_B2s

Virtual Machine Operating Systems

Configured required Data Collection rules



portal.azure.com/#@auroradefence.online/resource/subscriptions/48be1a9f-2246-4ff4-b523-d761bd6e7c22/resourceGroups/Aurora-Lab/provid...

Add data source

*Data source | Destination

Select which data source type and the data to collect for your resource(s).

Data source type *: Windows Event Logs

If using Sentinel, use the connector configuration for collecting Windows Security events to **avoid unexpected** **cost.** Learn More

Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event log

None [✓ Basic] Custom

Configure the event logs and levels to collect:

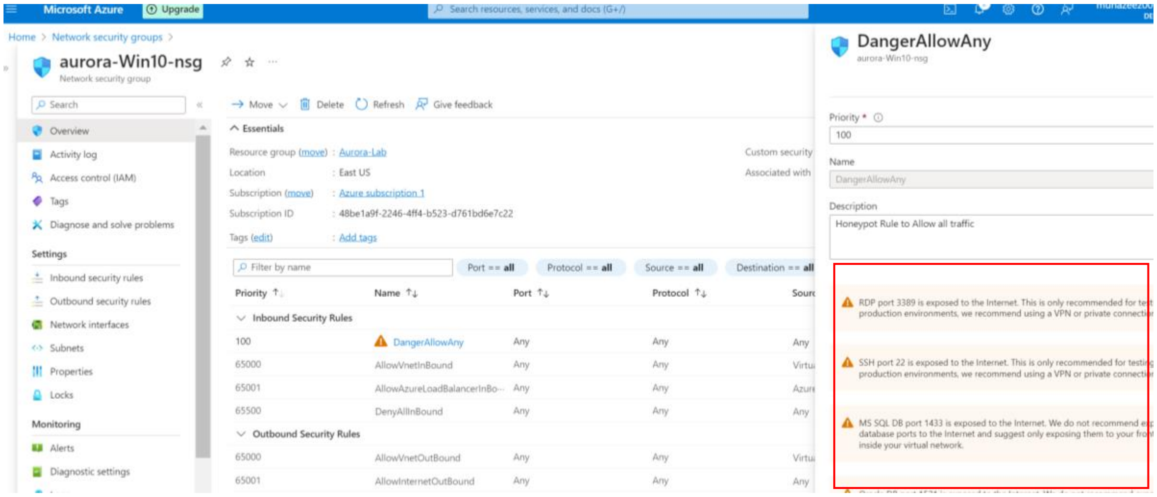
Application
- □ Critical
- □ Error
- □ Warning
- ☑ Information
- □ Verbose

Security
- ☑ Audit success
- ☑ Audit failure

Data Collection Sources

b) **Configured Firewall Rules**:

- Set up open firewall rules to allow public traffic to the honeypot.
- Allowed traffic on common attack vectors like SSH (port 22) and RDP (port 3389).



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Home > Network security groups >

aurora-Win10-nsg
Network security group

Resource group (move) : Aurora-Lab
Location : East US
Subscription (move) : Azure subscription 1
Subscription ID : 48be1a9f-2246-4ff4-b523-d761bd6e7c22
Tags (edit) : Add tags
Custom security
Associated with

Filter by name | Port == all | Protocol == all | Source == all | Destination == all

Priority	Name	Port	Protocol	Sourc
Inbound Security Rules				
100	⚠ DangerAllowAny	Any	Any	Any
65000	AllowVnetInBound	Any	Any	Virtu
65001	AllowAzureLoadBalancerInBo...	Any	Any	Azur
65500	DenyAllInBound	Any	Any	Any
Outbound Security Rules				
65000	AllowVnetOutBound	Any	Any	Virtu
65001	AllowInternetOutBound	Any	Any	Any

DangerAllowAny
aurora-Win10-nsg

Priority * : 100
Name : DangerAllowAny
Description : Honeypot Rule to Allow all traffic

⚠ RDP port 3389 is exposed to the Internet. This is only recommended for te production environments, we recommend using a VPN or private connecti

⚠ SSH port 22 is exposed to the Internet. This is only recommended for testi production environments, we recommend using a VPN or private connecti

⚠ MS SQL DB port 1433 is exposed to the Internet. We do not recommend e database ports to the Internet and suggest only exposing them to your fro inside your virtual network.

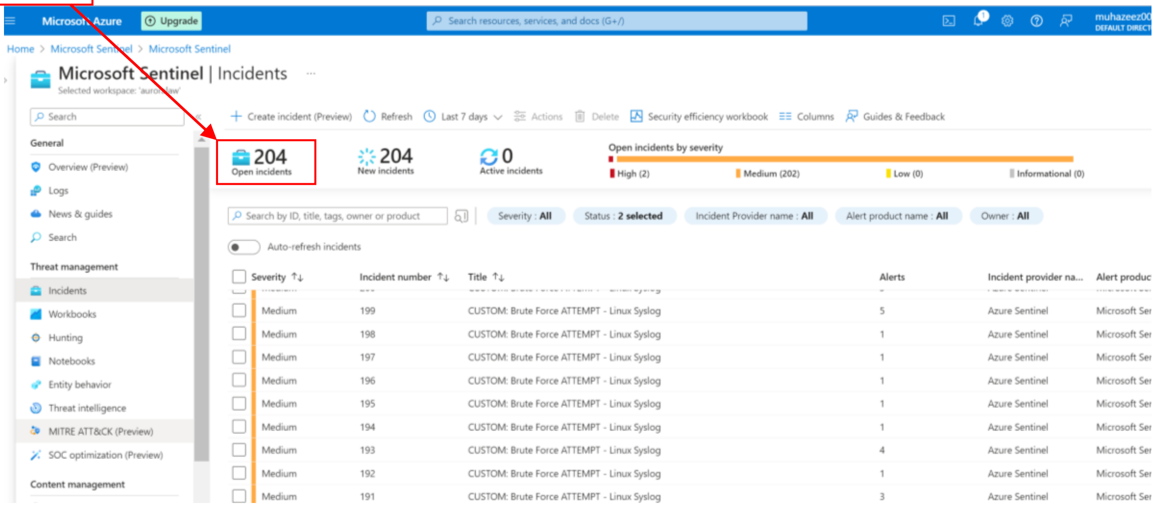
Open Ports

2. Monitoring and Data Collection

a) **Captured Brute Force Attempts**:

- Recorded a significant number of brute force login attempts targeting the honeypot.

Detected Incidents



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
muhazeez00
DEFAULT DIRECT
Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Incidents
Selected workspace: 'aurorlaw'

204 Open incidents | 204 New incidents | 0 Active incidents

Open incidents by severity: High (2) | Medium (202) | Low (0) | Informational (0)

Search by ID, title, tags, owner or product | Severity : All | Status : 2 selected | Incident Provider name : All | Alert product name : All | Owner : All

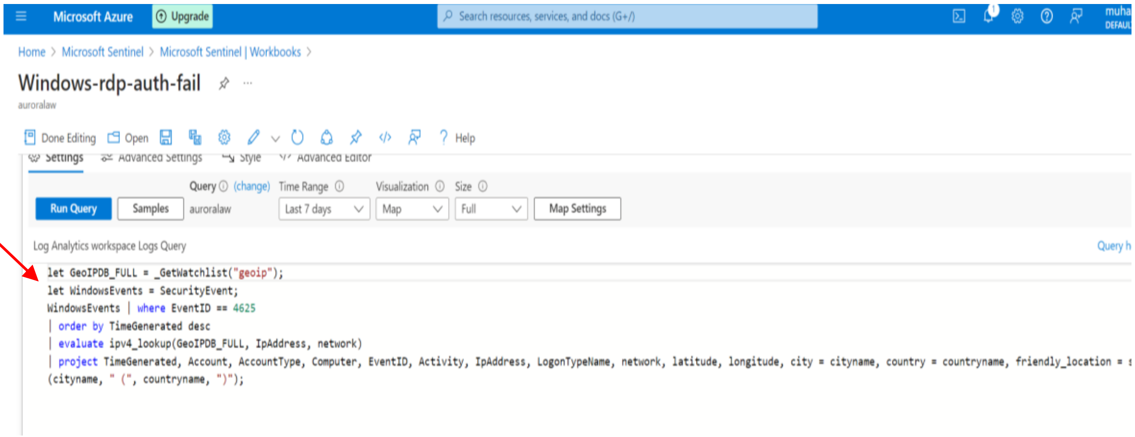
Auto-refresh incidents

Severity	Incident number	Title	Alerts	Incident provider na...	Alert produc
Medium	199	CUSTOM: Brute Force ATTEMPT - Linux Syslog	5	Azure Sentinel	Microsoft Ser
Medium	198	CUSTOM: Brute Force ATTEMPT - Linux Syslog	1	Azure Sentinel	Microsoft Ser
Medium	197	CUSTOM: Brute Force ATTEMPT - Linux Syslog	1	Azure Sentinel	Microsoft Ser
Medium	196	CUSTOM: Brute Force ATTEMPT - Linux Syslog	1	Azure Sentinel	Microsoft Ser
Medium	195	CUSTOM: Brute Force ATTEMPT - Linux Syslog	1	Azure Sentinel	Microsoft Ser
Medium	194	CUSTOM: Brute Force ATTEMPT - Linux Syslog	1	Azure Sentinel	Microsoft Ser
Medium	193	CUSTOM: Brute Force ATTEMPT - Linux Syslog	4	Azure Sentinel	Microsoft Ser
Medium	192	CUSTOM: Brute Force ATTEMPT - Linux Syslog	1	Azure Sentinel	Microsoft Ser
Medium	191	CUSTOM: Brute Force ATTEMPT - Linux Syslog	3	Azure Sentinel	Microsoft Ser

b) **Geolocation Mapping in Azure Sentinel**:

- Created three workbook queries to visualize and map the geolocation of adversaries:
  - **Nsg-malicious-allowed-in**: Monitored and visualized malicious traffic allowed through the network security group.
  - **linux-ssh-auth-fail**: Tracked and mapped failed SSH authentication attempts on Linux VMs.
  - **Windows-rdp-auth-fail**: Monitored and mapped failed RDP authentication attempts on Windows VMs.

Workbook Query



Windows-rdp-auth-fail

auroralaw

Query (change): auroralaw

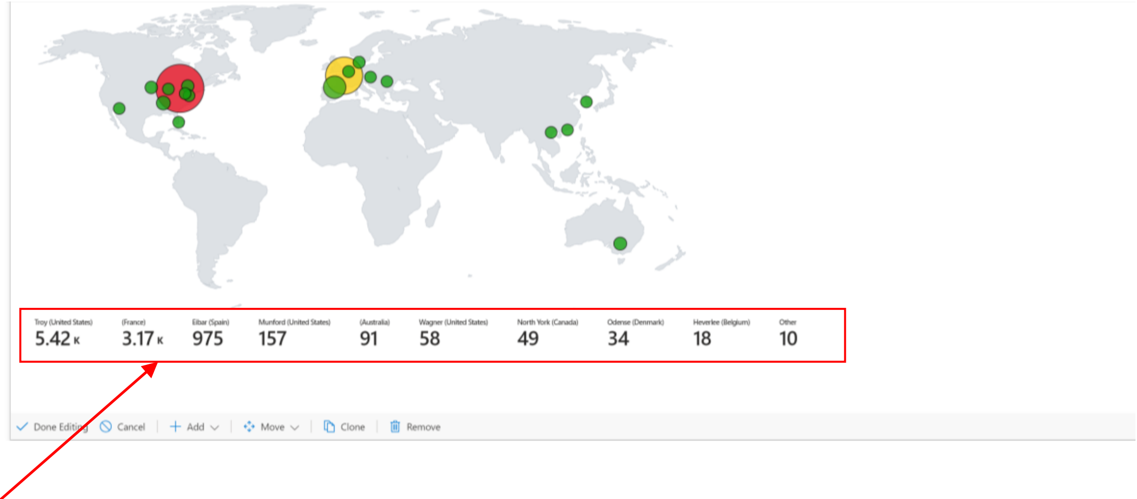
Time Range: Last 7 days

Visualization: Map

Size: Full

Log Analytics workspace Logs Query

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent;
WindowsEvents | where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)
| project TimeGenerated, Account, AccountType, Computer, EventID, Activity, IpAddress, LogonTypeName, network, latitude, longitude, city = cityname, country = countryname, friendly_location = s
(cityname, " (", countryname, ")");
```



Troy (United States)	(France)	Eibar (Spain)	Munford (United States)	(Australia)	Wagner (United States)	North York (Canada)	Odense (Denmark)	Heverlee (Belgium)	Other
5.42 K	3.17 K	975	157	91	58	49	34	18	10

Failed RDP Brute-force Attempts

3. Analytic Rules and Alerts

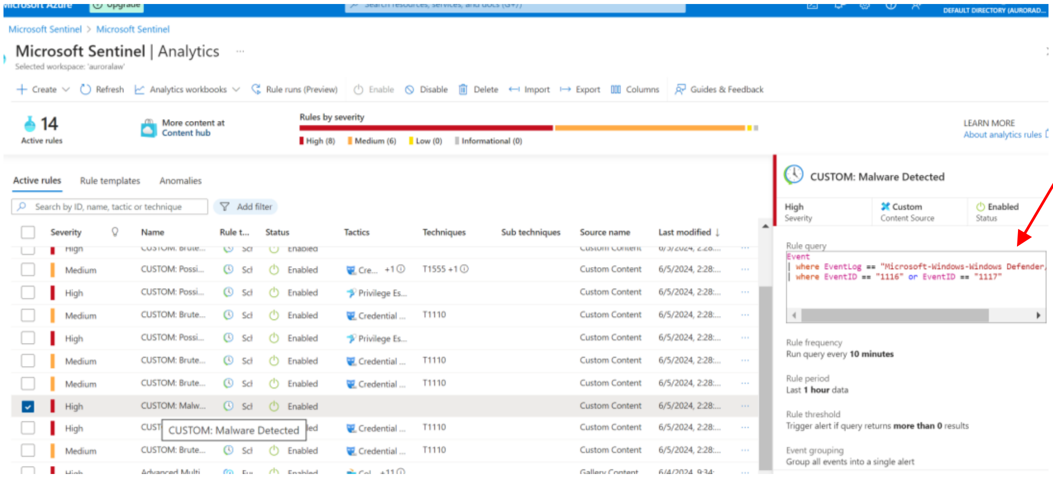
a) **Developed 14 Analytic Rules**:

- Created Kusto Query Language (KQL) rules to trigger alerts on suspicious activities.
- Focused on identifying brute force attempts, unusual login patterns, and potential malware activity.

b) **Example Analytic Rules**:

Malware Detection:

```
// Malware detected
SecurityEvent
| where EventLog == "Microsoft-Windows-Windows
Defender/Operational"
| where EventID == "1116" or EventID == "1117"
```



Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'auroralaw'

14 Active rules

More content at Content hub

Rules by severity: High (8) Medium (6) Low (0) Informational (0)

☐	Severity	Name	Rule t...	Status	Tactics	Techniques	Sub techniques	Source name	Last modified ↓	
☐	High	CUSTOM: Brute...	Sch	Enabled				Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Possi...	Sch	Enabled	Cre... +1	T1555 +1		Custom Content	6/5/2024, 2:28:...	···
☐	High	CUSTOM: Possi...	Sch	Enabled	Privilege Es...			Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Brute...	Sch	Enabled	Credential ...	T1110		Custom Content	6/5/2024, 2:28:...	···
☐	High	CUSTOM: Possi...	Sch	Enabled	Privilege Es...			Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Brute...	Sch	Enabled	Credential ...	T1110		Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Brute...	Sch	Enabled	Credential ...	T1110		Custom Content	6/5/2024, 2:28:...	···
☑	High	CUSTOM: Malw...	Sch	Enabled				Custom Content	6/5/2024, 2:28:...	···
☐	High	CUST CUSTOM: Malware Detected		...led	Credential ...	T1110		Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Brute...	Sch	Enabled	Credential ...	T1110		Custom Content	6/5/2024, 2:28:...	···
☐	High	Advanced Multi...	Fu...	Enabled	Col... +11			Gallery Content	6/4/2024, 9:34:...	···

CUSTOM: Malware Detected

High
Severity

Custom
Content Source

Enabled
Status

Rule query

```
Event
| where EventLog == "Microsoft-Windows-Windows Defender/
| where EventID == "1116" or EventID == "1117"
```

Rule frequency
Run query every **10 minutes**

Rule period
Last **1 hour** data

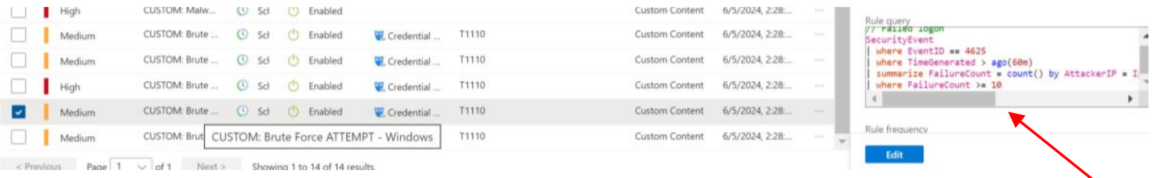
Rule threshold
Trigger alert if query returns **more than 0** results

Event grouping
Group all events into a single alert

Analytic Rule

RDP Brute Force Detection:

```
// Failed logon
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
|  summarize  FailureCount  =  count()  by  AttackerIP  =  IpAddress,
EventID, Activity, DestinationHostName = Computer
| where FailureCount >= 10
```



☐	Severity	Name	Rule t...	Status	Tactics	Techniques	Source name	Last modified	
☐	High	CUSTOM: Malw...	Sch	Enabled			Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Brute ...	Sch	Enabled	Credential ...	T1110	Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Brute ...	Sch	Enabled	Credential ...	T1110	Custom Content	6/5/2024, 2:28:...	···
☐	High	CUSTOM: Brute ...	Sch	Enabled	Credential ...	T1110	Custom Content	6/5/2024, 2:28:...	···
☑	Medium	CUSTOM: Brute ...	Sch	Enabled	Credential ...	T1110	Custom Content	6/5/2024, 2:28:...	···
☐	Medium	CUSTOM: Brut CUSTOM: Brute Force ATTEMPT - Windows				T1110	Custom Content	6/5/2024, 2:28:...	···

< Previous Page 1 of 1 Next > Showing 1 to 14 of 14 results.

Rule query

```
// Failed logon
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = I
| where FailureCount >= 10
```

Rule frequency

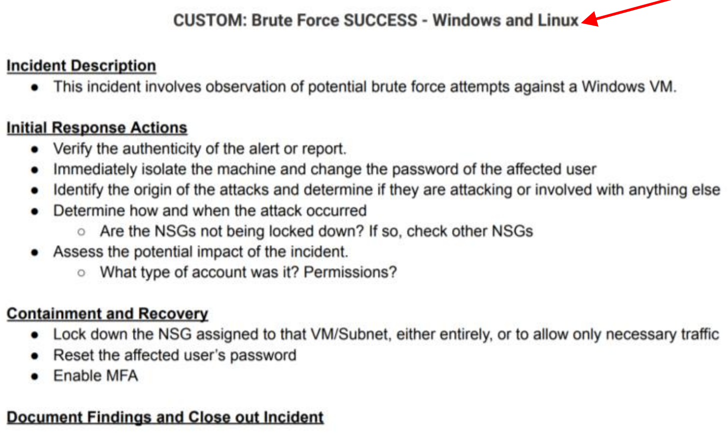
Analytic Rule

4. Incident Response Playbooks

a) **Developed Comprehensive Playbooks**:
   - Created automated response playbooks for different types of incidents:
     - **Brute Force Attempt**: Blocked IP addresses after a certain number of failed attempts.
     - **Malware Detected**: Quarantined affected machines and alerted the security team.

b) **Example Playbook Actions**:
   - **Brute Force Response**:
     - Triggered on detection of multiple failed login attempts.
     - Automatically added the attacking IP to a blocklist.

Playbook



CUSTOM: Brute Force SUCCESS - Windows and Linux

Incident Description
- This incident involves observation of potential brute force attempts against a Windows VM.

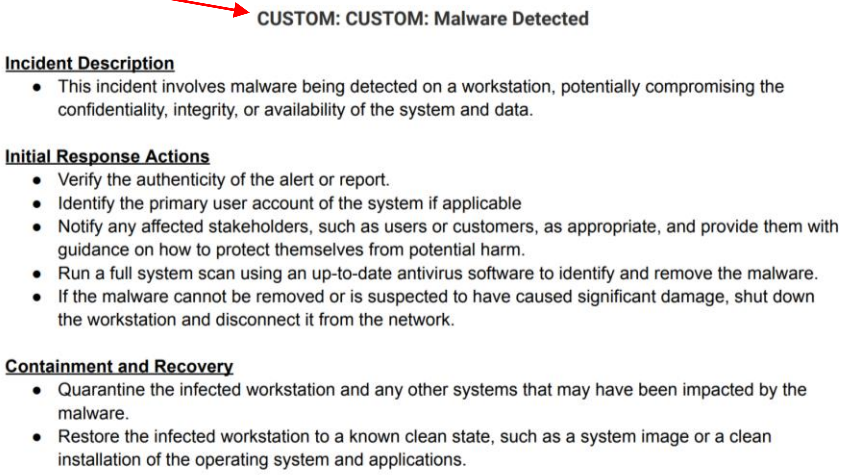
Initial Response Actions
- Verify the authenticity of the alert or report.
- Immediately isolate the machine and change the password of the affected user
- Identify the origin of the attacks and determine if they are attacking or involved with anything else
- Determine how and when the attack occurred
  - Are the NSGs not being locked down? If so, check other NSGs
- Assess the potential impact of the incident.
  - What type of account was it? Permissions?

Containment and Recovery
- Lock down the NSG assigned to that VM/Subnet, either entirely, or to allow only necessary traffic
- Reset the affected user's password
- Enable MFA

Document Findings and Close out Incident

   - **Malware Response**:
     - Triggered on detection of malware signatures.
     - Isolated the infected VM and initiated an automated malware scan.

Playbook



CUSTOM: CUSTOM: Malware Detected

Incident Description
- This incident involves malware being detected on a workstation, potentially compromising the confidentiality, integrity, or availability of the system and data.

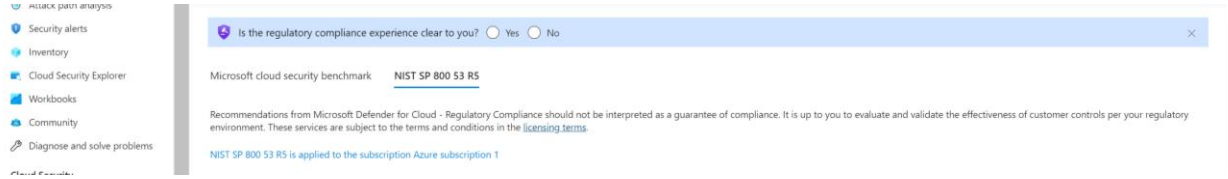
Initial Response Actions
- Verify the authenticity of the alert or report.
- Identify the primary user account of the system if applicable
- Notify any affected stakeholders, such as users or customers, as appropriate, and provide them with guidance on how to protect themselves from potential harm.
- Run a full system scan using an up-to-date antivirus software to identify and remove the malware.
- If the malware cannot be removed or is suspected to have caused significant damage, shut down the workstation and disconnect it from the network.

Containment and Recovery
- Quarantine the infected workstation and any other systems that may have been impacted by the malware.
- Restore the infected workstation to a known clean state, such as a system image or a clean installation of the operating system and applications.

5. Securing the Environment

a) **Implemented NIST 800-53 SC-7 (Boundary Protection)**:

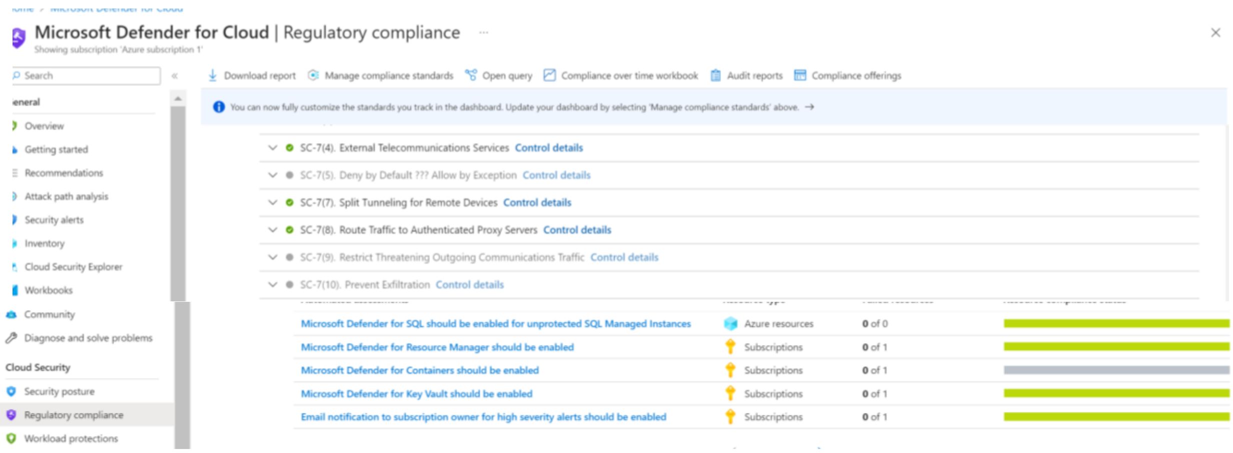
- Strengthened firewall rules to limit access only to trusted sources.
- Configured network security groups to enforce strict ingress and egress controls.



Is the regulatory compliance experience clear to you? ○ Yes ○ No

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the licensing terms.

NIST SP 800 53 R5 is applied to the subscription Azure subscription 1



Microsoft Defender for Cloud | Regulatory compliance

Showing subscription 'Azure subscription 1'

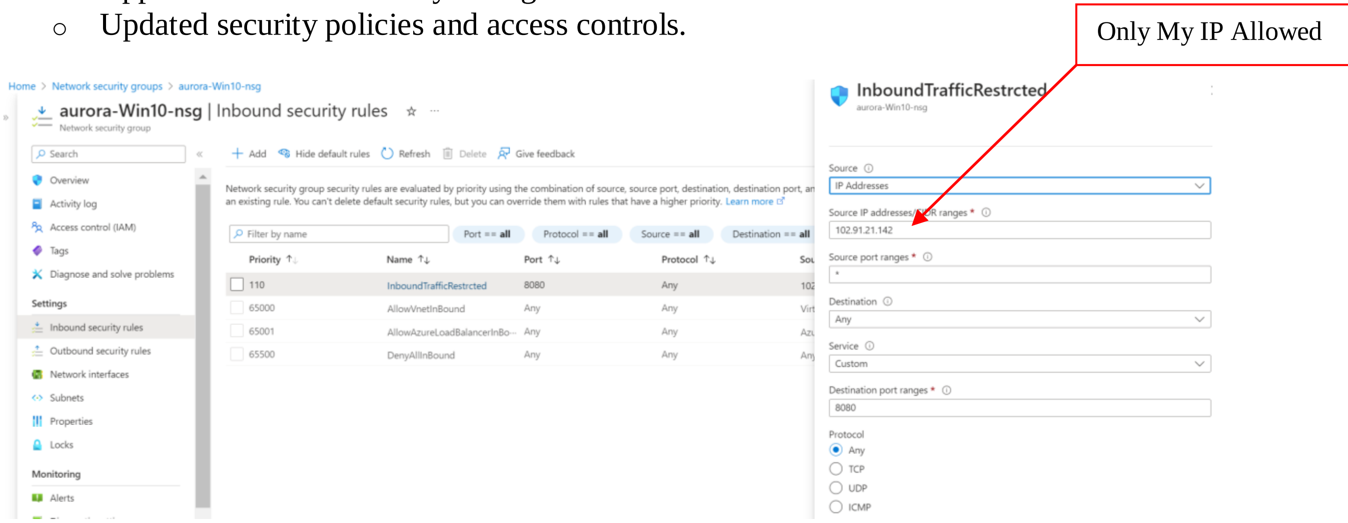
You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance standards' above. →

- SC-7(4). External Telecommunications Services Control details
- SC-7(5). Deny by Default ??? Allow by Exception Control details
- SC-7(7). Split Tunneling for Remote Devices Control details
- SC-7(8). Route Traffic to Authenticated Proxy Servers Control details
- SC-7(9). Restrict Threatening Outgoing Communications Traffic Control details
- SC-7(10). Prevent Exfiltration Control details

Microsoft Defender for SQL should be enabled for unprotected SQL Managed Instances	Azure resources	0 of 0	🟩
Microsoft Defender for Resource Manager should be enabled	Subscriptions	0 of 1	🟩
Microsoft Defender for Containers should be enabled	Subscriptions	0 of 1	▨
Microsoft Defender for Key Vault should be enabled	Subscriptions	0 of 1	🟩
Email notification to subscription owner for high severity alerts should be enabled	Subscriptions	0 of 1	🟩

b) **Tightened Security on Resources and VMs**:

- Applied additional security configurations to harden VMs.
- Updated security policies and access controls.



Only My IP Allowed

aurora-Win10-nsg | Inbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, an an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Priority	Name	Port	Protocol	Sou
110	InboundTrafficRestrcted	8080	Any	102
65000	AllowVnetInBound	Any	Any	Virt
65001	AllowAzureLoadBalancerInBo…	Any	Any	Azu
65500	DenyAllInBound	Any	Any	Any

InboundTrafficRestrcted

aurora-Win10-nsg

Source: IP Addresses

Source IP addresses/CIDR ranges *: 102.91.21.142

Source port ranges *: *

Destination: Any

Service: Custom

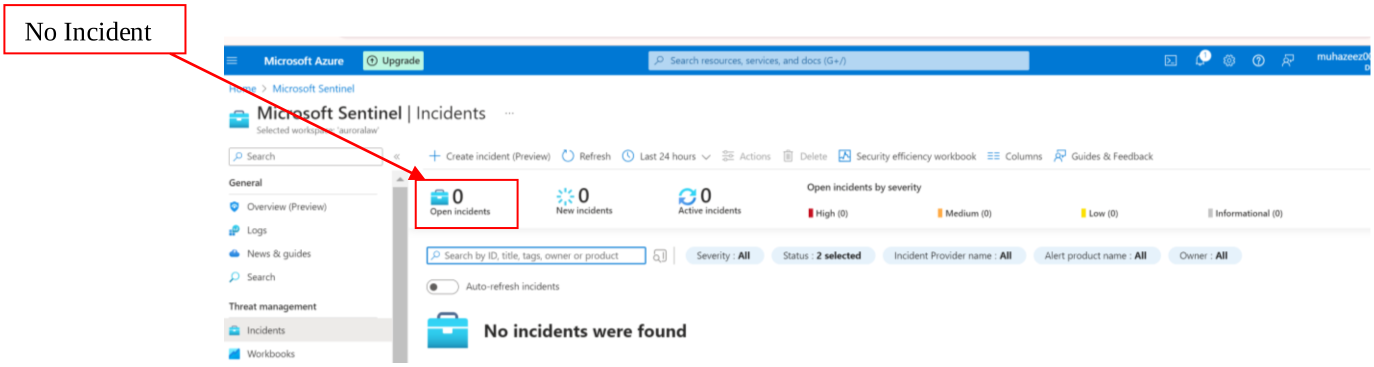
Destination port ranges *: 8080

Protocol: ● Any ○ TCP ○ UDP ○ ICMP

6. Verification and Final Assessment

a) **24-Hour Monitoring**:

- ○ Left the secured environment for an additional 24 hours to test and verify the security posture.
- ○ Monitored for any incidents or security breaches.


No Incident

Microsoft Sentinel | Incidents

Selected workspace: 'auroralaw'

0 Open incidents

0 New incidents

0 Active incidents

Open incidents by severity: High (0) Medium (0) Low (0) Informational (0)

Severity : **All** Status : **2 selected** Incident Provider name : **All** Alert product name : **All** Owner : **All**

No incidents were found

b) **Final Compliance Check**:

- ○ Achieved 100% compliance with no incidents recorded after the final security measures were implemented.
- ○ Confirmed that the environment was secure and resilient against the previously observed threats.

Key Skills and Expertise

- **Threat Detection and Analysis**: Proficient in using SIEM tools, such as Azure Sentinel, for monitoring and analyzing security events to identify potential threats.
- **Incident Response**: Experienced in developing and executing incident response playbooks to effectively manage and mitigate security incidents.
- **Security Operations**: Skilled in the day-to-day operations of a SOC, including log analysis, intrusion detection, and vulnerability management.
- **Network Security**: Knowledgeable in configuring and managing firewall rules, intrusion prevention systems, and other network security controls.
- **Cloud Security**: Familiar with securing cloud environments, particularly Azure, and implementing security measures in line with industry standards such as NIST 800-53.

Achievements

- Successfully deployed a honeypot in the cloud, attracting and analyzing brute force attacks and mapping adversary locations using Azure Sentinel's geolocation features.
- Created multiple workbook queries (Nsg-malicious-allowed-in, linux-ssh-auth-fail, Windows-rdp-auth-fail) to visualize and track malicious activities.
- Developed 14 analytic rules using Kusto Query Language (KQL) to trigger alerts on suspicious activities, enhancing the organization's threat detection capabilities.
- Designed and implemented comprehensive incident response playbooks to respond to various types of security incidents, including brute force attempts and malware detections.

- Achieved 100% compliance with zero incidents recorded after implementing NIST 800-53 SC-7 (Boundary Protection) and testing the security posture for 24 hours.

Conclusion

- This project demonstrated the effectiveness of using Azure Sentinel for threat detection and incident response. By deploying a honeypot, monitoring for malicious activity, creating analytic rules, and developing automated response playbooks, we were able to enhance the security posture significantly. Implementing NIST 800-53 SC-7 ensured robust boundary protection, resulting in zero incidents during the final compliance check. This marks the successful completion of the Threat Detection and Incident Response Project using Azure Sentinel

THANK YOU
ABDULAZEEZ MOHAMMED