Lab #16: **Perform Incident Handling (Utilize NIST 800-61)**

Purpose:

- We'll now perform incident response. We've generated plenty of incident alerts after exposing our lab environment to malicious traffice for 24 hours.
- We'll be hardening our environment once we start the **Containment, Eradication, and Recovery** phase of Incident Response (IR).
- We'll advise the incidents in accordance with NIST SP 800-61 (Incident Management Lifecycle).

Tasks:

1. **Incident Response #1 - Brute Force Success (Windows)**
   - Preparation
   - Detection & Analysis
   - Containment, Eradication, and Recovery
   - Document Findings (Including Root Cause)
2. **Incident Response #2 - Possible Privilege Escalation**
   - Preparation
   - Detection & Analysis
   - Containment, Eradication, and Recovery
   - Document Findings (Including Root Cause)
3. **Incident Response #3 - Brute Force Success (Linux)**
   - Preparation
   - Detection & Analysis
   - Containment, Eradication, and Recovery
   - Document Findings (Including Root Cause)
4. **Incident Response #4 - Possible Malware Outbreak**
   - Preparation
   - Detection & Analysis
   - Containment, Eradication, and Recovery
   - Document Findings (Including Root Cause)

Task 1: **Incident Response #1 - Brute Force Success (Windows)**

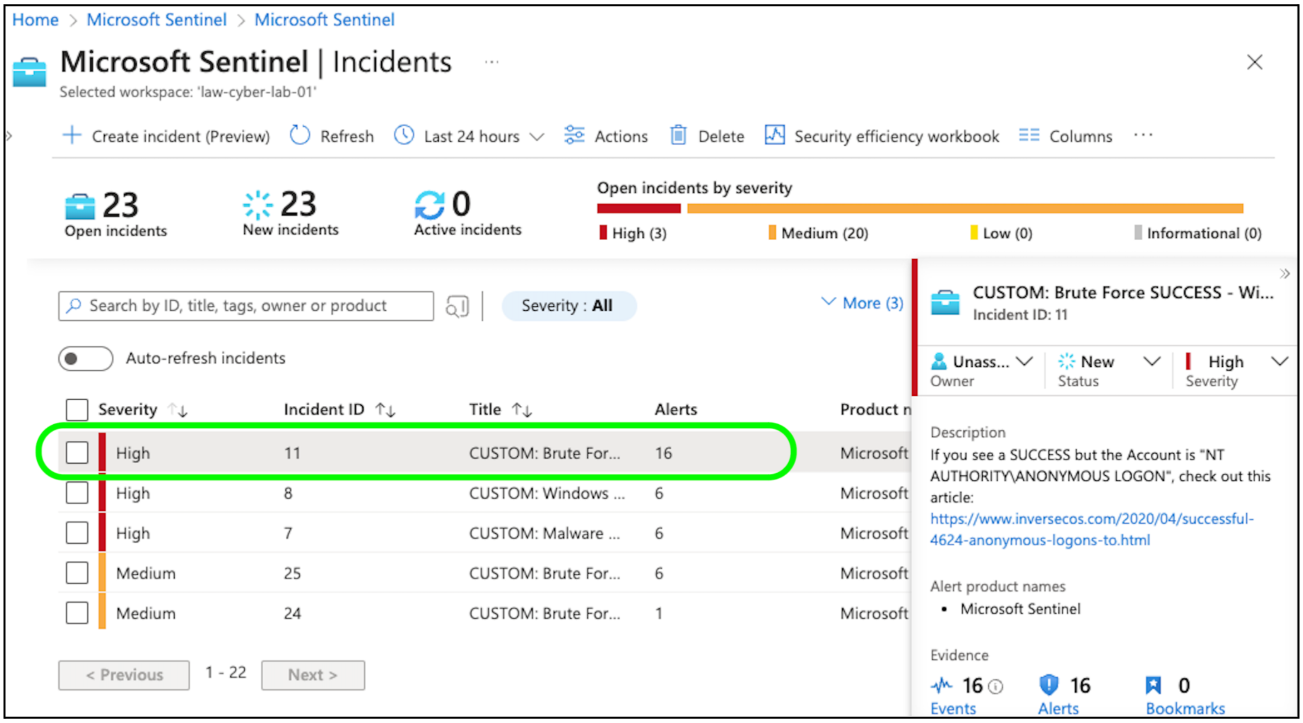
Preparation:

***Note**: We already completed this IR phase. We've previously set up logs to be ingested into our Log Analytics workspace. We also configured alert rules in Sentinel.*

Detection & Analysis:

1. **Azure** portal > **Sentinel** > **Incidents** > order the incidents by **Severity** >

2. Select top incident.



Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'law-cyber-lab-01'

23 Open incidents

23 New incidents

0 Active incidents

Open incidents by severity

High (3) Medium (20) Low (0) Informational (0)

Search by ID, title, tags, owner or product

Severity : All

More (3)

Auto-refresh incidents

□	Severity	Incident ID	Title	Alerts	Product n
□	High	11	CUSTOM: Brute For...	16	Microsoft
□	High	8	CUSTOM: Windows ...	6	Microsoft
□	High	7	CUSTOM: Malware ...	6	Microsoft
□	Medium	25	CUSTOM: Brute For...	6	Microsoft
□	Medium	24	CUSTOM: Brute For...	1	Microsoft

< Previous 1 - 22 Next >

CUSTOM: Brute Force SUCCESS - Wi...

Incident ID: 11

Unass... Owner | New Status | High Severity

Description

If you see a SUCCESS but the Account is "NT AUTHORITY\ANONYMOUS LOGON", check out this article: https://www.inversecos.com/2020/04/successful-4624-anonymous-logons-to.html

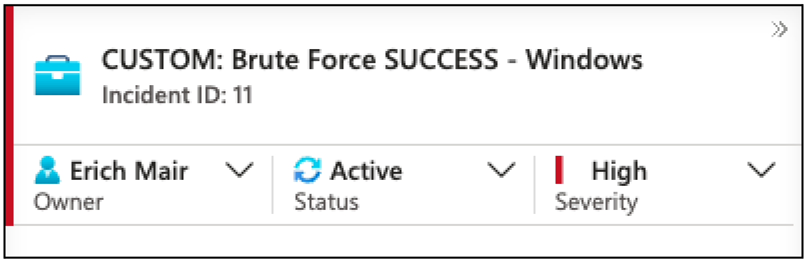
Alert product names

- Microsoft Sentinel

Evidence

16 Events | 16 Alerts | 0 Bookmarks

3. Set the **Severity**, **Status**, and **Owner** for the incident.

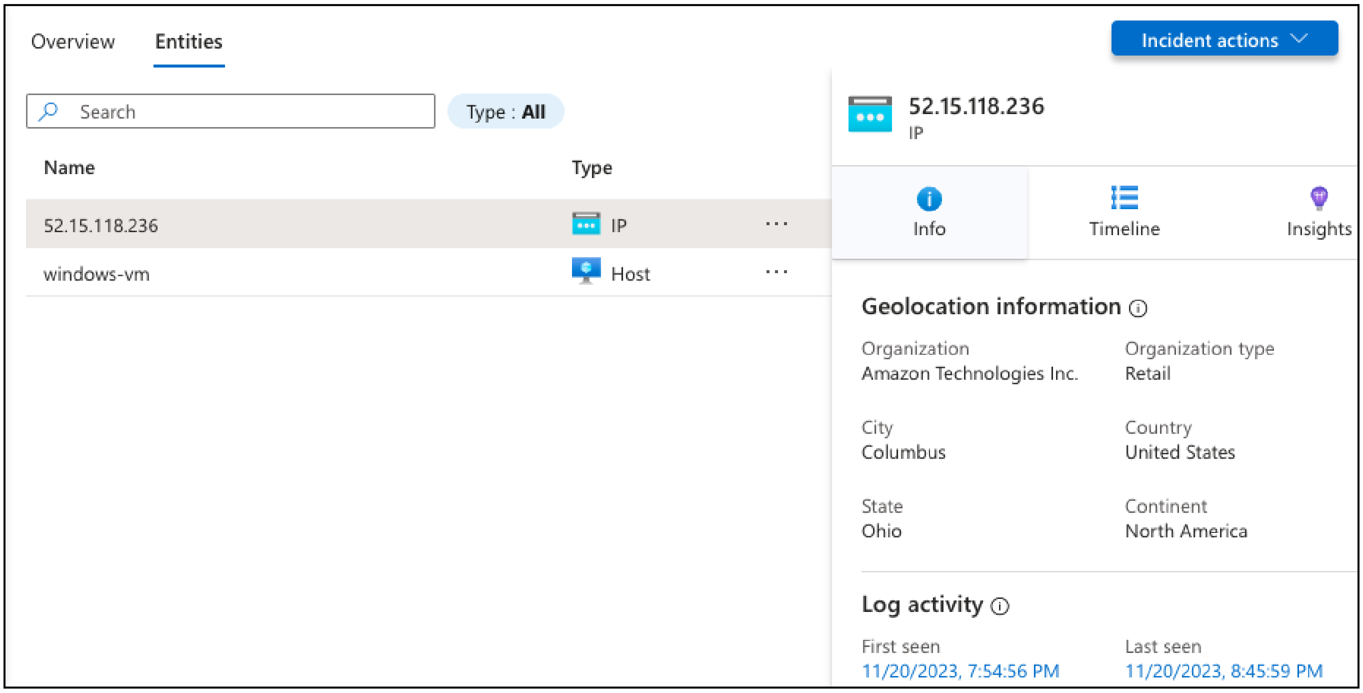


CUSTOM: Brute Force SUCCESS - Windows

Incident ID: 11

Erich Mair Owner | Active Status | High Severity

4. Select **View Full Details**.
5. Observe the Activity Log (view history of the incident)
6. Observe Entities and Incident Timelines. We see the attacker who was performing brute force attempts.



Name	Type
52.15.118.236	IP
windows-vm	Host

52.15.118.236

IP

Geolocation information

Organization: Amazon Technologies Inc.

Organization type: Retail

City: Columbus

Country: United States

State: Ohio

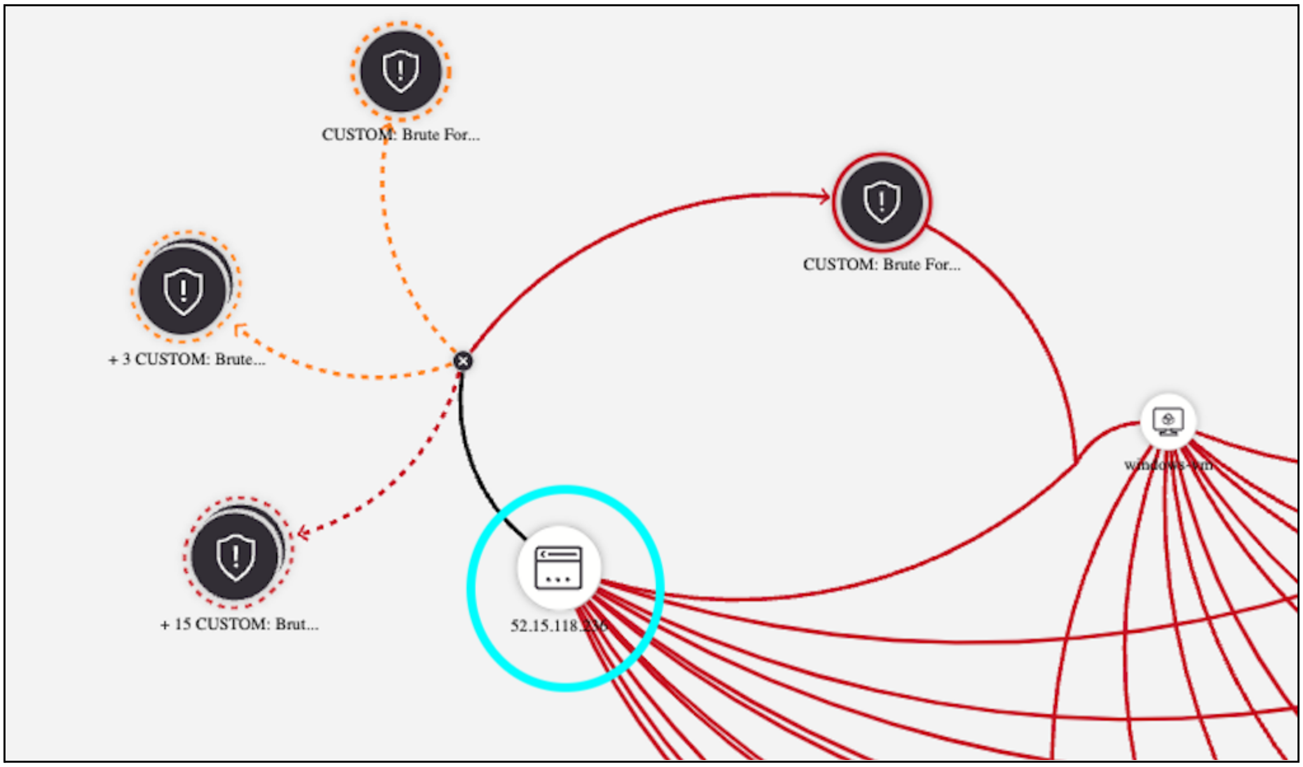
Continent: North America

Log activity

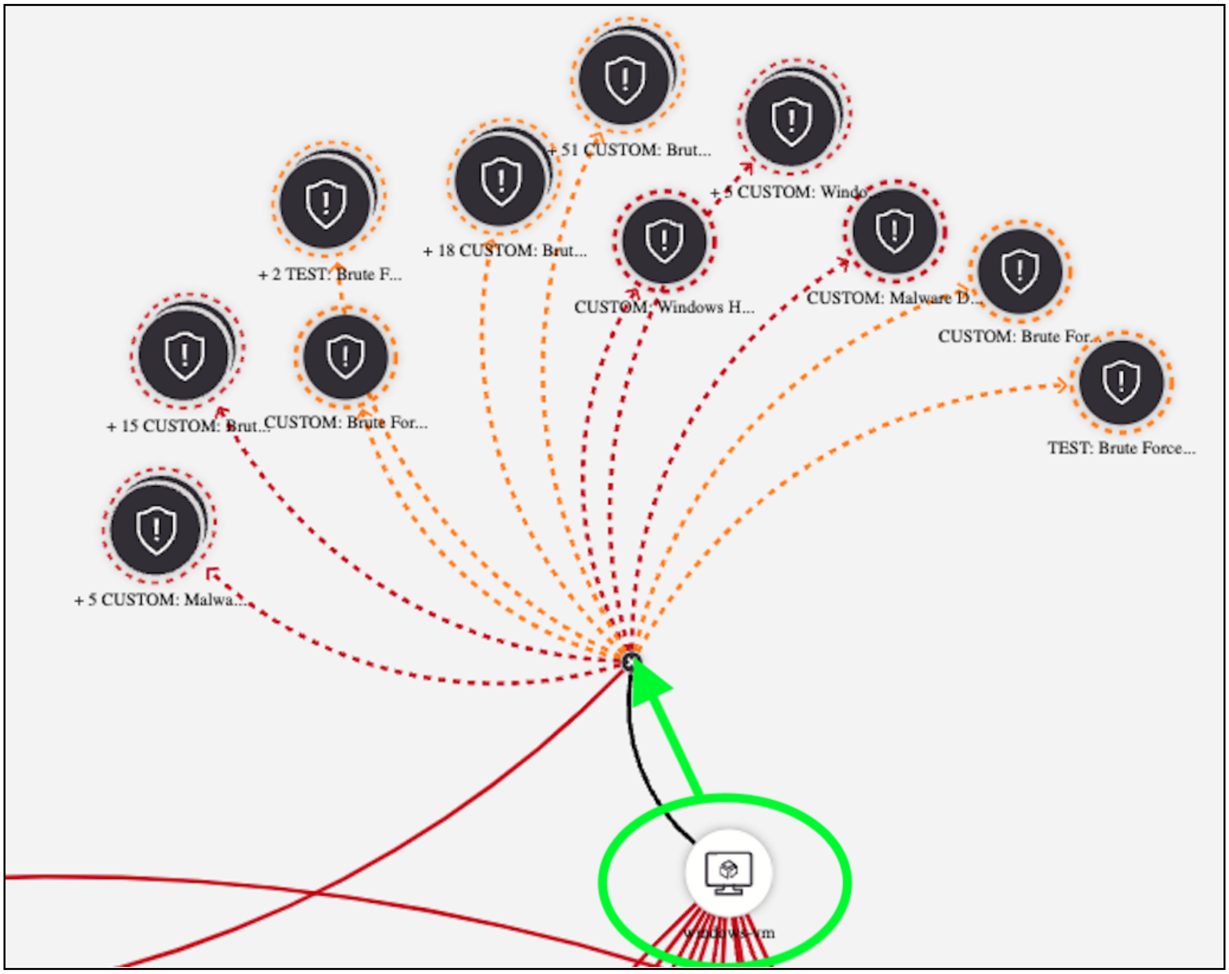
First seen: 11/20/2023, 7:54:56 PM

Last seen: 11/20/2023, 8:45:59 PM

7. Select **Investigate** to further investigate the incident.

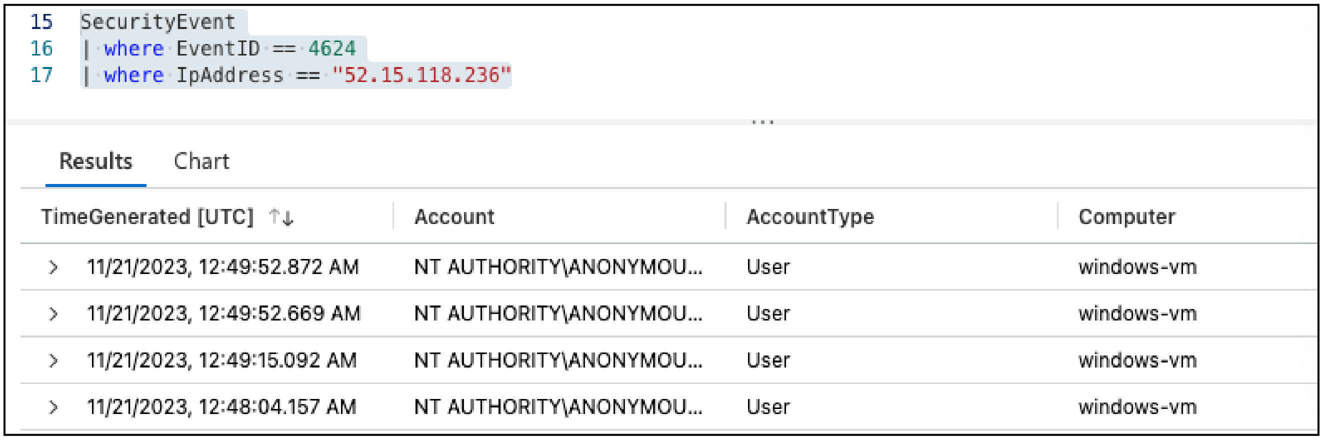


***Note**: "We see that this attacker entity was involved in other brute force attempts and successes."*



> ***Note**: "We see that the windows-vm was involved in other incidents. We should inspect why so many alerts were generated (because it's purposefully over-exposed to the internet)."*

8. Determine the legitimacy of the incident (True Positive, False Positive, etc.).
    a. Go to Log Analytics workspace > Run this query to analyze the attacker IP:
    SecurityEvent | where EventID == 4624 | where IpAddress == "52.15.118.236"



```
SecurityEvent
| where EventID == 4624
| where IpAddress == "52.15.118.236"
```

TimeGenerated [UTC] ↑↓	Account	AccountType	Computer
› 11/21/2023, 12:49:52.872 AM	NT AUTHORITY\ANONYMOU...	User	windows-vm
› 11/21/2023, 12:49:52.669 AM	NT AUTHORITY\ANONYMOU...	User	windows-vm
› 11/21/2023, 12:49:15.092 AM	NT AUTHORITY\ANONYMOU...	User	windows-vm
› 11/21/2023, 12:48:04.157 AM	NT AUTHORITY\ANONYMOU...	User	windows-vm

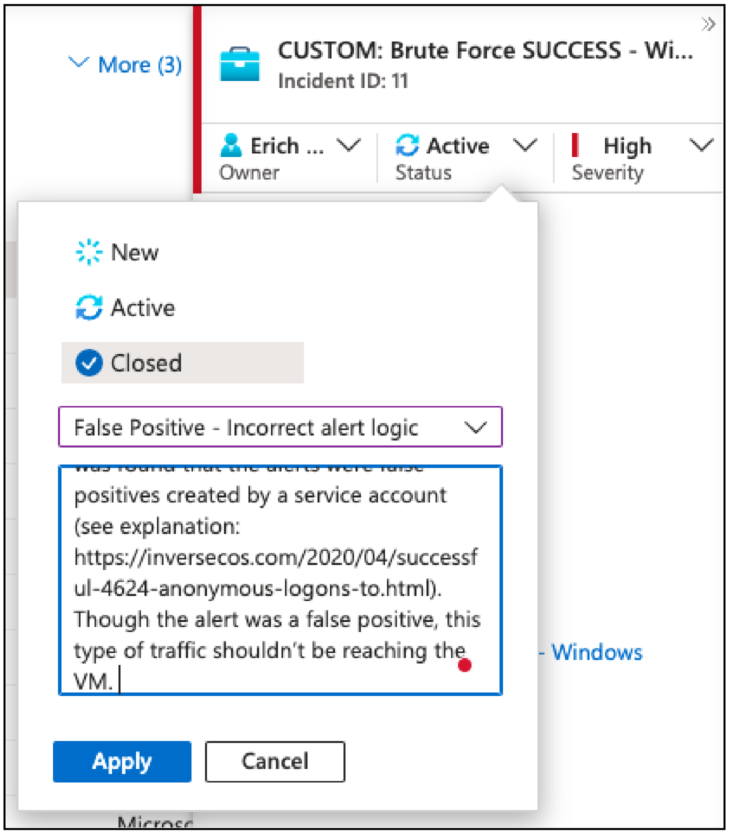
> ***Note**: "It initially seemed like an attacker successfully brute-forced via utilizing SMB. But upon further investigation it was found that the alerts were **false positives** created by a service account (see explanation: https://inversecos.com/2020/04/successful-4624-anonymous-logons-to.html). Though the alert was a false positive, this type of traffic shouldn't be reaching the VM."*

Containment, Eradication, and Recovery:

1. Per the "Incident Response PlayBook", we'll lock down the NSGs:
    a. Edit the "DANGER_AllowAnyCustomAnyInbound" inbound rule to only allow one IP (our IP).
    b. Delete the rule that allows inbound RDP.

Document Findings (Including Root Cause):

1. Documented the findings of the incident and labeled it as a "False Positive". Closed the incident.



CUSTOM: Brute Force SUCCESS - Wi...
Incident ID: 11

Owner: Erich ...
Status: Active
Severity: High

New
Active
Closed

False Positive - Incorrect alert logic

was found that the alerts were false positives created by a service account (see explanation: https://inversecos.com/2020/04/successful-4624-anonymous-logons-to.html). Though the alert was a false positive, this type of traffic shouldn't be reaching the VM.

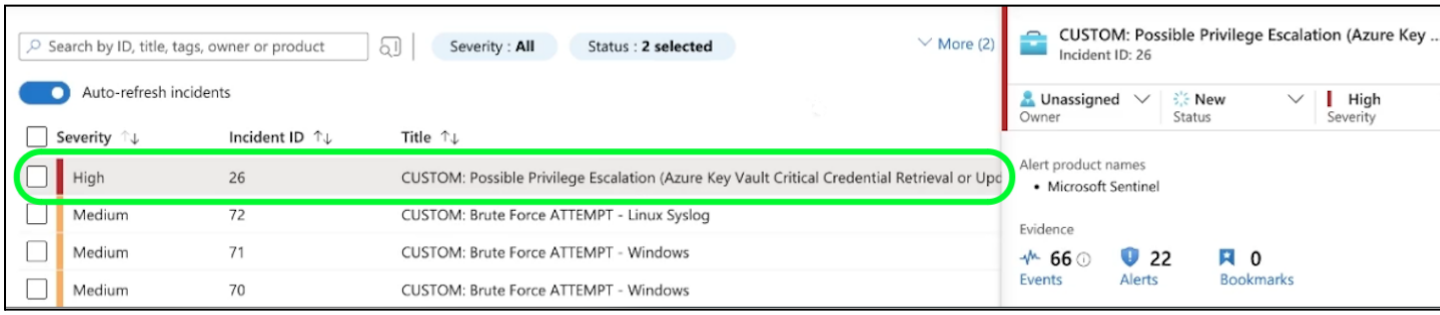
Task 2: Incident Response #2 - Possible Privilege Escalation

Preparation:

***Note**: We already completed this IR phase. We've previously set up logs to be ingested into our Log Analytics workspace. We also configured alert rules in Sentinel.*

Detection & Analysis:

1. **Azure** portal > **Sentinel** > **Incidents** > order the incidents by **Severity** >
2. Select the **Possible Privilege Escalation** alert.



Severity	Incident ID	Title
High	26	CUSTOM: Possible Privilege Escalation (Azure Key Vault Critical Credential Retrieval or Upd
Medium	72	CUSTOM: Brute Force ATTEMPT - Linux Syslog
Medium	71	CUSTOM: Brute Force ATTEMPT - Windows
Medium	70	CUSTOM: Brute Force ATTEMPT - Windows

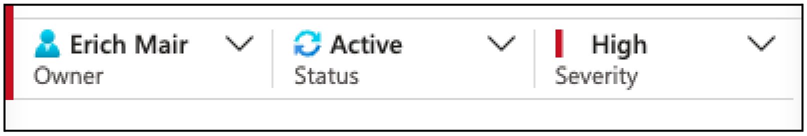
CUSTOM: Possible Privilege Escalation (Azure Key ..
Incident ID: 26

Owner: Unassigned
Status: New
Severity: High

Alert product names
- Microsoft Sentinel

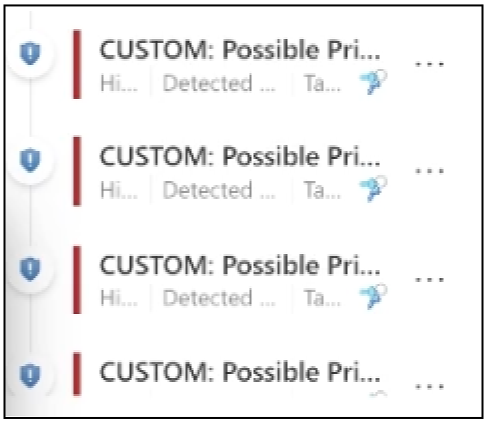
Evidence
66 Events
22 Alerts
0 Bookmarks

3. Set the **Severity**, **Status**, and **Owner** for the incident.



Owner: Erich Mair
Status: Active
Severity: High

4. Select **View Full Details**.
5. We see many alerts triggered for this incident. Let's start writing our notes.



CUSTOM: Possible Pri...
Hi... | Detected ... | Ta...

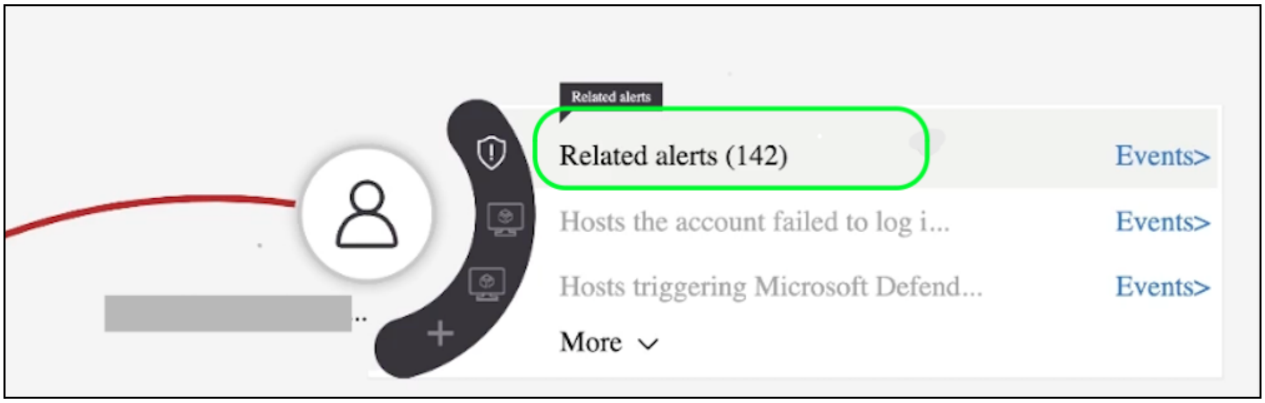
CUSTOM: Possible Pri...
Hi... | Detected ... | Ta...

CUSTOM: Possible Pri...
Hi... | Detected ... | Ta...

CUSTOM: Possible Pri...

***Note**: "Several alerts were triggered by a user (NAME, EMAIL) who viewed a secret (critical credentials) many times. It seems like possible suspicious behavior. Need to investigate further…"*

6. Select **Investigate** to inspect it further > select the **Entity** and view the **Related Alerts**



Related alerts (142) Events>

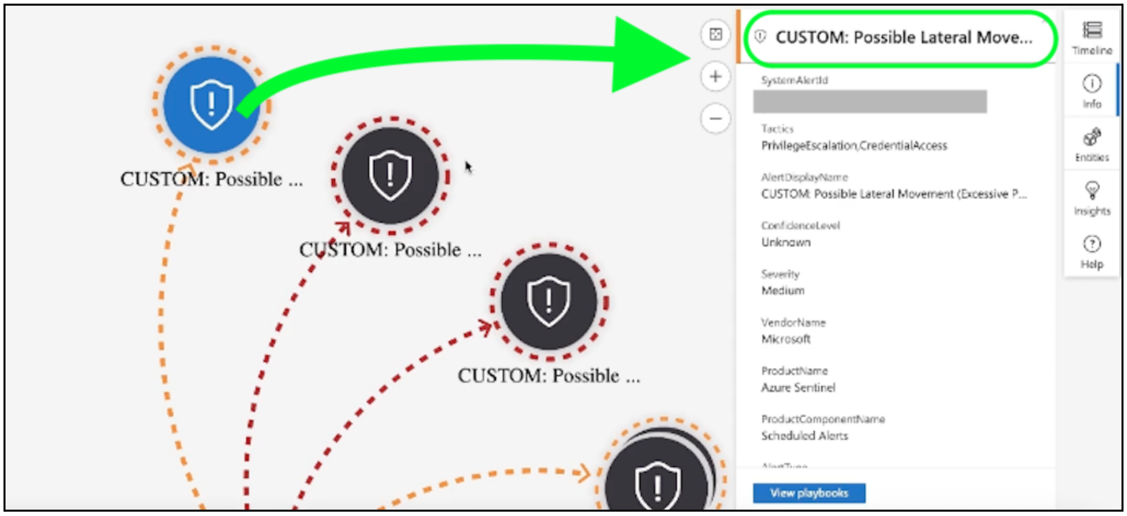
Hosts the account failed to log i... Events>

Hosts triggering Microsoft Defend... Events>

More

[redacted]

7. We see that this entity has triggered a **Possible Lateral Movement** alert as well.



CUSTOM: Possible Lateral Move...

SystemAlertId
[redacted]

Tactics
PrivilegeEscalation,CredentialAccess

AlertDisplayName
CUSTOM: Possible Lateral Movement (Excessive P...

ConfidenceLevel
Unknown

Severity
Medium

VendorName
Microsoft

ProductName
Azure Sentinel

ProductComponentName
Scheduled Alerts

a. Add more notes to our documentation:

> ***Note***: *"…It's an internal user that viewed critical credentials many times, and they were also involved in other incidents including **Excessive Password Resets** and **Global Admin Role Assignment**…"*

8. Determine the legitimacy of the incident by reaching out to the user and their supervisor.

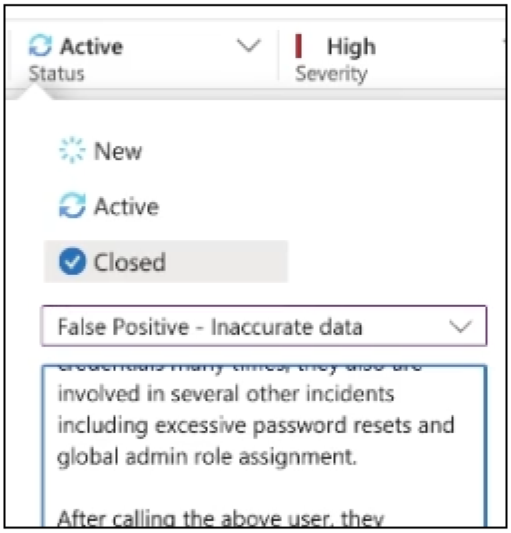
> ***Note***: *"…After contacting the user's supervisor directly, and discussing with the user, it's confirmed that their actions were legitimate and non-malicious. Closing out this incident as a **False Positive**. "*

Containment, Eradication, and Recovery:

1. N/A

Document Findings (Including Root Cause):

1. Document the findings of the incident and labeled it as a "False Positive". Close the incident.



Active
Status

High
Severity

New

Active

Closed

False Positive - Inaccurate data

credentials many times, they also are involved in several other incidents including excessive password resets and global admin role assignment.

After calling the above user, they

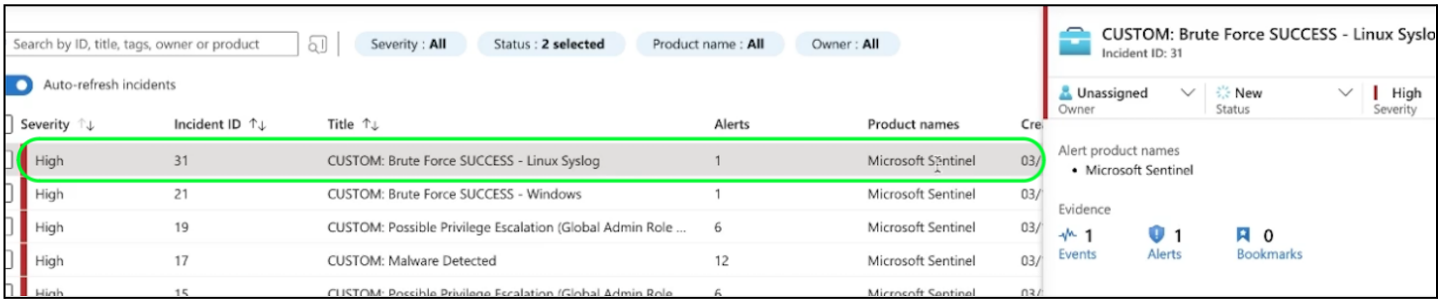
Task 3: Incident Response #3 - Brute Force Success (Linux)

Preparation:

***Note**: We already completed this IR phase. We've previously set up logs to be ingested into our Log Analytics workspace. We also configured alert rules in Sentinel.*

Detection & Analysis:

1. **Azure** portal > **Sentinel** > **Incidents** > order the incidents by **Severity** >
2. Select the **Linux Brute Force Success** alert.



Search by ID, title, tags, owner or product | Severity : **All** | Status : **2 selected** | Product name : **All** | Owner : **All**

Auto-refresh incidents

Severity ↑↓	Incident ID ↑↓	Title ↑↓	Alerts	Product names	Cre
High	31	CUSTOM: Brute Force SUCCESS - Linux Syslog	1	Microsoft Sentinel	03/
High	21	CUSTOM: Brute Force SUCCESS - Windows	1	Microsoft Sentinel	03/
High	19	CUSTOM: Possible Privilege Escalation (Global Admin Role ...	6	Microsoft Sentinel	03/
High	17	CUSTOM: Malware Detected	12	Microsoft Sentinel	03/
High	15	CUSTOM: Possible Privilege Escalation (Global Admin Role	6	Microsoft Sentinel	03/

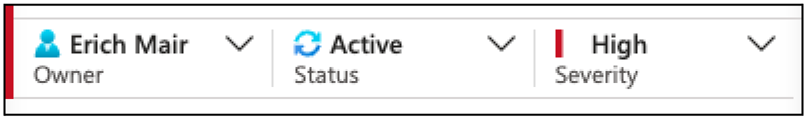
CUSTOM: Brute Force SUCCESS - Linux Syslo
Incident ID: 31

Owner: Unassigned | Status: New | Severity: High

Alert product names
- Microsoft Sentinel

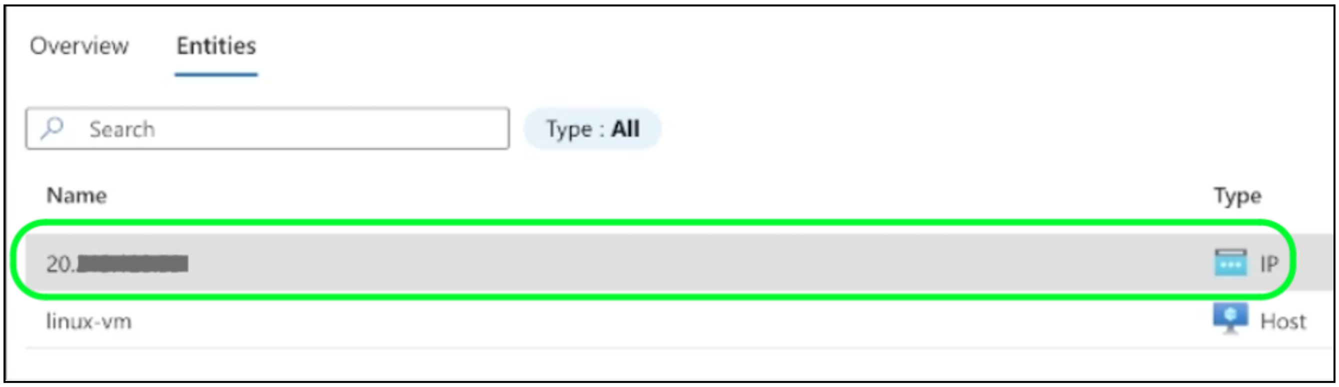
Evidence
1 Events | 1 Alerts | 0 Bookmarks

3. Set the **Severity**, **Status**, and **Owner** for the incident.

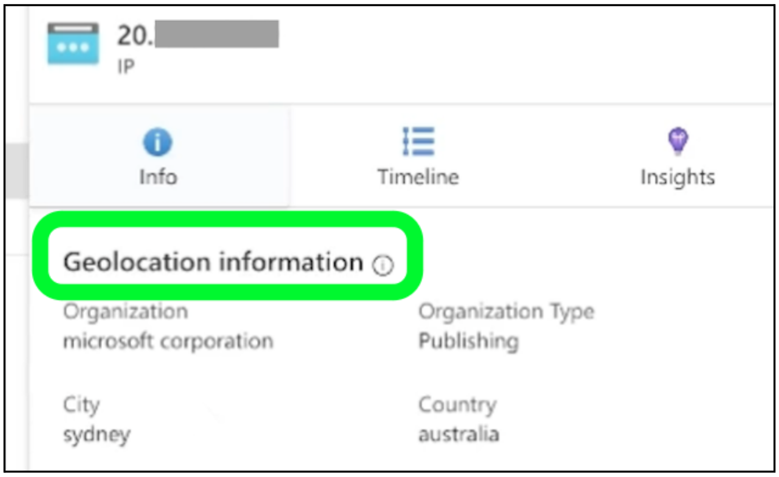


Owner: Erich Mair | Status: Active | Severity: High

4. Select **View Full Details**.
5. We see the entity that triggered this alert (our attack-vm, located in a different country).



Name	Type
20.[redacted]	IP
linux-vm	Host

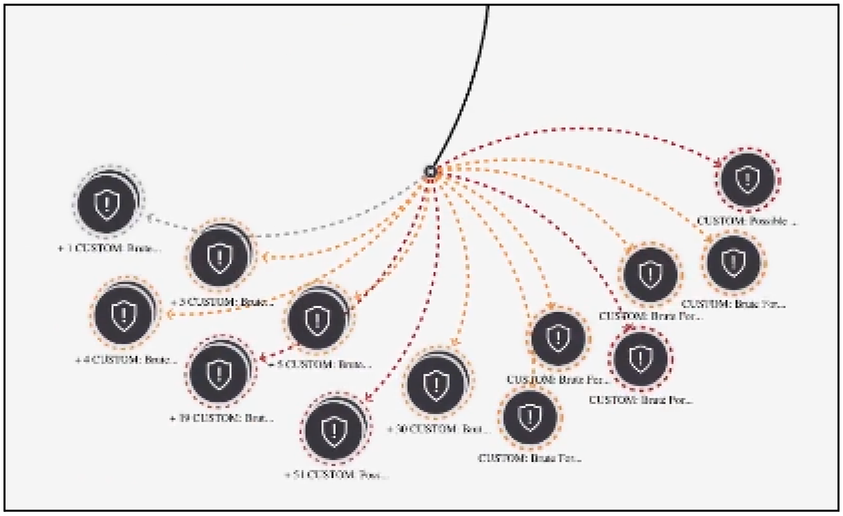


20.[redacted]
IP

Geolocation information

Organization microsoft corporation	Organization Type Publishing
City sydney	Country australia

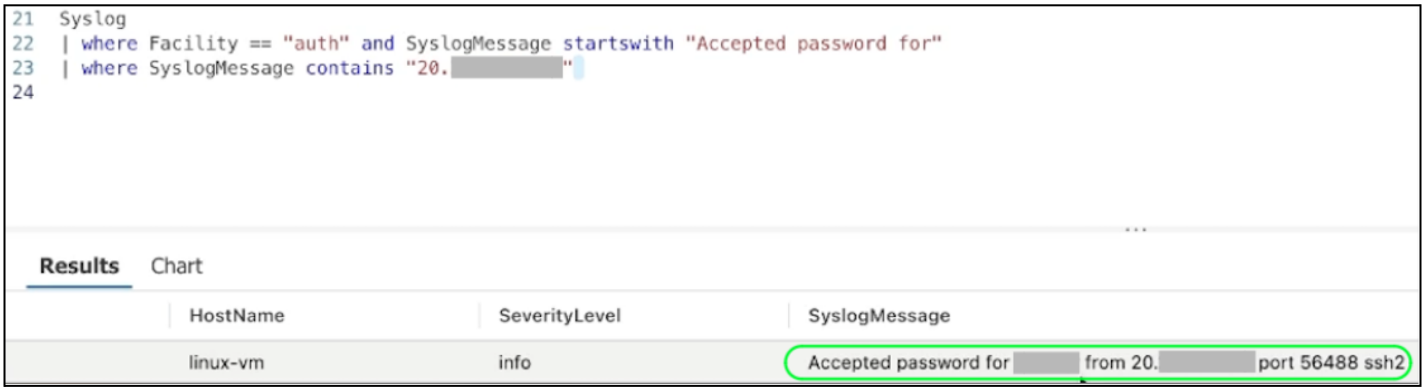
6. Select **Investigate** to see other events that originated from this attacker/entity.



   a. Let's start writing our notes.

   > ***Note***: *"Attacker at [IP Address] was involved with several other incidents that triggered alerts. Need to investigate further…"*

7. Went to Logs Analytics workspace to investigate the malicious IP further. We confirmed that the IP did make a successful connection to our linux-vm.



```
Syslog
| where Facility == "auth" and SyslogMessage startswith "Accepted password for"
| where SyslogMessage contains "20.[redacted]"
```

HostName	SeverityLevel	SyslogMessage
linux-vm	info	Accepted password for [redacted] from 20.[redacted] port 56488 ssh2

> ***Note***: *(I'm pretending that this was a malicious IP that connected to our linux-vm) "The malicous IP (IP Address) did successfully connect to linux-vm. This is a* ***True Positive****. Need to perform containment and remediation steps…"*

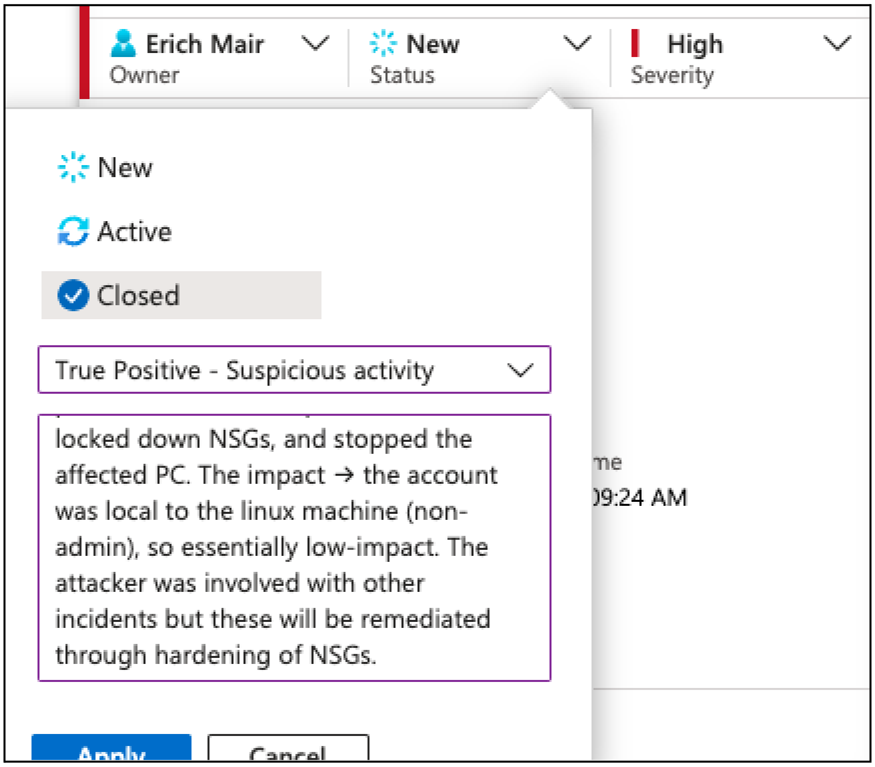
Containment, Eradication, and Recovery:

1. Per the "Incident Response PlayBook", we'll perform these steps:
   a. Stopped the affected PC
   b. Reset the account's password
   c. Hardened the NSG (we already performed this though)

> ***Note***: *"…Remediated by resetting account password for the compromised user, locked down NSGs, and stopped the affected PC. The impact → the account was local to the linux machine (non-admin), so essentially low-impact. The attacker was involved with other incidents but these will be remediated through hardening of NSGs."*

Document Findings (Including Root Cause):

1. Document the findings of the incident and labeled it as a “True Positive”. Close the incident.



True Positive - Suspicious activity

locked down NSGs, and stopped the affected PC. The impact → the account was local to the linux machine (non-admin), so essentially low-impact. The attacker was involved with other incidents but these will be remediated through hardening of NSGs.

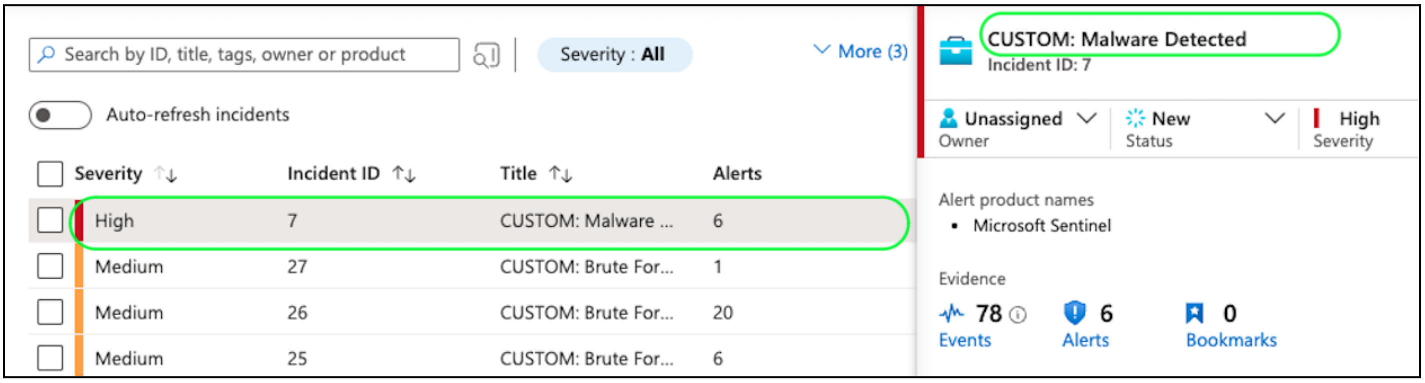
Task 4: Incident Response #4 - Possible Malware Outbreak

Preparation:

Note: *We already completed this IR phase. We’ve previously set up logs to be ingested into our Log Analytics workspace. We also configured alert rules in Sentinel.*

Detection & Analysis:

1. **Azure** portal > **Sentinel** > **Incidents** > order the incidents by **Severity** >
2. Select the **Linux Brute Force Success** alert.



Severity	Incident ID	Title	Alerts
High	7	CUSTOM: Malware ...	6
Medium	27	CUSTOM: Brute For...	1
Medium	26	CUSTOM: Brute For...	20
Medium	25	CUSTOM: Brute For...	6

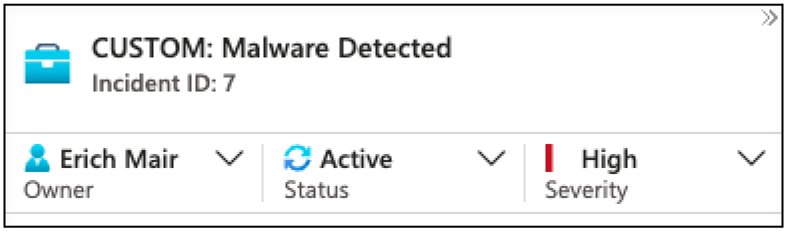
CUSTOM: Malware Detected
Incident ID: 7

Unassigned Owner | New Status | High Severity

Alert product names
- Microsoft Sentinel

Evidence
78 Events | 6 Alerts | 0 Bookmarks

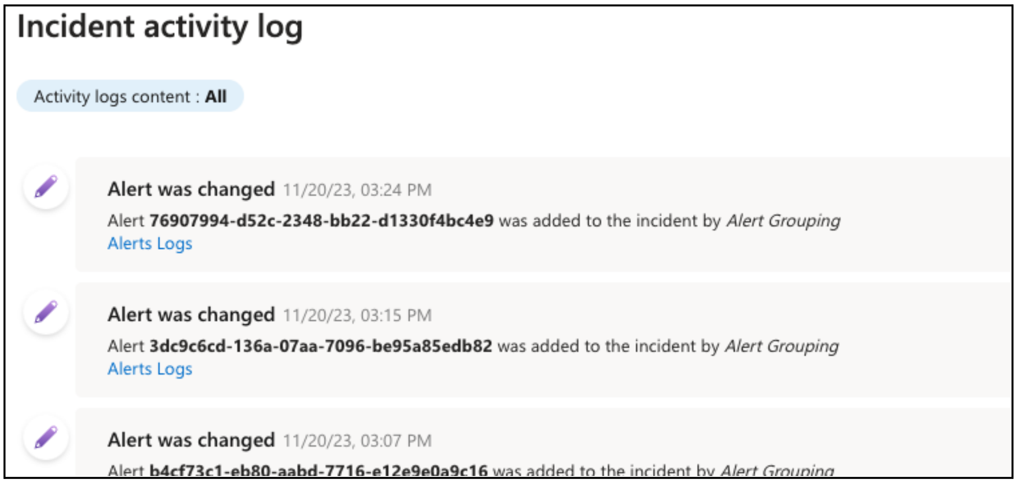
3. Set the **Severity**, **Status**, and **Owner** for the incident.



CUSTOM: Malware Detected
Incident ID: 7

Erich Mair Owner	Active Status	High Severity

4. Select **View Full Details**.
5. We see that the entity triggered several alerts (generated by our ‘test’ malware script).



Incident activity log

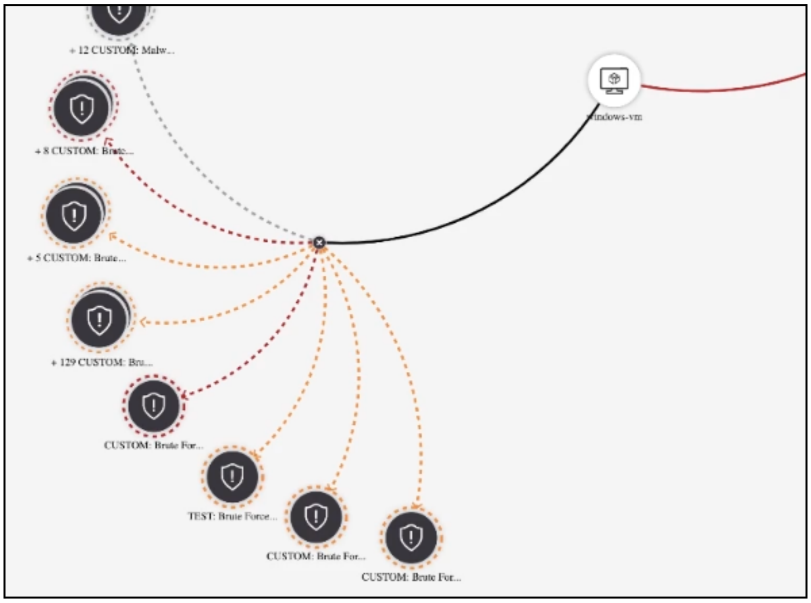
Activity logs content : **All**

Alert was changed 11/20/23, 03:24 PM
Alert **76907994-d52c-2348-bb22-d1330f4bc4e9** was added to the incident by *Alert Grouping*
Alerts Logs

Alert was changed 11/20/23, 03:15 PM
Alert **3dc9c6cd-136a-07aa-7096-be95a85edb82** was added to the incident by *Alert Grouping*
Alerts Logs

Alert was changed 11/20/23, 03:07 PM
Alert **b4cf73c1-eb80-aabd-7716-e12e9e0a9c16** was added to the incident by *Alert Grouping*

6. Select **Investigate** to see other events that originated from this attacker/entity.

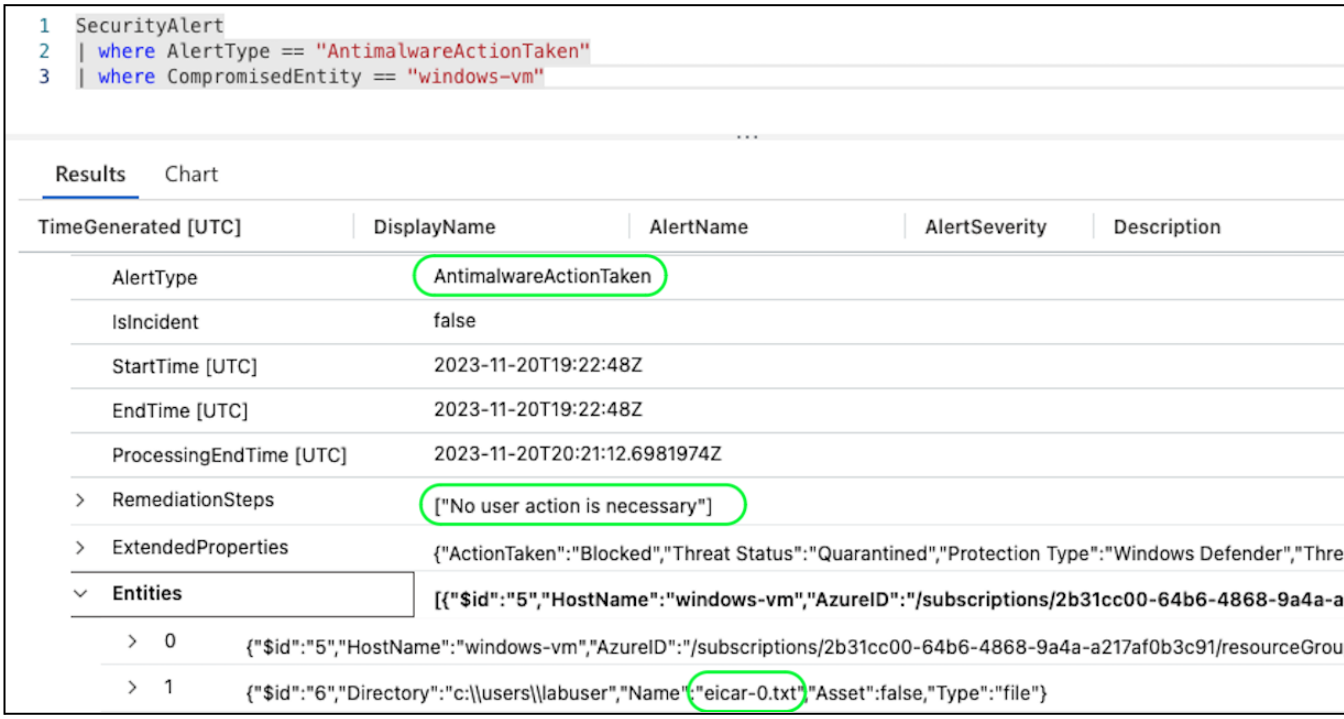


   a. Let’s start writing our notes.

   Note*: Windows-vm was involved with several activities that raised alerts.*

7. Let’s examine the query that generated this alert.

a. Copy the rule’s **query** > **Log Analytics workspace** >



```
SecurityAlert
| where AlertType == "AntimalwareActionTaken"
| where CompromisedEntity == "windows-vm"
```

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	Description

AlertType	AntimalwareActionTaken
IsIncident	false
StartTime [UTC]	2023-11-20T19:22:48Z
EndTime [UTC]	2023-11-20T19:22:48Z
ProcessingEndTime [UTC]	2023-11-20T20:21:12.6981974Z
› RemediationSteps	["No user action is necessary"]
› ExtendedProperties	{"ActionTaken":"Blocked","Threat Status":"Quarantined","Protection Type":"Windows Defender","Thre
⌄ Entities	[{"$id":"5","HostName":"windows-vm","AzureID":"/subscriptions/2b31cc00-64b6-4868-9a4a-a
› 0	{"$id":"5","HostName":"windows-vm","AzureID":"/subscriptions/2b31cc00-64b6-4868-9a4a-a217af0b3c91/resourceGrou
› 1	{"$id":"6","Directory":"c:\\users\\labuser","Name":"eicar-0.txt","Asset":false,"Type":"file"}

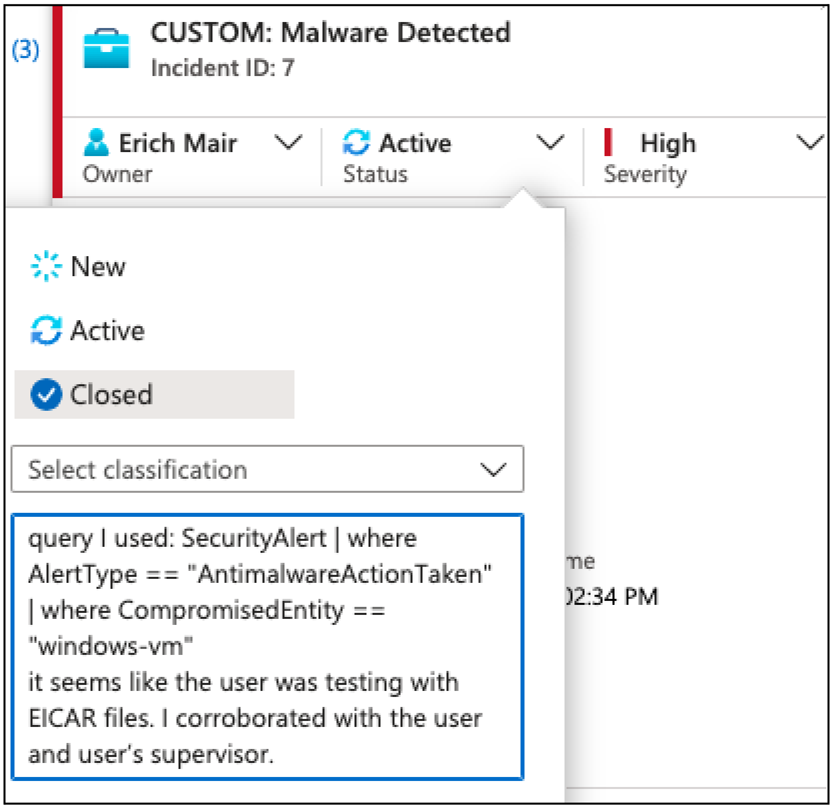
Note: *“This alert was a **False Positive**. Here is the query I used:*
SecurityAlert | where AlertType == "AntimalwareActionTaken"
| where CompromisedEntity == "windows-vm"
it seems like the user was testing with EICAR files. I corroborated with the user and the user's supervisor.”

Containment, Eradication, and Recovery:

1. N/A

Document Findings (Including Root Cause):

1. Documented the findings of the incident and labeled it as a “Benign Positive”. Close the incident.



query I used: SecurityAlert | where AlertType == "AntimalwareActionTaken" | where CompromisedEntity == "windows-vm"
it seems like the user was testing with EICAR files. I corroborated with the user and user's supervisor.

End:

- We’ve performed incident response on our lab environment and hardened our lab environment.
- We’ll soon expose our lab environment again for 24 hours We’ll then compare results of ‘Before’ and ‘After’ securing/hardening our environment.