Microsoft Sentinel Implementation and Threat Intelligence Integration

Objective

The objective of this project is to enhance the security posture of the organization by implementing advanced automation and threat intelligence capabilities within Microsoft Sentinel. This includes the creation of automation rules, playbooks, custom detection rules, and threat intelligence profiles to streamline security operations, improve incident response times, and proactively detect and mitigate potential threats.

Executive Summary

This project focuses on the implementation and integration of Microsoft Sentinel with advanced threat intelligence to bolster the organization's security infrastructure. Key achievements include the development of automation rules and playbooks for incident triage and response, the creation of custom detection rules for identifying potential brute force attacks, and the profiling of the APT28 threat actor. Additionally, a custom detection rule based on APT28 threat intelligence was developed to identify and respond to activities associated with this sophisticated threat actor. The project also involved the development of a custom workbook for visualizing security data, providing security analysts with a comprehensive overview of potential security events.

1. Automation Rule Implementation in Microsoft Sentinel

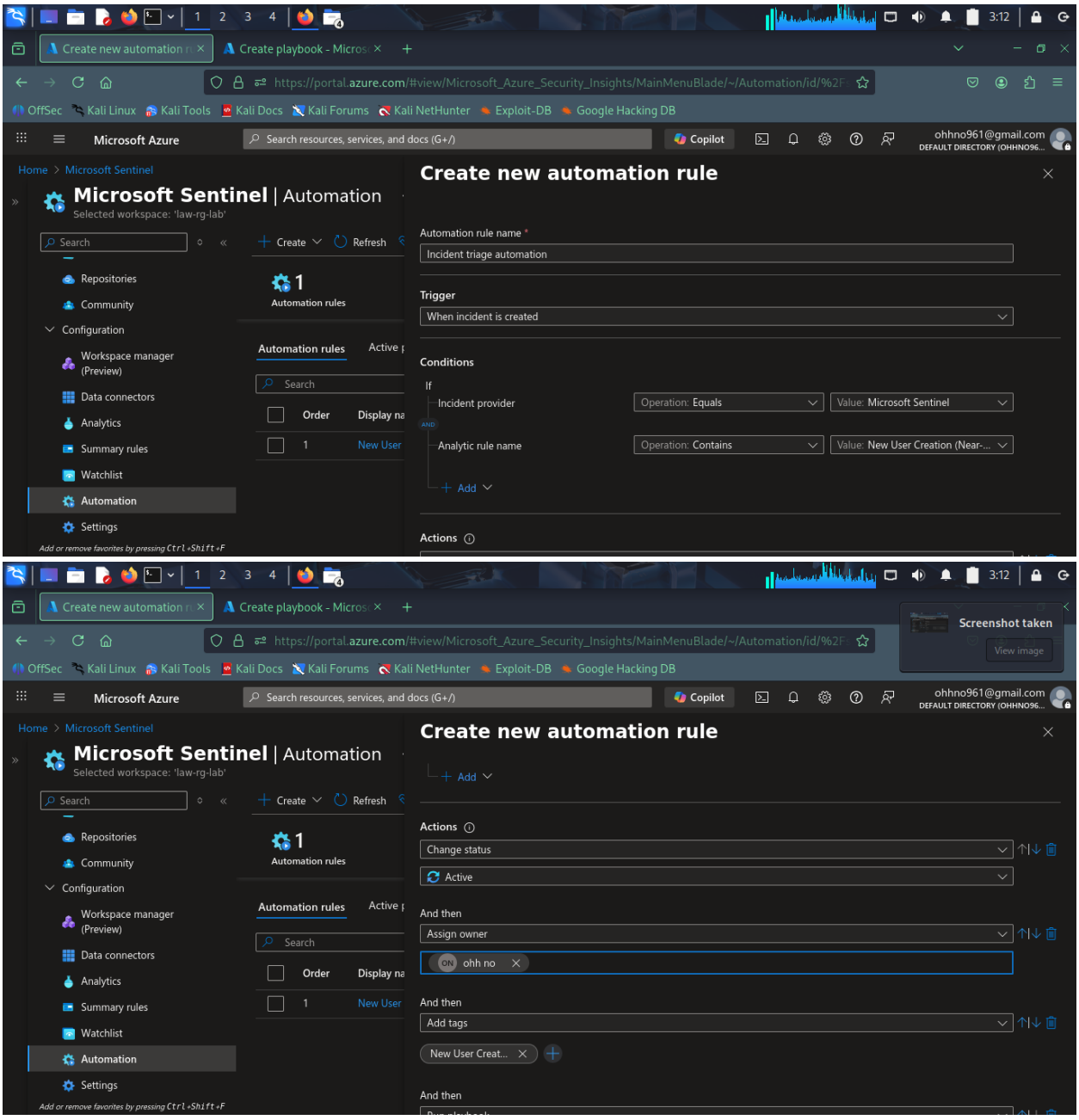
1.1. Creating an Automation Rule for Incident Triage

An automation rule named "Incident Triage Automation" was successfully created within Microsoft Sentinel. This rule is configured to trigger when a new incident is created. The primary condition for this rule is that the incident provider must be "Microsoft Sentinel" and the specific analytical rule name that triggers the automation is "New user is created". This setup ensures that the automation is precisely targeted at incidents generated by this particular detection rule, streamlining the initial response to new user creation events which can sometimes indicate malicious activity or policy violations. The creation of this rule marks a foundational step in automating routine security operations, allowing for faster and more consistent initial handling of specific incident types.

1.2. Configuring Playbooks for Automated Responses

As part of the automation strategy, a playbook named "New_User_Created_Email_Notification" was developed. This playbook is designed to be

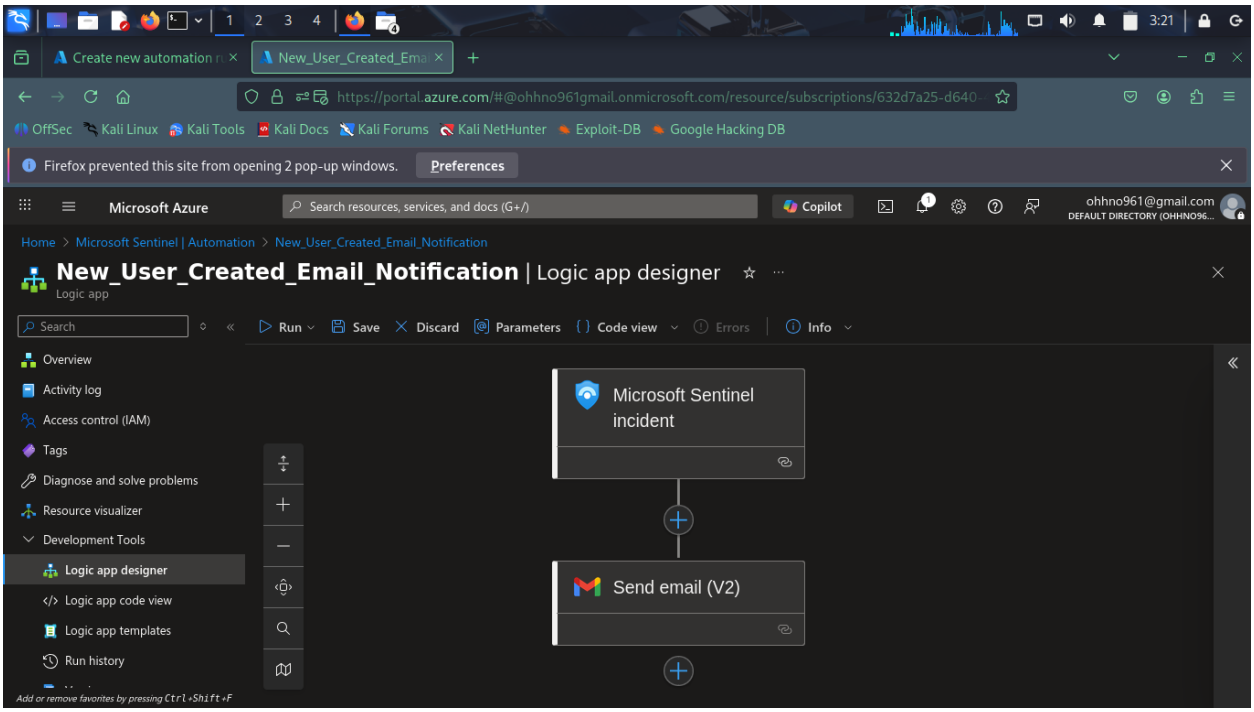
triggered by the "Incident Triage Automation" rule. Its core function is to send an email notification to the designated security team or relevant personnel whenever the "New user is created" alert is triggered. The playbook utilizes the Gmail connector (or a similar email connector like Office 365 Outlook if Gmail is not directly available or preferred) to dispatch these notifications. The email content can be customized to include dynamic details from the incident, such as the username of the newly created account and the time of creation, providing immediate context to the security team. This automated notification system ensures that potential security events related to user account creation are promptly brought to the attention of responders, facilitating quicker investigation and mitigation if necessary.

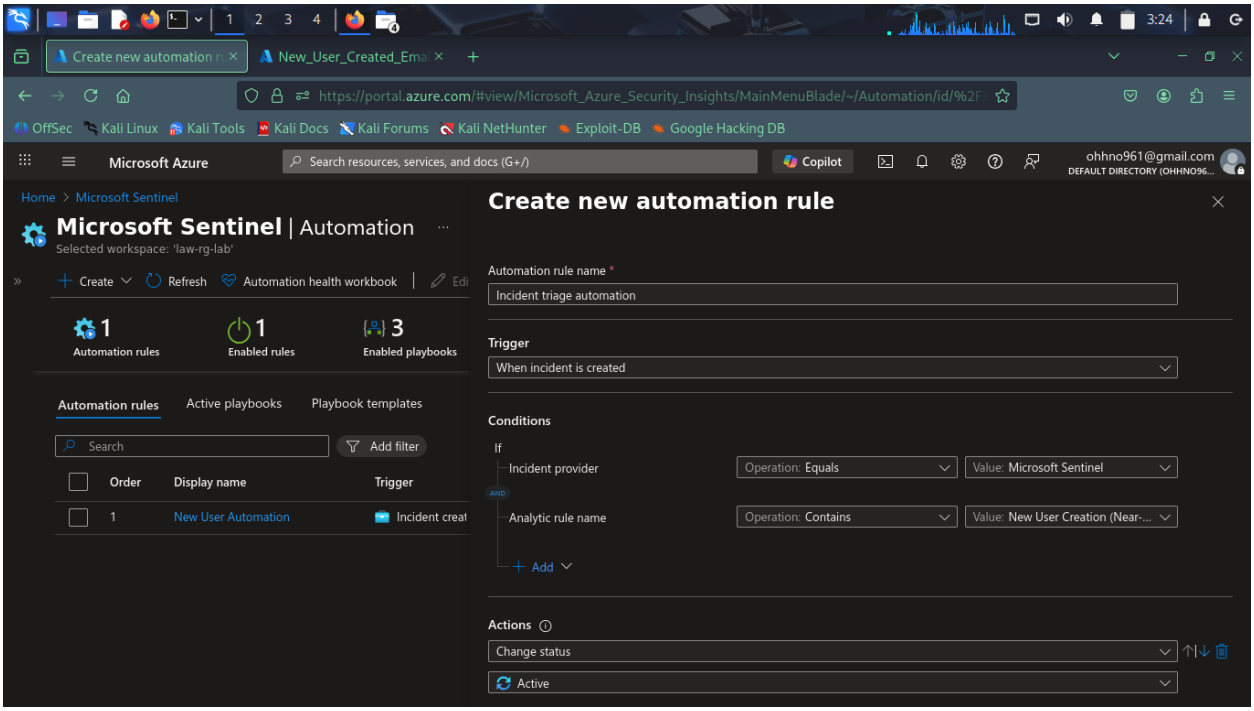


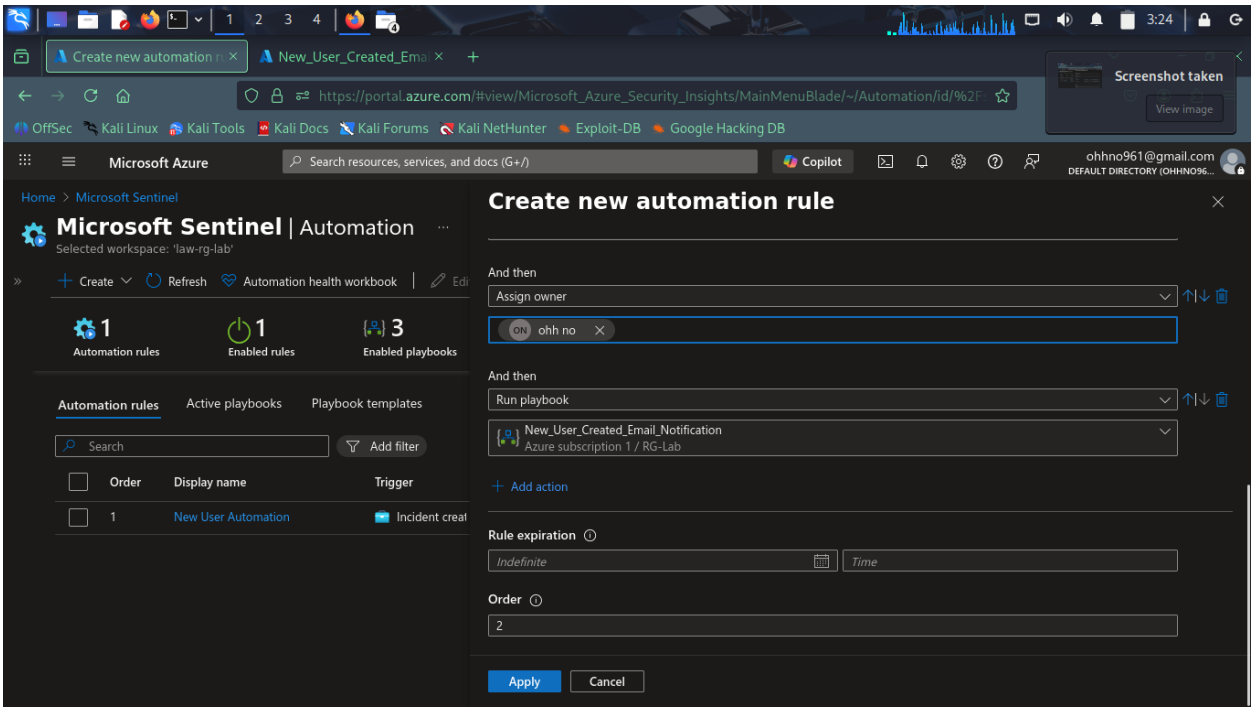
1.3. Setting Up Email Notifications for New User Creation Alerts

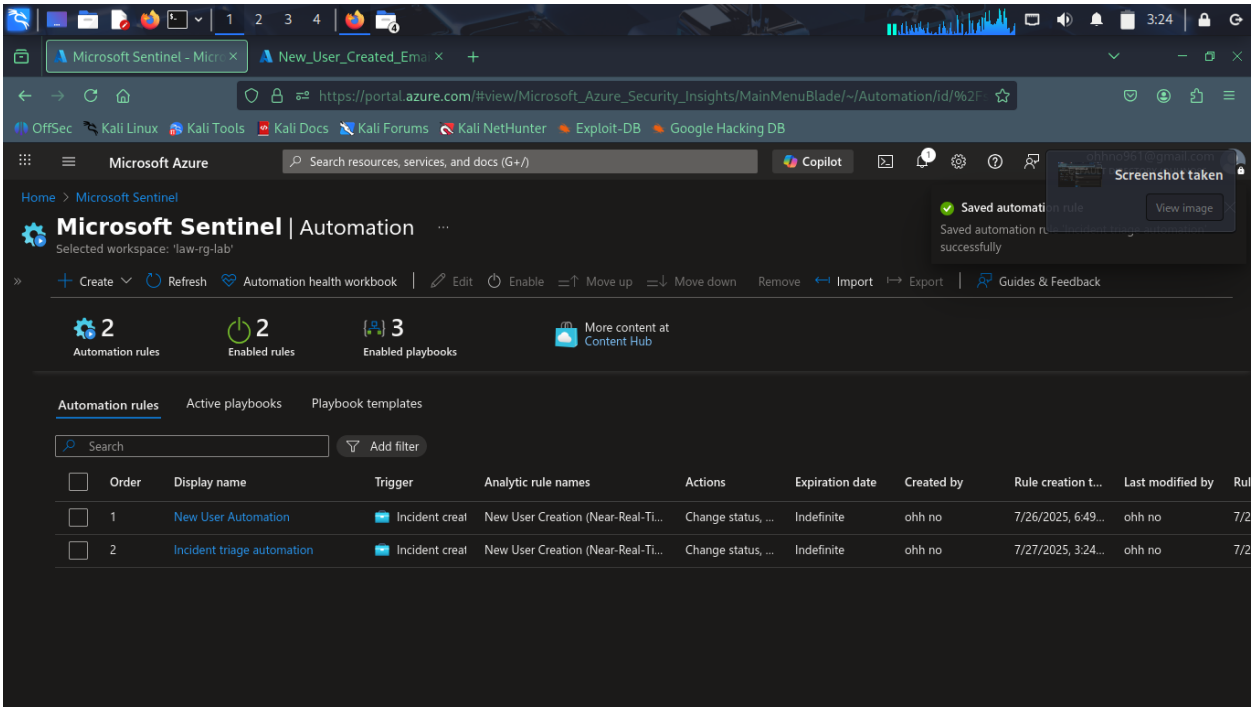
The "New_User_Created_Email_Notification" playbook was specifically configured to address the need for immediate awareness of new user creation events. The actions defined within the "Incident Triage Automation" rule include running this playbook. When an incident is created by the "New user is created" analytical rule, the automation rule not only changes the incident status and assigns an owner but also triggers this email notification playbook. The setup involved creating a connection to an email service (e.g., Gmail) within the playbook, defining the recipient's email address, subject line, and the

body of the email. This ensures that for every alert of this nature, a predefined set of personnel receives an email, enabling rapid assessment and response to potentially unauthorized or suspicious account creations, thereby enhancing the organization's security monitoring capabilities.





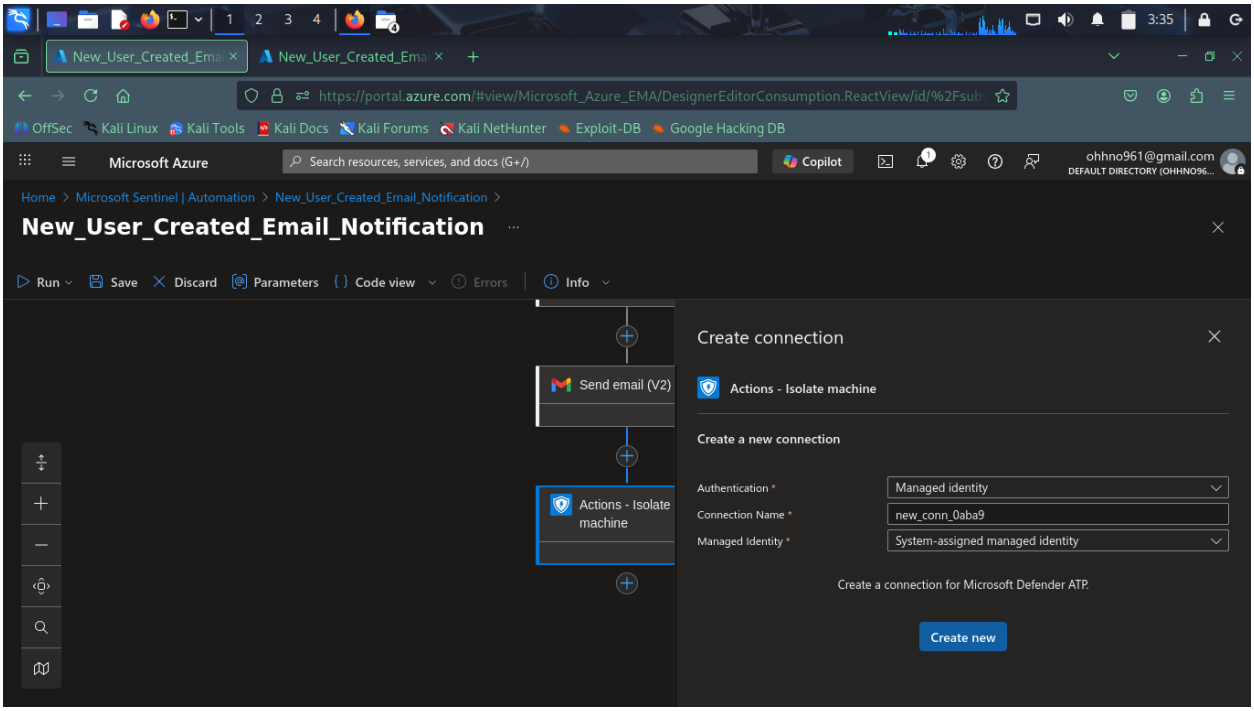


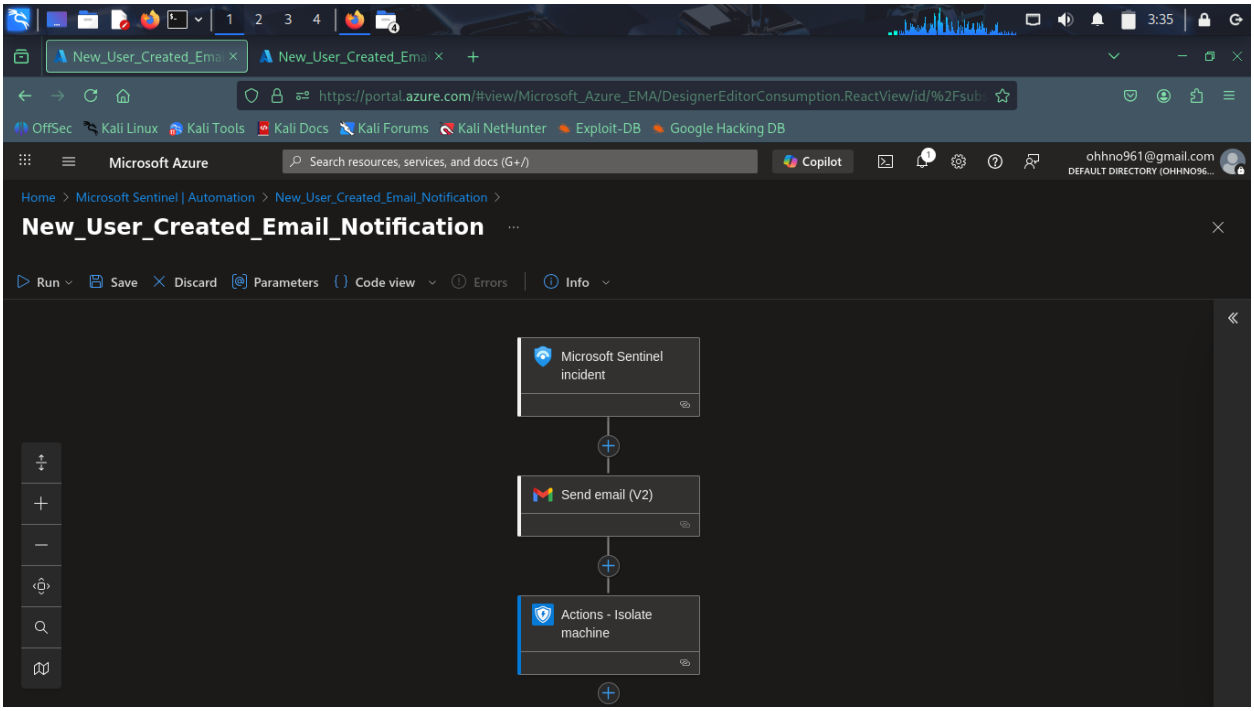


1.4. Developing a Playbook for Machine Isolation

A playbook was conceptualized and partially configured to automatically isolate a machine in response to a security incident. This playbook would leverage the Microsoft Defender for Endpoint connector (or similar endpoint security solutions integrated with Sentinel) and utilize the "Isolate machine" action. The intended workflow is that when a high-severity incident is detected, indicating a compromised machine, this playbook would be triggered.

The Machine ID, obtained dynamically from the incident information, would be passed to the "Isolate machine" action. Parameters for this action include the Machine ID, an optional comment (e.g., "Machine isolated due to suspicious activity"), and the isolation type (e.g., "Full" isolation for maximum security). While the full implementation and testing with actual Machine IDs were pending, the structure for such an automated containment response was established, demonstrating a proactive approach to limiting the impact of security breaches.





2. Custom Detection Rule Creation in Microsoft Sentinel

2.1. Developing a Scheduled Query Rule for Potential Brute Force Attacks

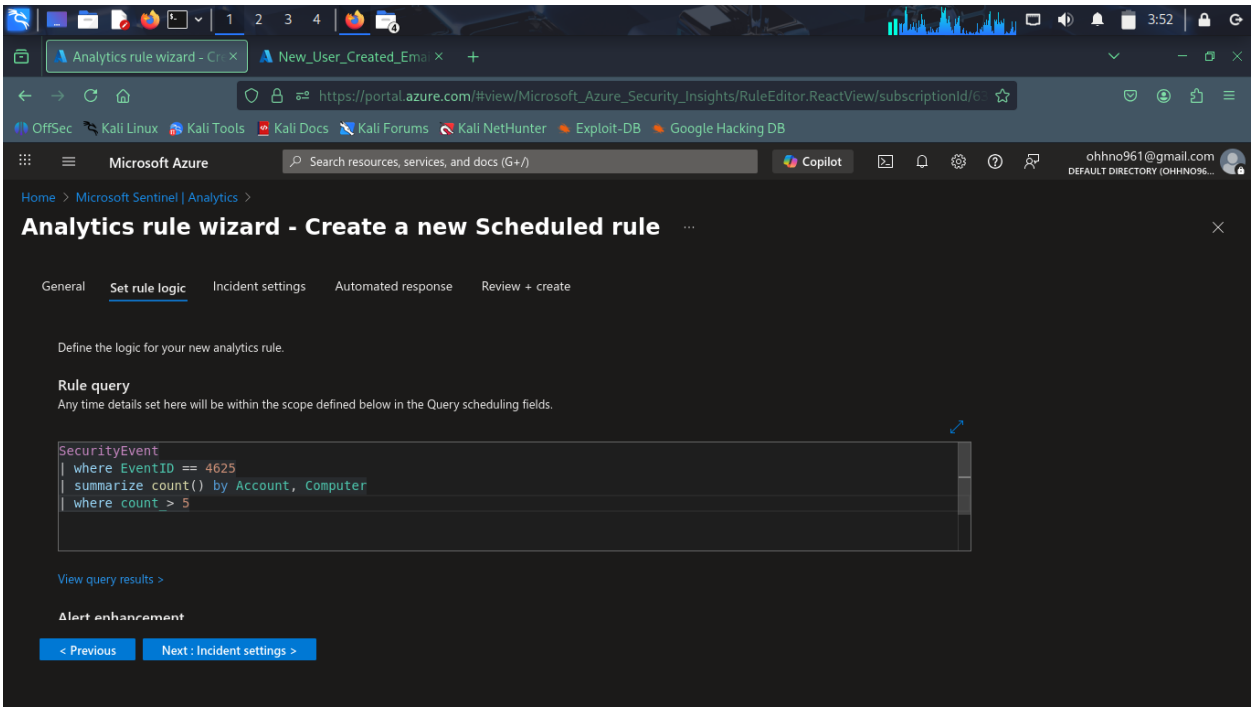
A custom scheduled query rule named "Potential Brute Force Attack" was developed in Microsoft Sentinel. The purpose of this rule is to detect multiple failed login attempts originating from the same IP address, a common indicator of brute force attacks. The rule's description clearly states its function: "Detects multiple failed login attempts from the same IP address." This rule was assigned a High severity level, reflecting the significant risk posed by brute force attacks. Relevant MITRE ATT&CK tactics were associated with the rule, primarily "Initial Access" and "Credential Access", as these are the primary objectives of such attacks. The creation of this rule enhances the organization's ability to identify and respond to attempts to gain unauthorized access to systems and accounts through repetitive password guessing.

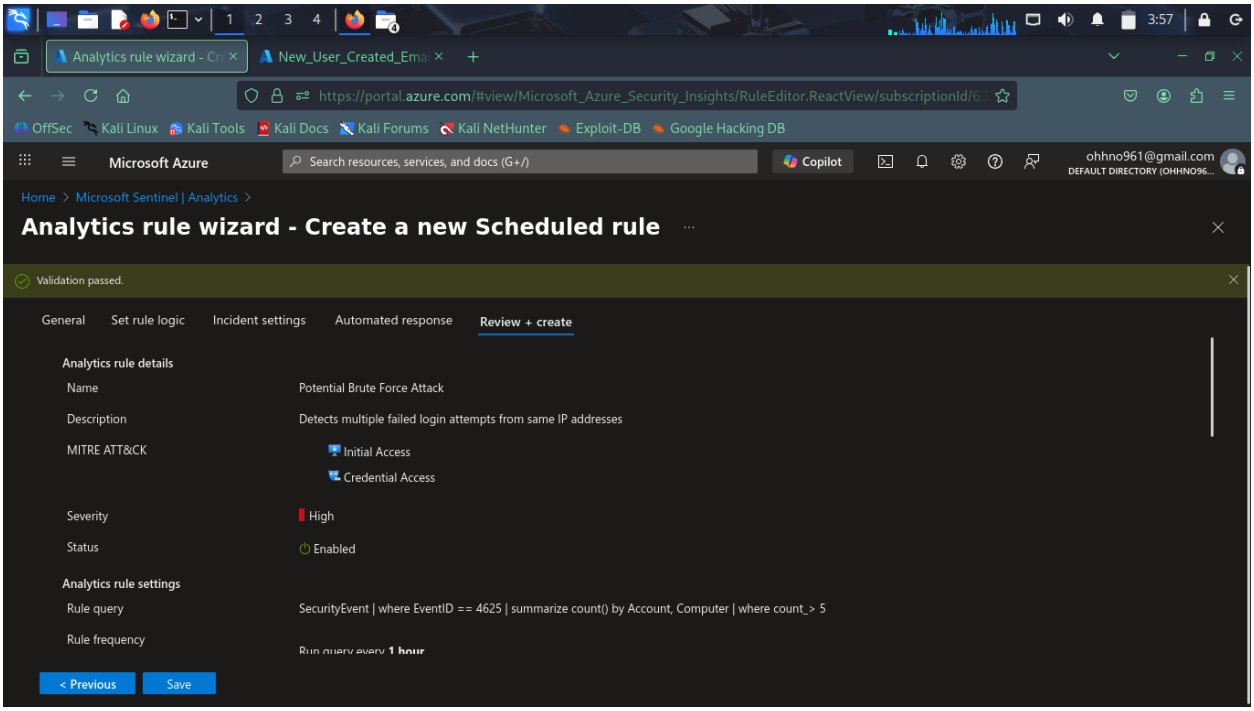
2.2. Defining Rule Logic and Query Scheduling

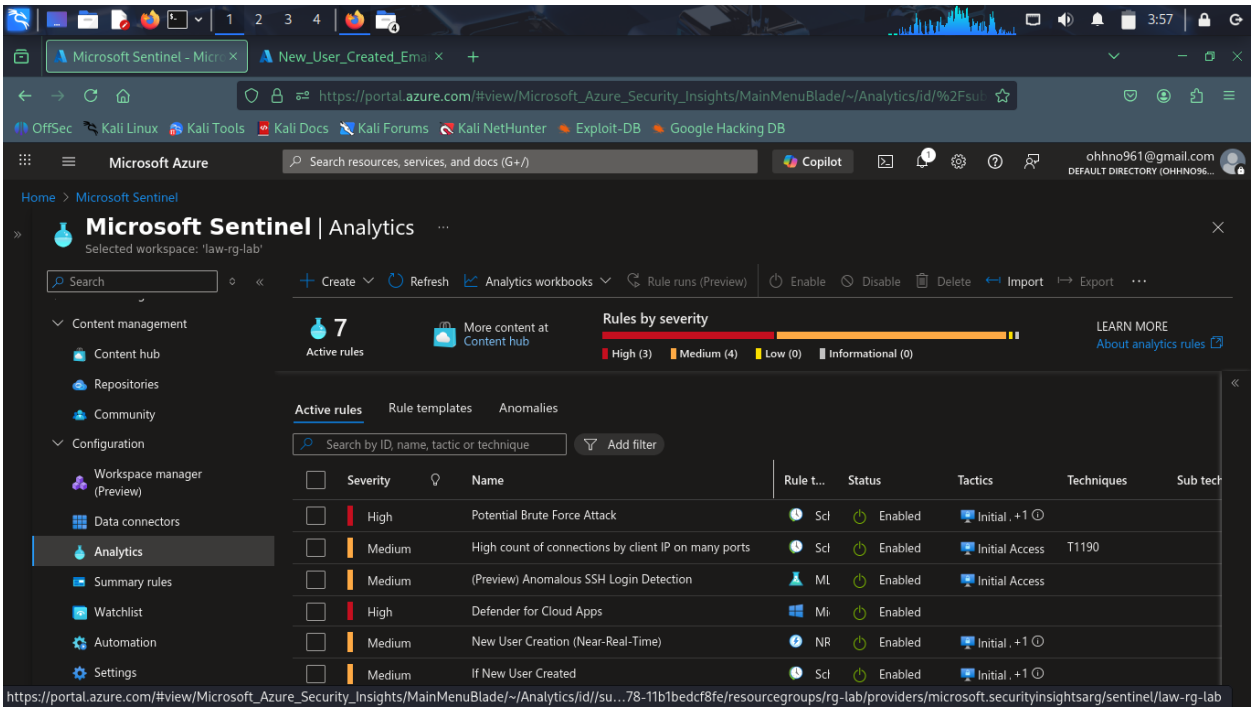
The rule logic for the "Potential Brute Force Attack" detection rule is defined by a Kusto Query Language (KQL) query. The specific query used is:

```
SecurityEvent
| where EventID == 4625
| summarize count() by Account, Computer
| where count_ > 5
```

This query searches the SecurityEvent table for events with EventID 4625, which signifies an account failed to log on. It then summarizes these events, counting the number of failed logins by Account and Computer. An alert is triggered if the count of failed login attempts (count_) for a specific account and computer exceeds 5. The query is scheduled to run every 1 hour and looks back at data from the last 1 hour. An alert is generated when the number of query results is greater than or equal to 5. Event grouping is configured to group all events into a single alert, providing a consolidated view of the brute force attempt rather than multiple individual alerts. Suppression is left turned off, ensuring all detected instances are reported. The rule is set to run automatically upon creation.


Analytics rule wizard - Cre
New_User_Created_Ema
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/RuleEditor.ReactView/subscriptionId/6
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Define the logic for your new analytics rule.
Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.
SecurityEvent
| where EventID == 4625
| summarize count() by Account, Computer
| where count_ > 5
View query results >
Alert enhancement
< Previous
Next : Incident settings >


Analytics rule wizard - Cre
New_User_Created_Ema
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/RuleEditor.ReactView/subscriptionId/6
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
Validation passed.
General
Set rule logic
Incident settings
Automated response
Review + create
Analytics rule details
Name
Potential Brute Force Attack
Description
Detects multiple failed login attempts from same IP addresses
MITRE ATT&CK
Initial Access
Credential Access
Severity
High
Status
Enabled
Analytics rule settings
Rule query
SecurityEvent | where EventID == 4625 | summarize count() by Account, Computer | where count_> 5
Rule frequency
Run query every 1 hour
< Previous
Save



3. Custom Workbook Development for Security Data Visualization

3.1. Creating a New Workbook and Adding Data Queries

A new workbook was created to facilitate the visualization of security data. The process began by navigating to the Azure Workbooks service and selecting the option to create a new workbook. For data sourcing, "Logs" were selected as the data source type, specifically utilizing "Log Analytics" as the resource type. The relevant Azure subscription and resource group containing the Log Analytics workspace were chosen to connect the workbook to the organization's log data. This setup allows the workbook to query and display information from the logs ingested by Microsoft Sentinel, providing a flexible canvas for building custom security dashboards and reports. The initial step involved adding a query to this workbook to fetch relevant security event data for visualization.

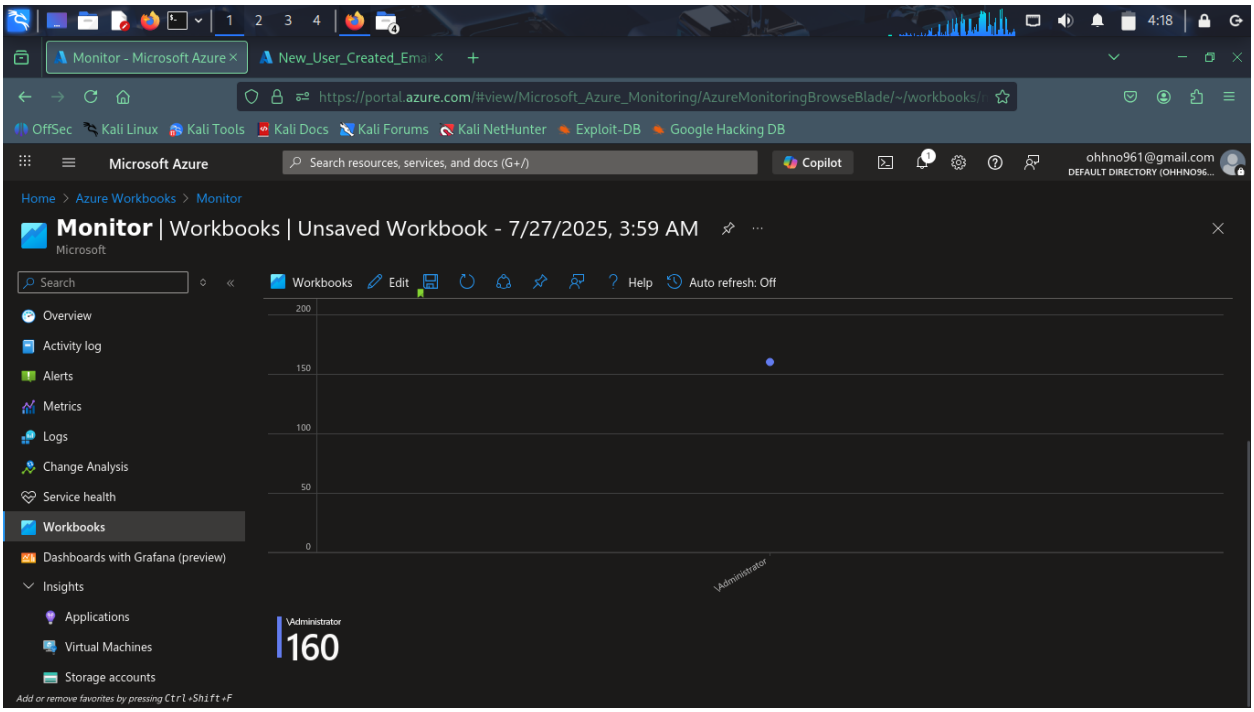
3.2. Configuring Visualizations for Security Event Analysis

Within the newly created workbook, a query was added to analyze security events. The KQL query used was the same as the one for the "Potential Brute Force Attack" detection rule:

SecurityEvent | where EventID == 4625 | summarize count() by Account, Computer | where count_ > 5

This query retrieves instances of multiple failed login attempts. For visualization, a Line chart was selected to display the data, with a Large size chosen for better visibility. The time range for the data displayed in the workbook was left at the default setting initially,

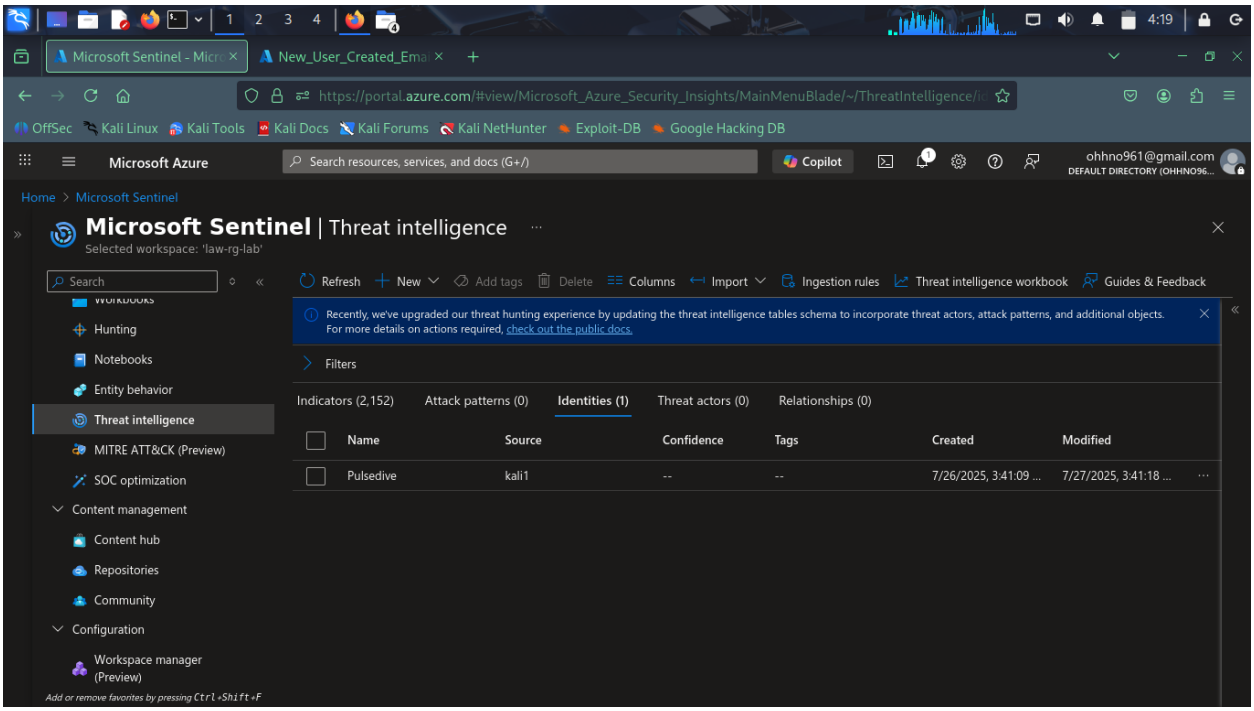
with the understanding that it can be adjusted as needed for specific analysis tasks. The primary purpose of this visualization is to provide an overview of failed login activity, allowing security analysts to spot trends or anomalies that might warrant further investigation. While the initial chart displayed a single dot due to the aggregation in the query (lacking a time component for the X-axis), the setup demonstrates the process of connecting workbooks to log data and configuring basic visualizations.

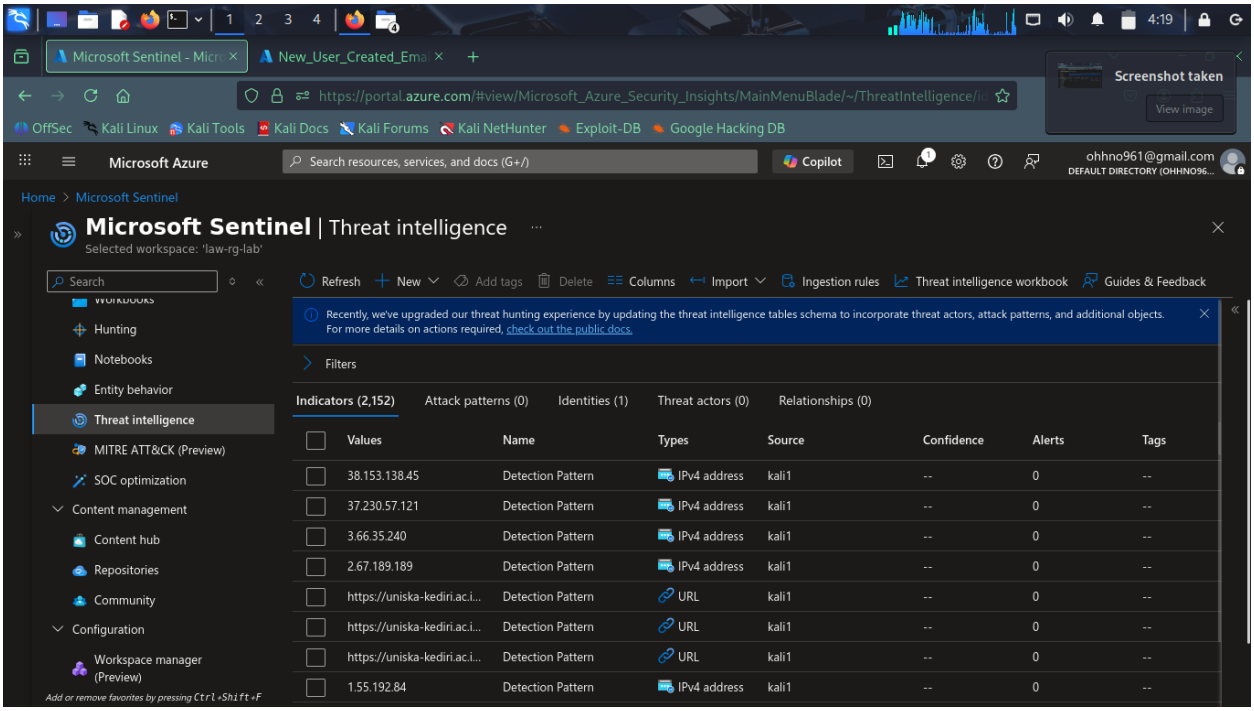


4. Advanced Threat Intelligence Integration and Utilization

4.1. Exploring Microsoft Sentinel's Threat Intelligence Capabilities

The project involved an exploration of Microsoft Sentinel's integrated threat intelligence capabilities. This was initiated by navigating to the "Threat Management" section within the Microsoft Sentinel workspace and then to "Threat Intelligence". This area provides access to various resources, including threat intelligence workbooks and analytics rules that leverage threat data. The platform allows for the ingestion and management of threat indicators, such as known malicious IP addresses, domains, and file hashes. During this exploration, existing indicators were reviewed, and the process of adding new threat intelligence objects was investigated. This foundational understanding is crucial for leveraging external threat feeds and internal intelligence to enhance detection and response capabilities within Sentinel.





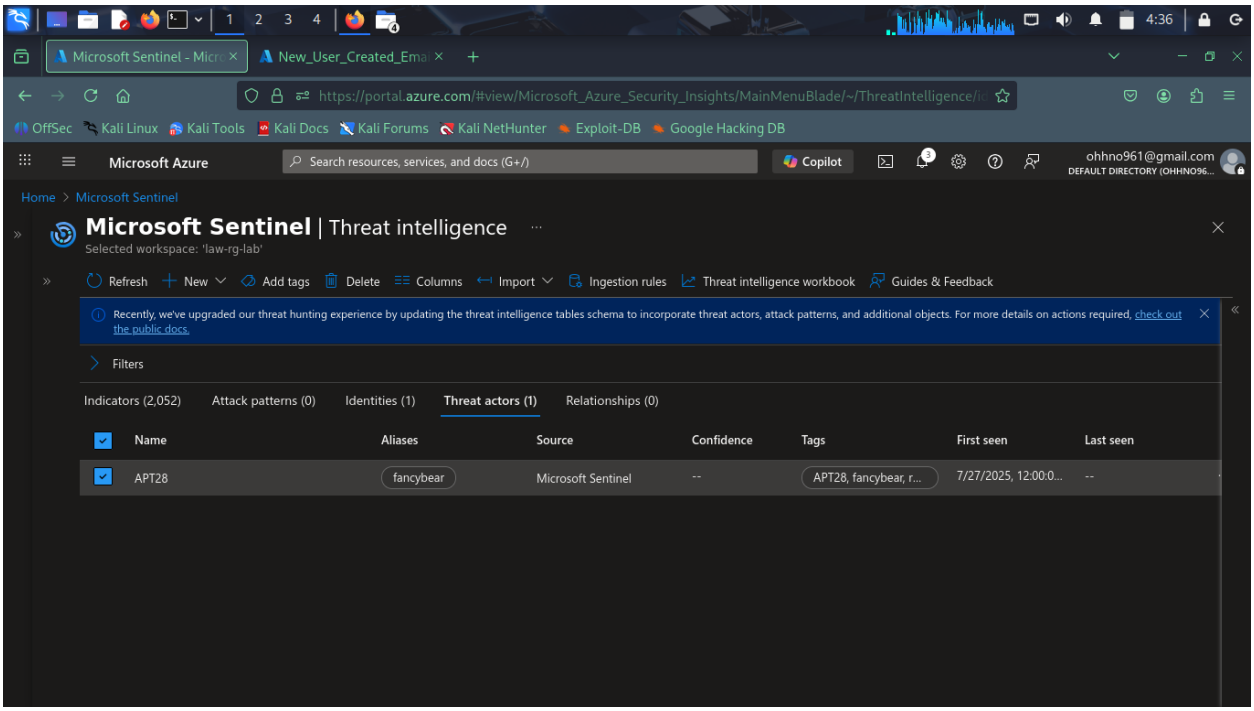
4.2. Profiling a Known Threat Actor: APT28 (Fancy Bear/Sofacy Group)

A detailed threat intelligence object was created for the APT28 (also known as Fancy Bear or Sofacy Group) threat actor. This profiling aimed to consolidate known information about this group within Microsoft Sentinel for enhanced detection and understanding. The following table summarizes the key attributes defined for the APT28 threat actor object:

Attribute	Value
Object Type	Threat Actor
Name	APT28
Aliases	Fancy Bear, Sofacy Group
First Seen	[Date of creation]
Role	Operator
Goal	Cyber espionage, Intelligence Gathering
Resource Level	Government
Sophistication	Advanced
Primary Motivation	Organizational Gain
Secondary Motivation	Ideology
Source	Microsoft Sentinel
Description	APT28 is a Russian cyber espionage group known for their sophisticated campaigns targeting government and military organizations worldwide. Also known as Fancy Bear or Sofacy Group.
Tags	APT28, Fancy Bear, cyber espionage, Russia
Traffic Light Protocol (TLP)	Red
Severity (0–5)	5 (Very High)

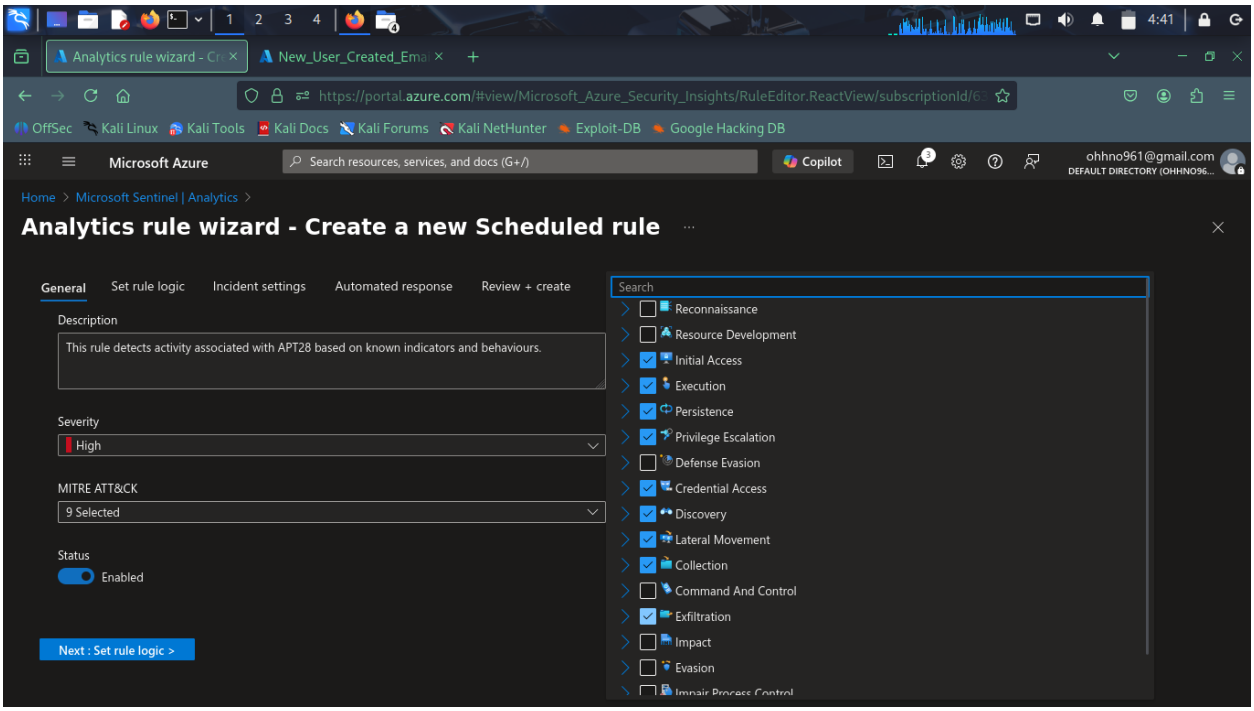
Table 1: APT28 Threat Actor Profile in Microsoft Sentinel

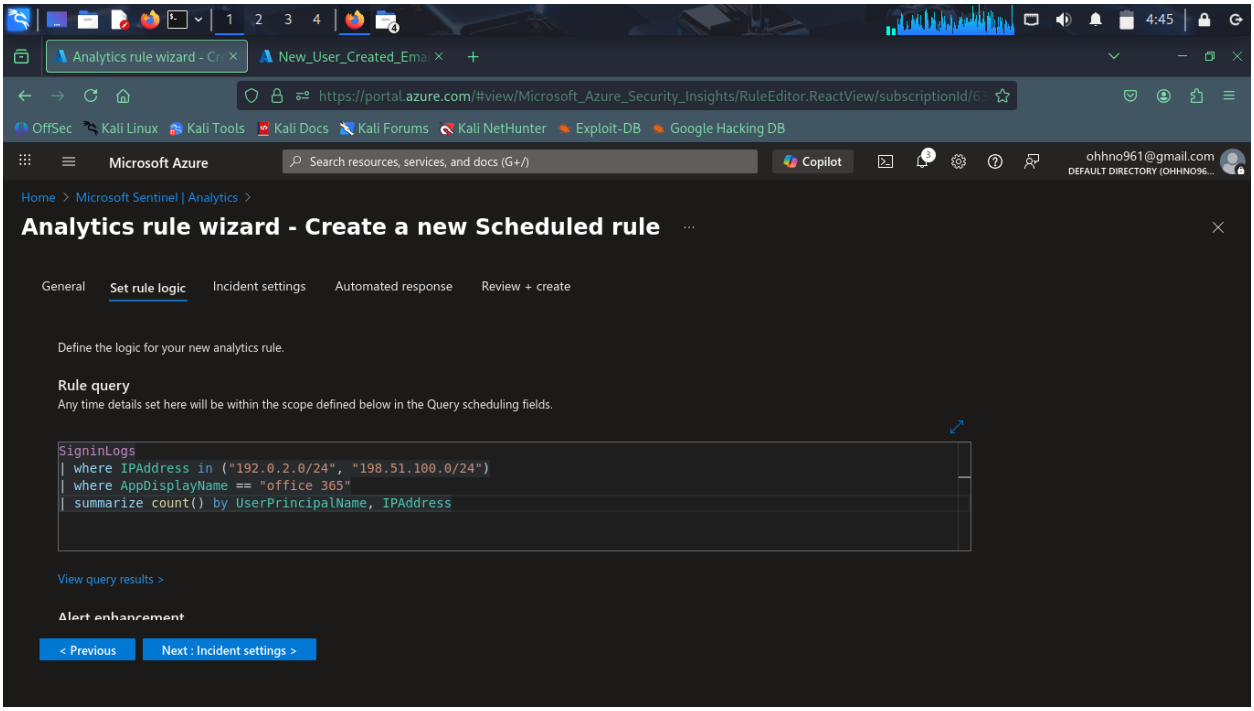
This comprehensive profile allows security teams to quickly understand the nature of the threat posed by APT28 and to correlate internal security events with this known adversary.
|

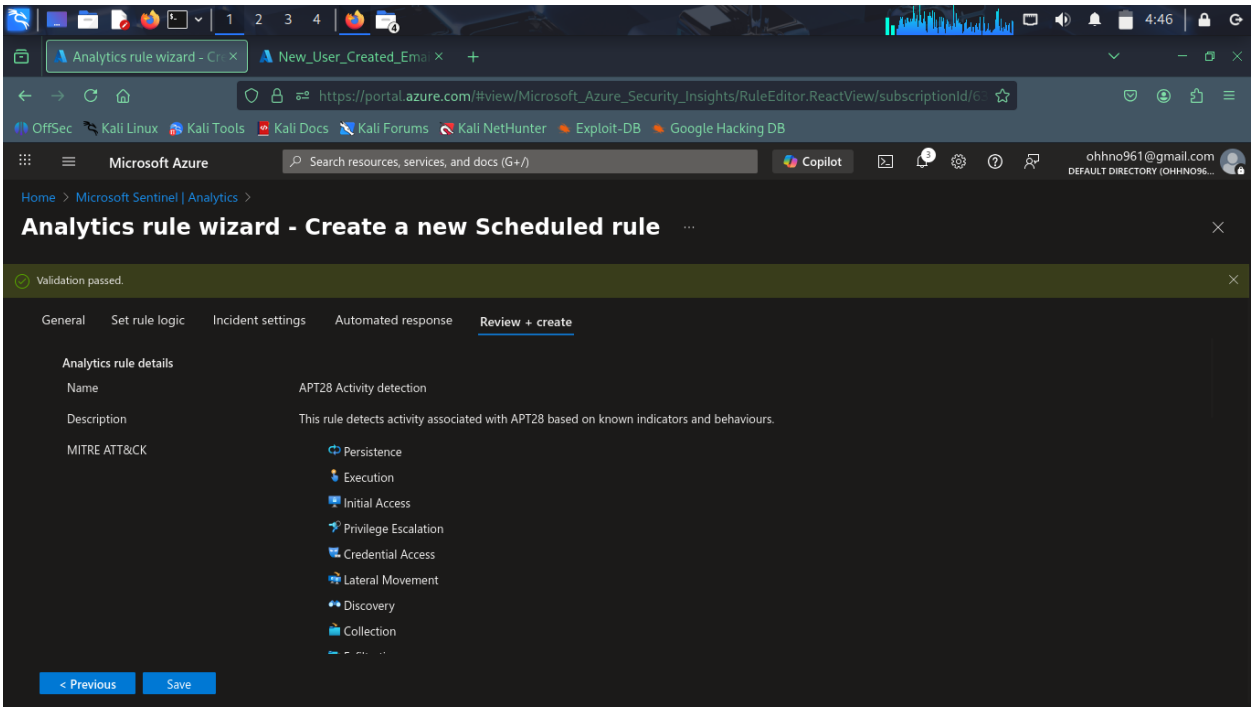


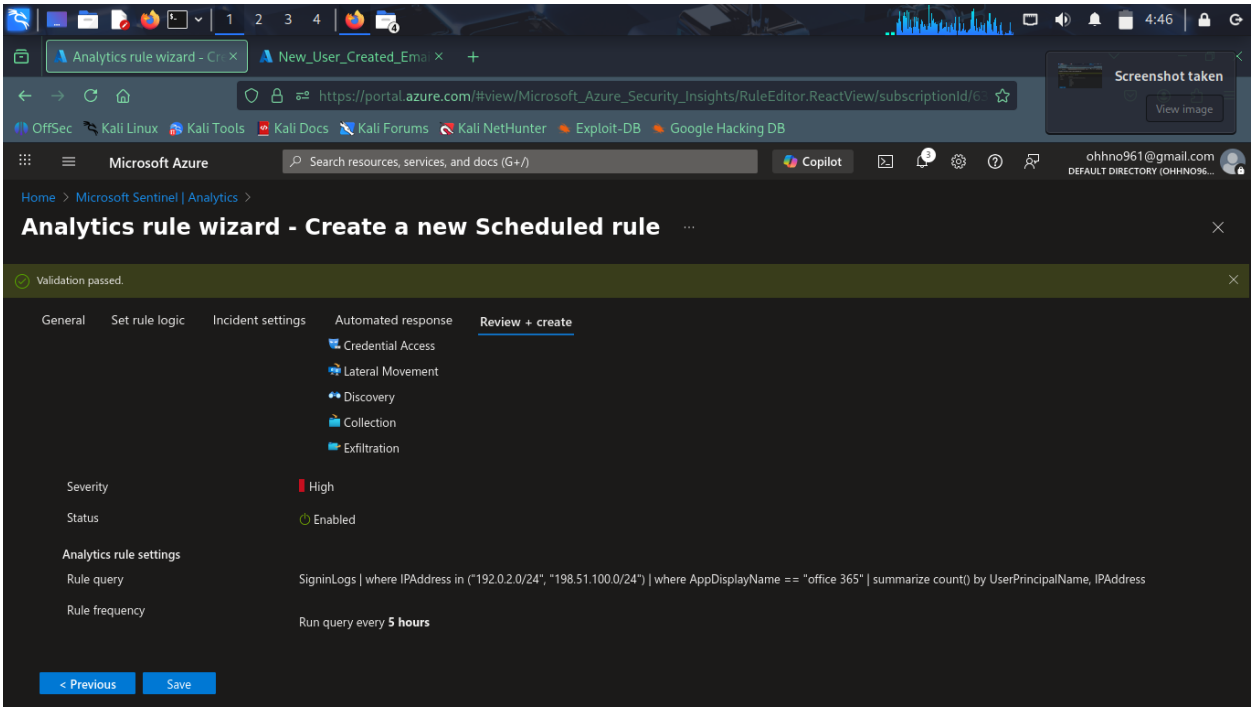
4.3. Creating a Custom Detection Rule Based on APT28 Threat Intelligence

Building upon the APT28 threat intelligence profile, a custom scheduled query rule named "APT28 Activity Detection" was created. This rule is designed to identify potential malicious activity associated with the APT28 threat actor within the organization's environment. The rule's description is: "This rule detects activity associated with the APT28 threat actor, based on known indicators and behaviors." It is assigned a High severity level. The MITRE ATT&CK tactics selected for this rule include Initial Access, Execution, Persistence, Privilege Escalation, Credential Access, Discovery, Lateral Movement, Collection, and Exfiltration, reflecting the broad range of techniques typically employed by APT28. The core of this rule is a KQL query that searches for specific Indicators of Compromise (IoCs) or behavioral patterns linked to APT28.


Analytics rule wizard - Cre
New_User_Created_Ema
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/RuleEditor.ReactView/subscriptionId/6
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Description
This rule detects activity associated with APT28 based on known indicators and behaviours.
Severity
High
MITRE ATT&CK
9 Selected
Status
Enabled
Next : Set rule logic >
Search
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command And Control
Exfiltration
Impact
Evasion


Analytics rule wizard - Cre
New_User_Created_Ema
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/RuleEditor.ReactView/subscriptionId/6
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Define the logic for your new analytics rule.
Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.
SigninLogs
| where IPAddress in ("192.0.2.0/24", "198.51.100.0/24")
| where AppDisplayName == "office 365"
| summarize count() by UserPrincipalName, IPAddress
View query results >
Alert enhancement
< Previous
Next : Incident settings >





Conclusion

The successful implementation of Microsoft Sentinel and the integration of advanced threat intelligence have significantly enhanced the organization's ability to detect, respond to, and mitigate security threats. By automating routine security operations and leveraging threat intelligence, the organization can now proactively identify and address potential

security incidents, reducing the risk of unauthorized access and data breaches. The creation of custom detection rules and threat actor profiles, such as the APT28 profile, further strengthens the organization's defensive capabilities. Moving forward, the organization should continue to refine and expand these capabilities, ensuring that security operations remain robust and adaptive to evolving threats.