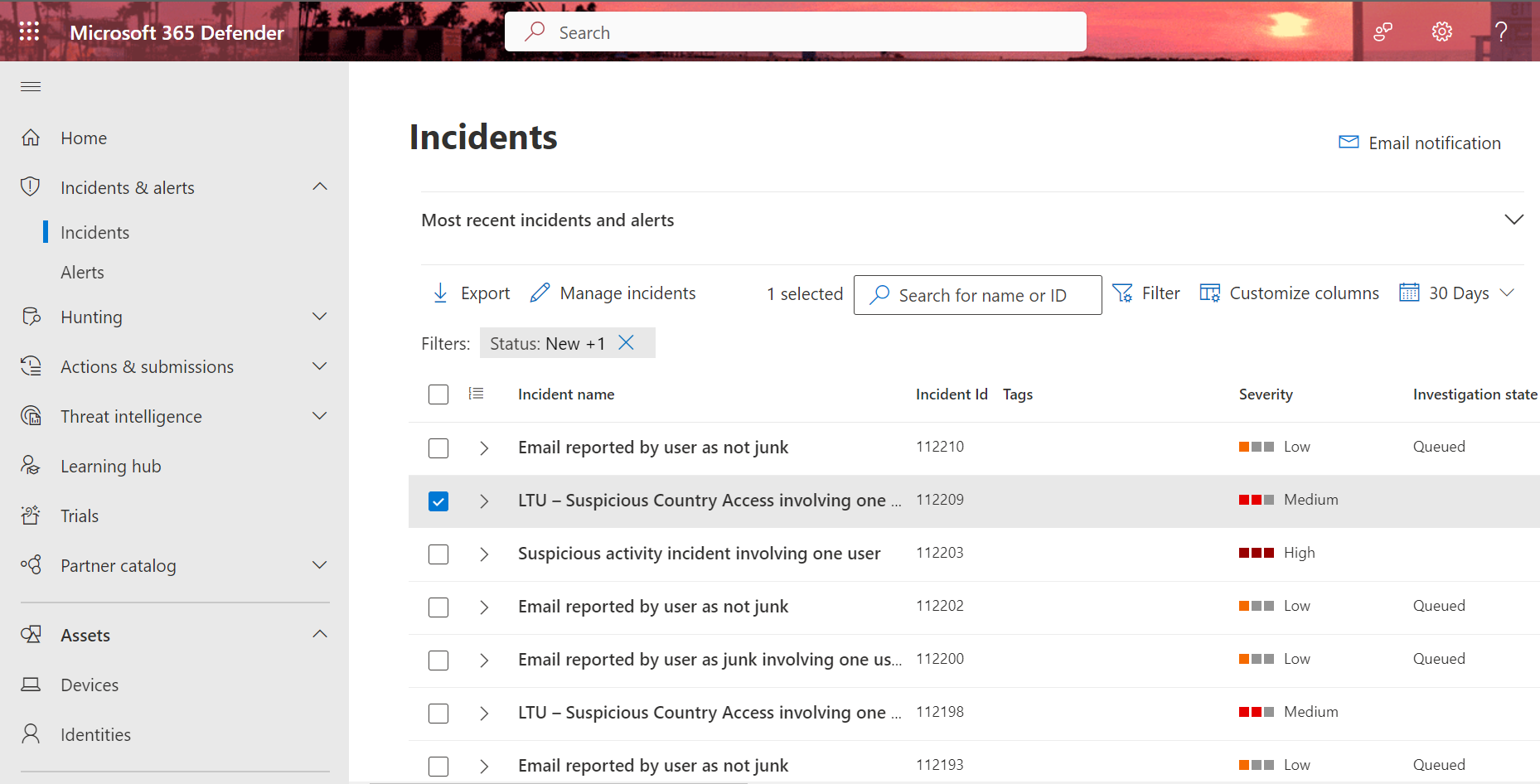
**Playbook for handling suspicious country access for one user alerts**

**Steps by step guide to handle and manage incidents and alerts on Microsoft defender 365:**

1. **First open Microsoft 365 defender and go to incident and alert tab:**

[**https://security.microsoft.com/homepage?tid=9aee26d8-97c2-4fad-8900-96735f6dc73f**](https://security.microsoft.com/homepage?tid=9aee26d8-97c2-4fad-8900-96735f6dc73f)

1. **Open the Incident page to review all the incidents and alerts.**

****

***Fig.1 Select incident.***

* In the incident page you can review all the past six months and ongoing alerts running along with their Incident Id’s, severity, and investigation state.
* When an incident or alert is generated, it needs to be assigned to someone for resolution.
* If you want to work on any particular incident, then you have to select that incident like showed in above figure 1.
* We can also manage and select one more incident at a time.

1. **Manage incident:**

A screenshot of a computer

Description automatically generated

**Fig 1.2 Managing Incidents**

* Then after selecting particular incident which we are working on. Then click on manage incident in order manage and assign that incident **as active, resolved or in progress.**
* We take responsibility for the incident, and if the specific alert remains unresolved, we must choose 'currently active'; otherwise, we select 'resolved' or 'currently in progress.
* **Upon clicking the Filter button**, we have the option to **refine our alert** selection, allowing us to focus solely on alerts with particular statuses, such as 'Not solved,' 'active,' or 'in progress,' if desired.

**Different types of alert status and its use:**

* **Not Solved:** This status indicates that the incident has not been resolved or checked by anyone until now.
* **Currently Active:** This status indicates that the incident is still ongoing and hasn't been resolved yet.
* **Resolved:** This status would be used when the incident has been completely resolved, and the issue is no longer active.
* **Currently in Progress:** It is used when someone is actively working on resolving the incident, but it hasn't been completely resolved yet.

**Investigation Steps:**

1. **Review and Manage Incident:**

* Identify suspicious user activity originating from an IP address potentially associated with a malicious actor.
* Classify the incident based on its severity.

A screenshot of a computer screen

Description automatically generated

***Fig 1.3 It’s to guide incident management and classification.***

1. **Collect Incident Information:**

* Note the **Incident ID for future reference**.
* Document the date and time of access.
* Examine the nature of access attempts:
* Are there mostly failed sign-in attempts?
* Is there a **suspicious time interval** between sign-in attempts?
* Review **access dates and locations.**

1. **Investigate the IP Address:**

* Check for successful sign-ins with **MFA prompts**, which may indicate non-malicious activity.
* Examine the use of anonymous proxies or the Tor network.
* Determine if the IP address is associated with a trustworthy VPN.
* Search for other IPs with the same subnet/ISP.
* Check the IP address against the tenant's recent **activity log.**
* Look for other suspicious activities or alerts originating from the IP.
* Assess the IP address's risk score using tools like RiskIQ.
* Investigate the use of protocols like **POP3, IMAP, and SMTP**.

A screenshot of a computer

Description automatically generated**Figure 2. The Device type field shows *Unknown (BAV2ROPC)* user agent in Microsoft 365 Defender.**

4. **Investigate Suspicious User activity after sign-In:**

• **Review accounts** that signed in from the **suspicious IP.**

• Search for **malicious or unusual activities** in these accounts after sign-in.

• Validate the preceding account activity for commonalities.

• Check for **other alerts received by the user.**

• Examine if the alert is part of a **larger incident**.

A screenshot of a computer

Description automatically generated

***Fig 3. Analysing user profile, location, device and Ip address***

II. **Recommended Actions for Suspicious Country Access for one user alerts:**

1. **Investigation and Verification:**

• Thoroughly investigate the alert.

• Verify the user's identity.

2. **Account Security:**

• Disable compromised accounts if necessary.

• Prompt the user to change their password.

• Enforce multi-factor authentication (MFA).

3. **User Communication:**

• Notify the user about the incident and recommended security measures.

4. **Email and Access Review:**

• Check for unauthorized email forwarding rules.

• Review access logs for signs of unauthorized access.

5. **Access Control:**

• Block or restrict access from suspicious locations.

6. **Escalation and Ongoing Response:**

• Escalate the alert when needed.

• Conduct threat hunting and remediation.

7. **Compliance and Documentation:**

• Report to compliance and legal teams if necessary.

• Document all actions and findings.

8. **Communication and Monitoring:**

• Communicate with relevant stakeholders.

• Implement continuous monitoring.

9. **Post-Incident Review:**

• Conduct a post-incident review for improvements.

**Advanced hunting queries for investigating suspicious country access involving one user alert:**

[**https://argonsys.com/microsoft-cloud/library/microsoft-defender-for-endpoint-commonly-used-queries-and-examples/**](https://argonsys.com/microsoft-cloud/library/microsoft-defender-for-endpoint-commonly-used-queries-and-examples/)

* The "SampleUser" is a placeholder for the actual username or account name you want to investigate. When you run these queries in your Microsoft Defender for Endpoint environment, you should replace "SampleUser" with the username of the user you are investigating.
* You should use the actual field name that corresponds to the username or account name in your environment. In most cases, this field will be named something like "InitiatingUser," "UserPrincipalName,"

1. **Suspicious Login Attempts:**

* Identify login attempts from countries or regions unusual for the user.

**Query:**

DeviceNetworkEvents

| where ActionType == "LogonSuccess"

| where IPAddress !in ("192.168.1.100") // Replace with the user's usual IP

| where tostring(InitiatingUser) == "SampleUser"

Working Query:

let suspiciousLogins = IdentityLogonEvents

| where LogonType == "Failure" // Check the exact column name for failed logins

| project AccountSid,TargetDeviceName,extent\_id(), AccountDisplayName, IPAddress, LogonType;

suspiciousLogins

1. **Anomalous Traffic Patterns:**

* Detect patterns of repeated or irregular logins.

**Query:**

DeviceNetworkEvents

| where ActionType == "LogonSuccess"

| where tostring(InitiatingUser) == "SampleUser"

| extend Date = format\_datetime(EventTime, 'yyyy-MM-dd')

| summarize LoginCount = count() by Date

| order by Date asc

let anomalousTraffic = NetworkTraffic // Assuming the table name is NetworkTraffic

| where Protocol != "HTTP" and DestinationPort == 443

| project Protocol, DestinationPort, RemoteIP;

anomalousTraffic

1. **Tor Network or Anonymous Proxies:**

• Check for logins originating from Tor or anonymous proxies:

**Query:**

DeviceNetworkEvents

| where ActionType == "LogonSuccess"

| where IPAddress in ("1.1.1.1", "2.2.2.2") // Replace with known Tor or proxy IP ranges

| where tostring(InitiatingUser) == "SampleUser"

let torAndProxyConnections = ExternalData // Assuming the table name is ExternalData

| where Category == "Proxy/Anonymizer" or Category == "Tor"

| project Category, IPAddress;

torAndProxyConnections

1. **Suspicious User-Agent Strings:**

• Investigate logins with suspicious User-Agent strings:

**Query:**

DeviceNetworkEvents

| where ActionType == "LogonSuccess"

| where tostring(InitiatingUser) == "SampleUser"

| where tostring(UserAgent) == "Unknown (BAV2ROPC)"

**let suspiciousUserAgents = WebBrowser**

**| where tostring(UserAgent) contains "suspicious\_string"**

**| project UserAgent, RemoteIP, Url;**

**suspiciousUserAgents**

1. **Geographical Anomalies:**

• Identify logins from different geographic locations within a short time frame:

**Query:**

DeviceNetworkEvents

| where ActionType == "LogonSuccess"

| where tostring(InitiatingUser) == "SampleUser"

| extend Date = format\_datetime(EventTime, 'yyyy-MM-dd')

| summarize LoginCount = count() by Date, IPAddress

| where LoginCount > 1

**let geographicalAnomalies = SigninLogs**

**| join kind=inner (DeviceInfo**

**| project DeviceId, CountryCode) on DeviceId**

**| summarize Count=count() by CountryCode**

**| order by Count desc;**

**geographicalAnomalies**

1. **Multiple Users from Suspicious IP:**

• Detect if multiple users log in from the same suspicious IP

**Query:**

DeviceNetworkEvents

| where ActionType == "LogonSuccess"

| where IPAddress == "192.168.1.100" // Replace with the suspicious IP

| where isnotempty(InitiatingUser)

| summarize UserCount = dcount(InitiatingUser) by IPAddress

| where UserCount > 1

let suspiciousIPs = SecurityEvent

| where tostring(IPAddress) == "suspicious\_ip"

| join kind=inner (SigninLogs

| project UserPrincipalName, IPAddress) on IPAddress

| summarize UserCount=count() by UserPrincipalName

| order by UserCount desc;

suspiciousIPs

These advanced hunting queries can help to proactively detect and investigate suspicious country access involving a one user.