**CLOUD-BASED SECURITY MONITORING SYSTEM USING MICROSOFT SENTINEL**

**Project Overview**

This project is a robust cloud-native security monitoring solution built with Microsoft Sentinel. It is designed to:

* Detect brute-force attacks
* Automate incident response
* Provide real-time threat visualization

Leveraging Sentinel's analytics and automation capabilities, this system proactively enhances

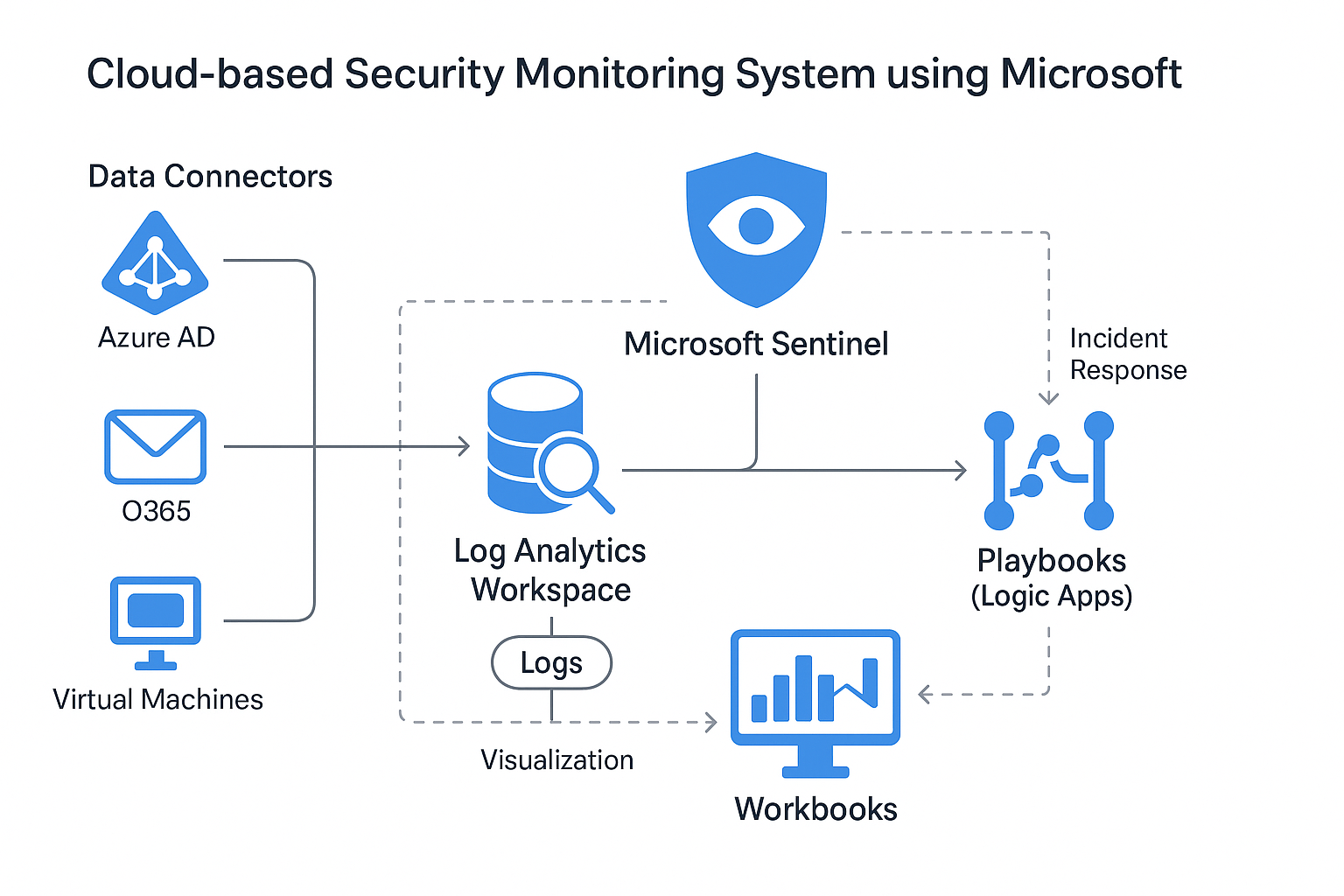
**Features**

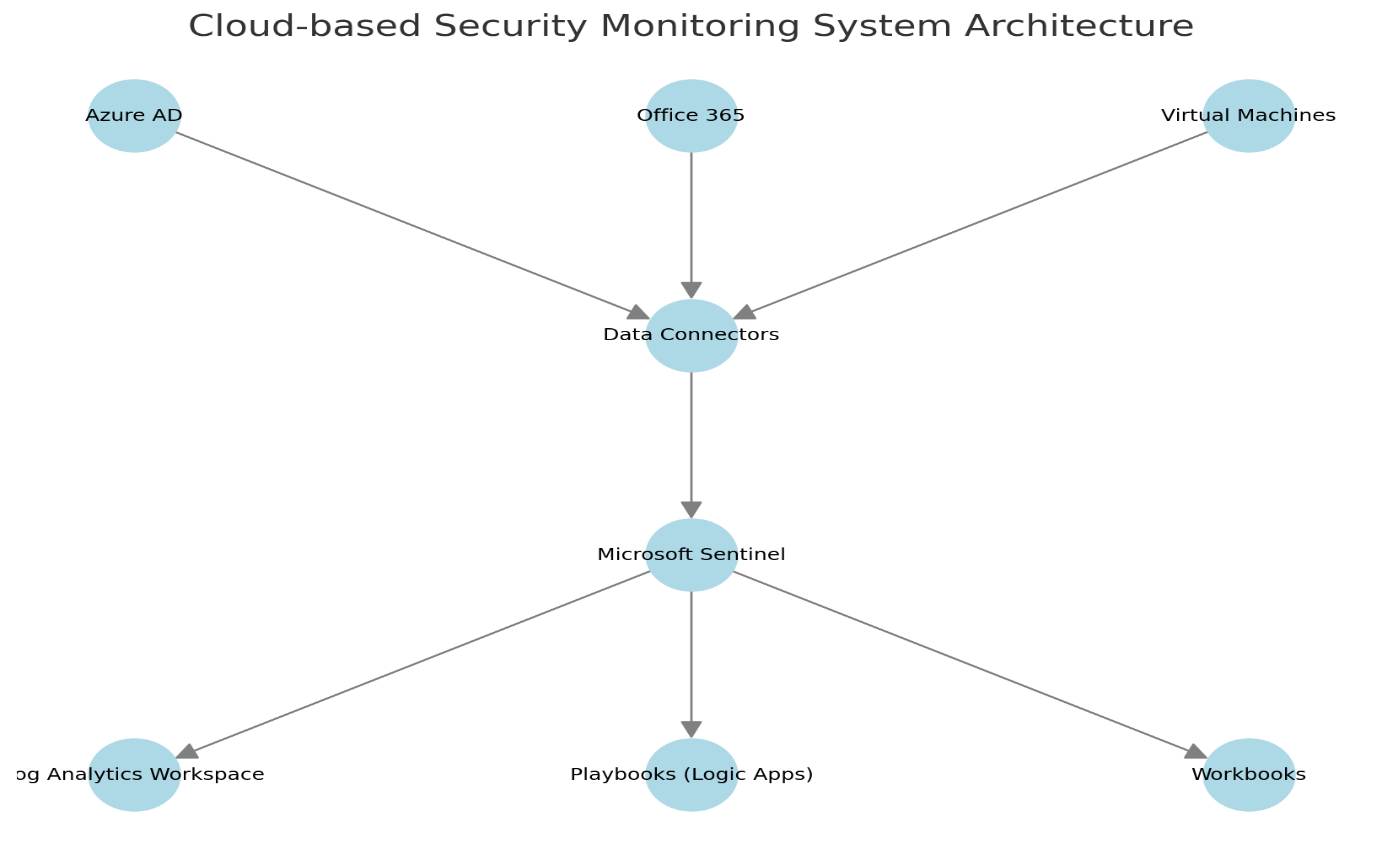
* Brute-force Attack Detection: Identifies unauthorized access attempts on Azure-based resources.
* Automated Incident Response: Deploys predefined playbooks to contain and mitigate threats instantly.
* Real-time Threat Visualization: Displays interactive dashboards for continuous monitoring of security events.
* Scalable and Cloud-Native: Seamlessly integrates with Azure services, supporting large-scale deployments.

**Architecture Diagram**

The architecture includes:

* Microsoft Sentinel: Central SIEM platform for threat detection and incident response.
* Data Connectors: Integration with Azure AD, Office 365, and Virtual Machines for log ingestion.
* Log Analytics Workspace: Secure storage of event logs and analytics data.
* Playbooks (Logic Apps): Automated responses for threat containment and notifications.
* Workbooks: Custom visualizations for threat monitoring.



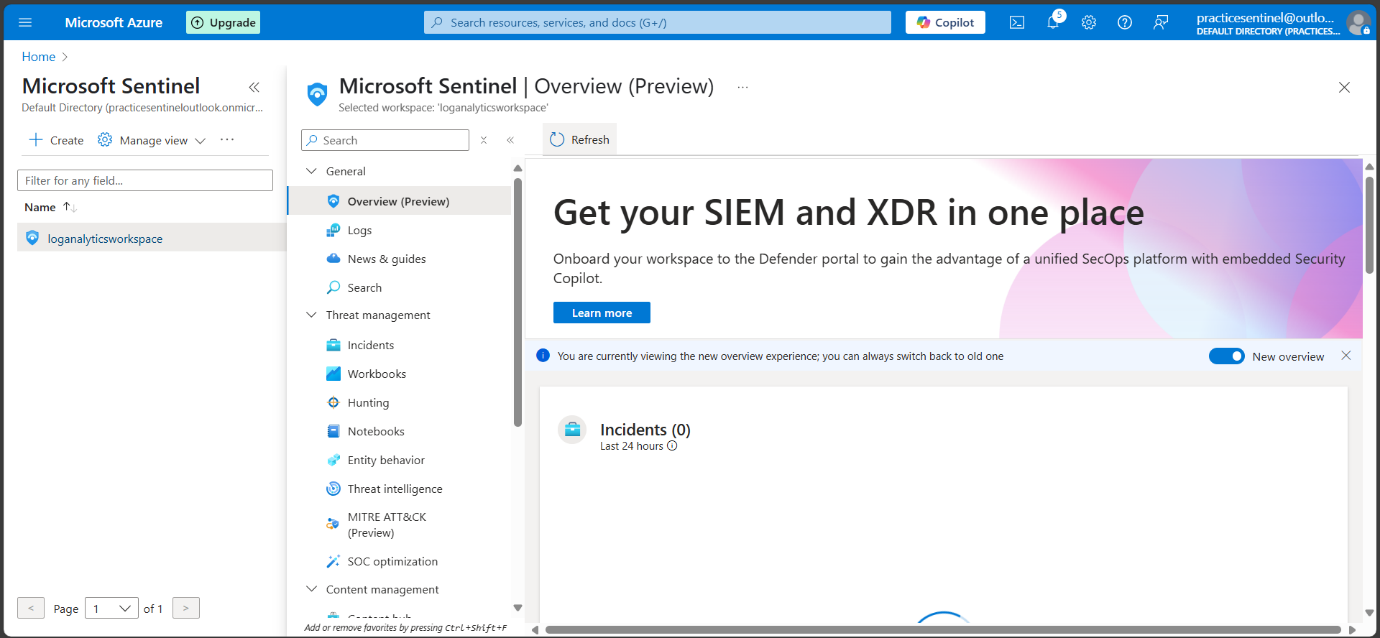
****

**Components:**

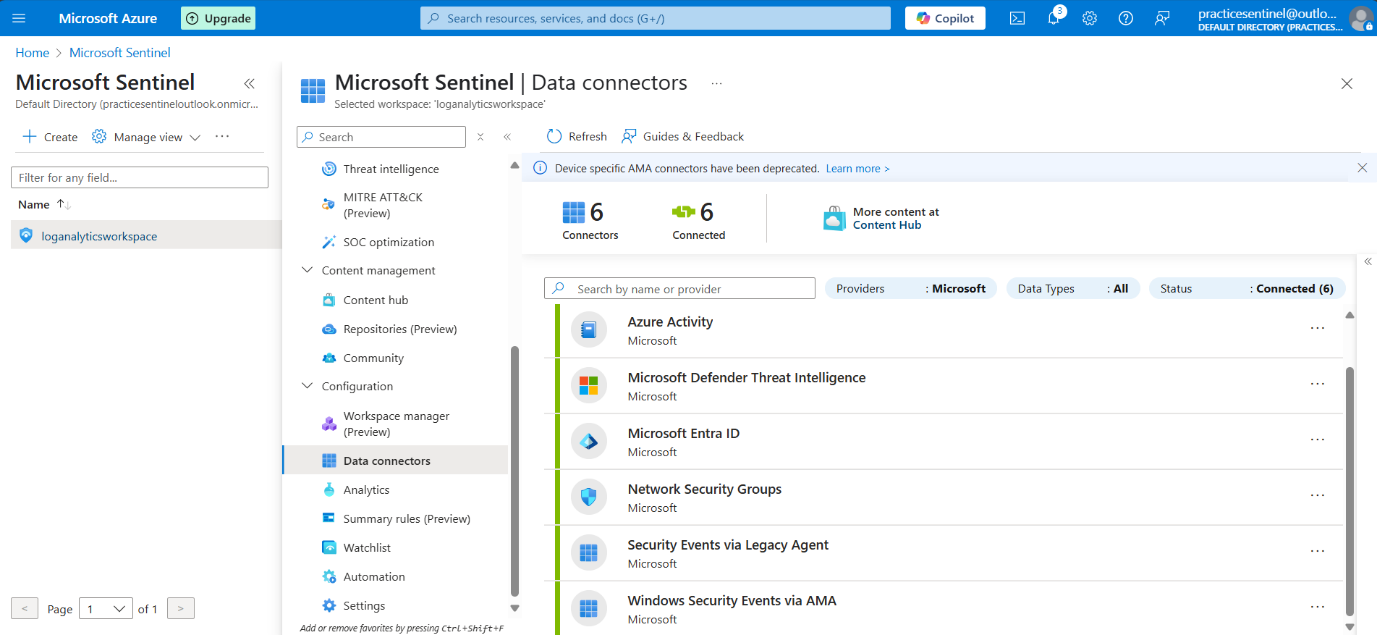
* Microsoft Sentinel: SIEM platform for detection & response.
* Data Connectors: Collect logs from Azure AD, Office 365, and Virtual Machines.
* Log Analytics Workspace: Centralized log storage and analytics.
* Logic Apps (Playbooks): Automate incident response.
* Workbooks: Custom dashboards for monitoring.

**Setup and Configuration**

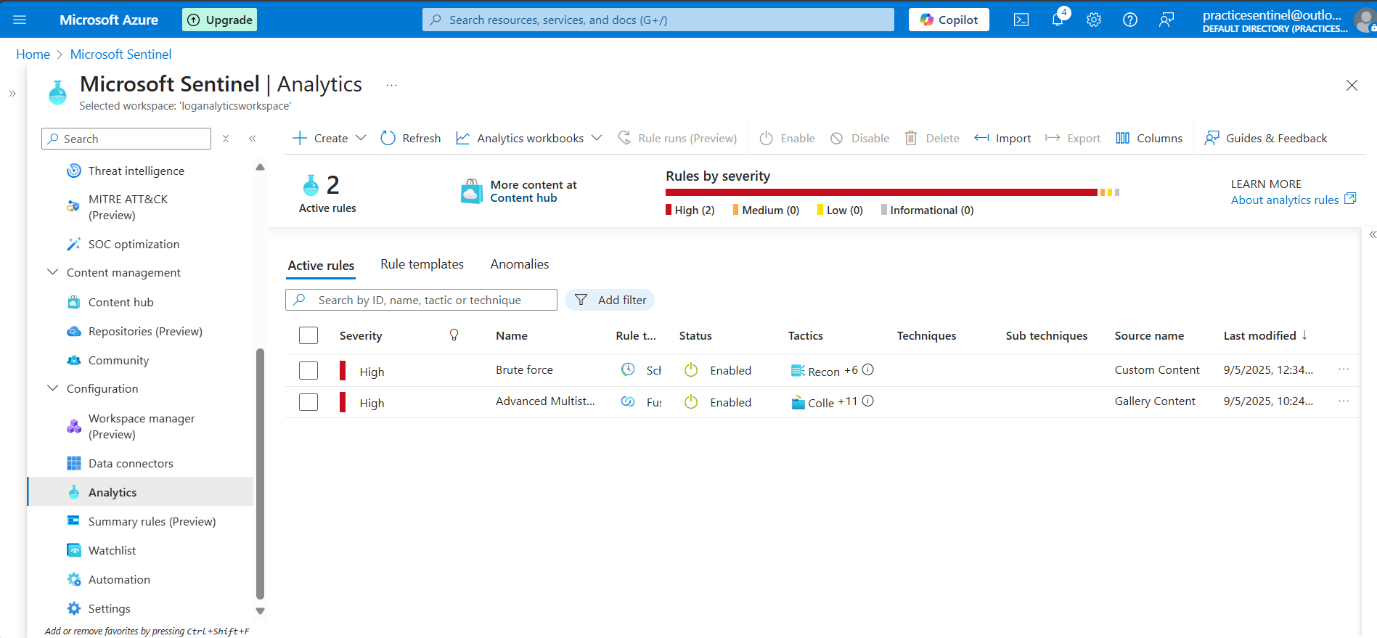
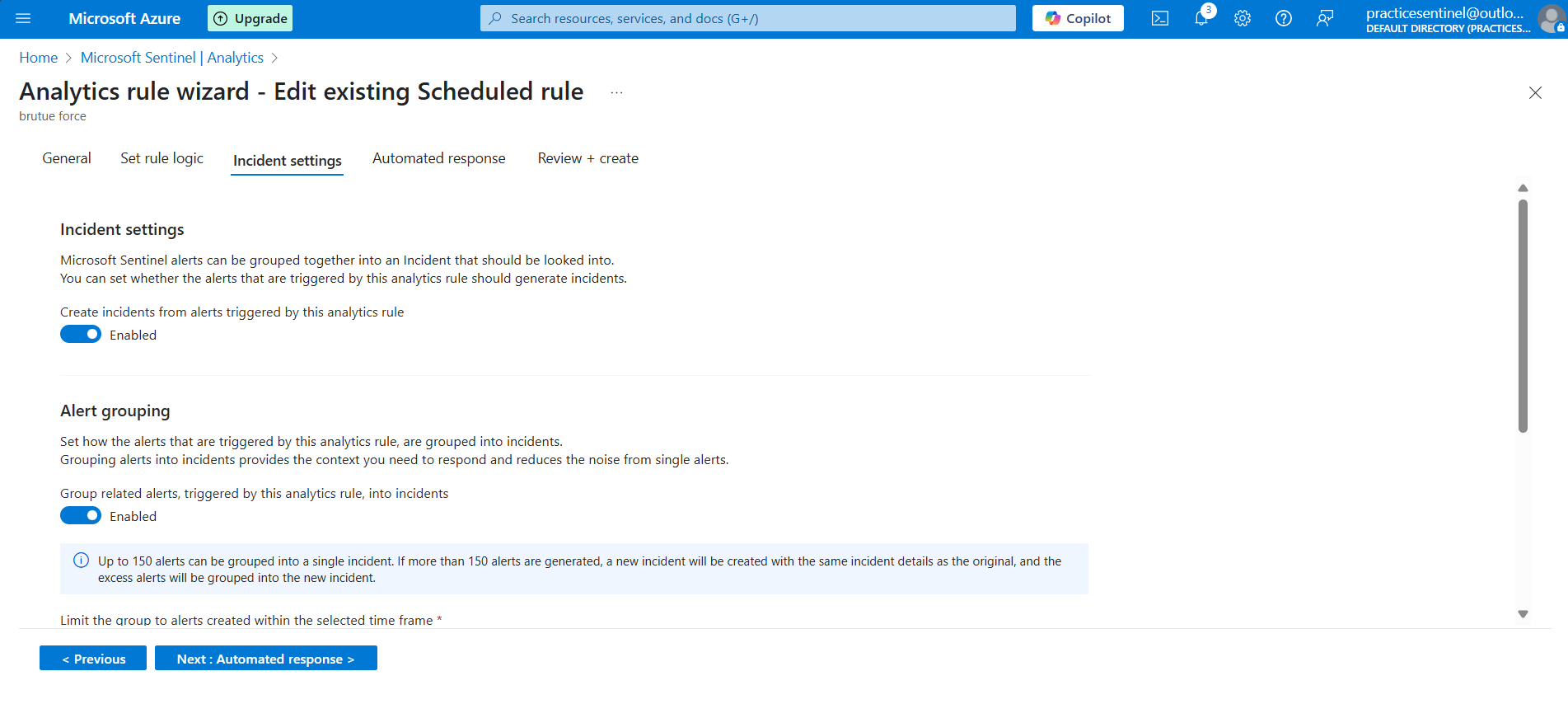
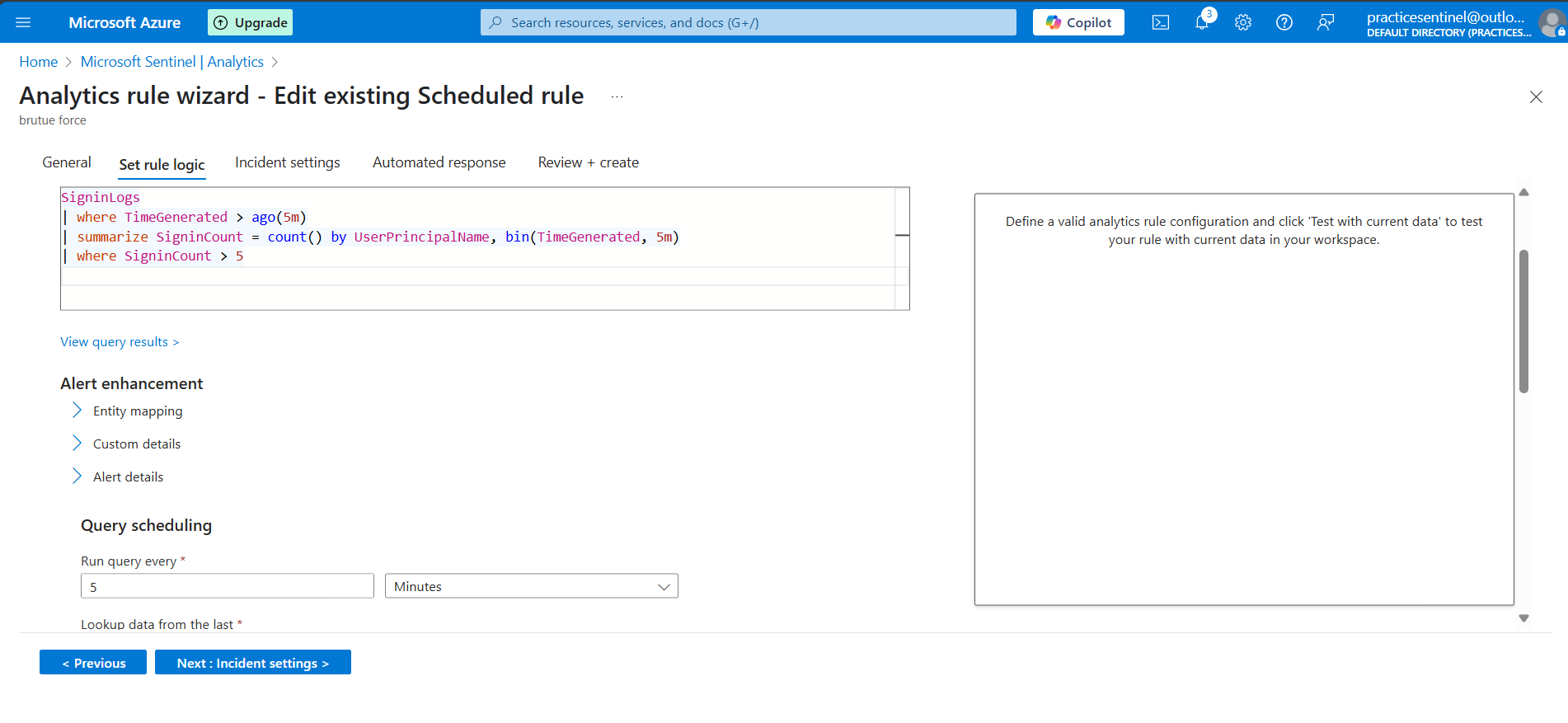
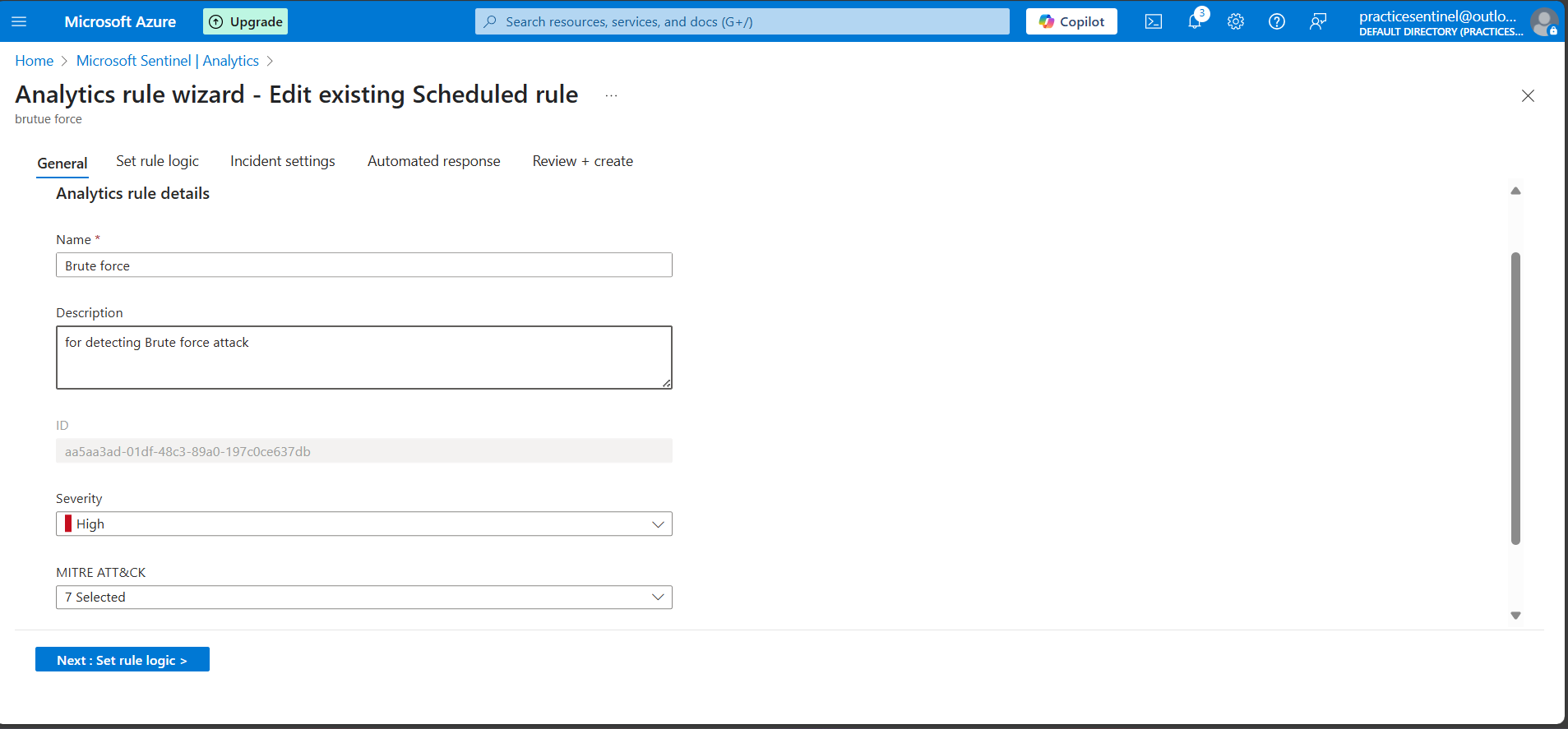
1. Deploy Microsoft Sentinel in the Azure Portal.



1. Configure Data Connectors for Azure AD, Office 365, and Virtual Machines.



1. Create Analytics Rules to detect brute-force attempts and suspicious activities.

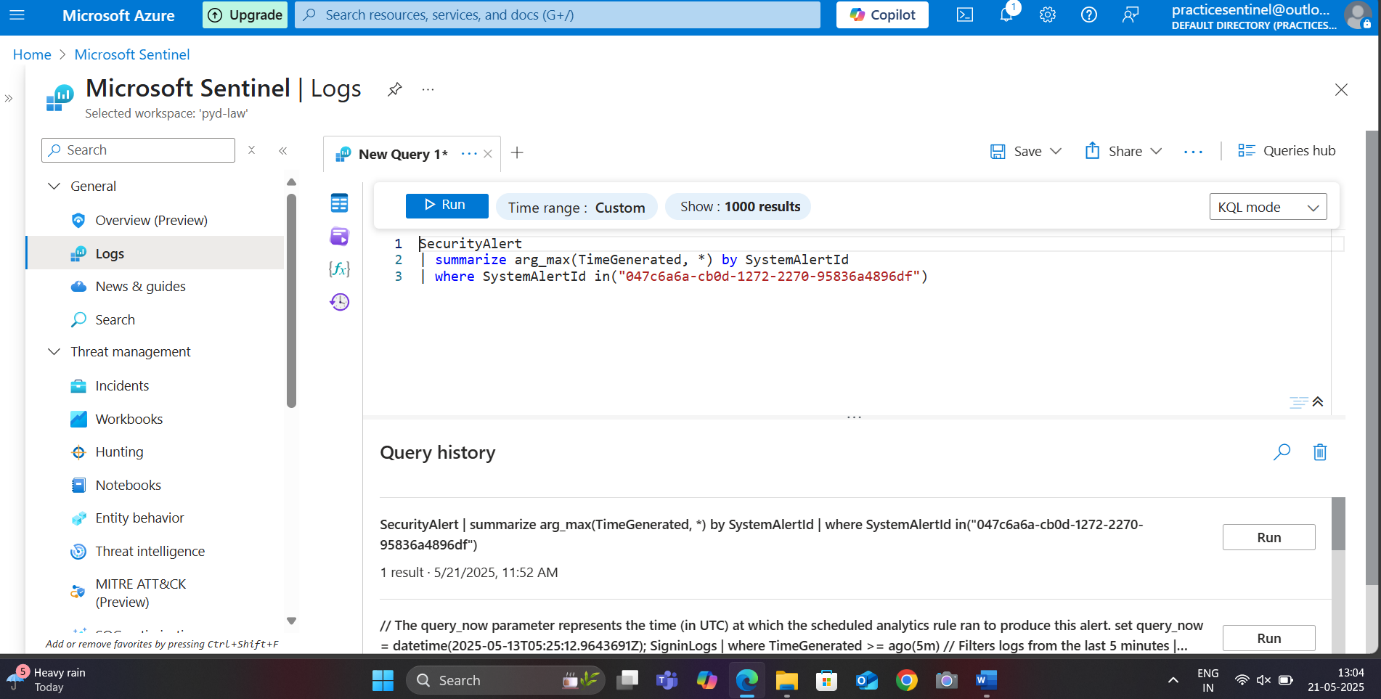


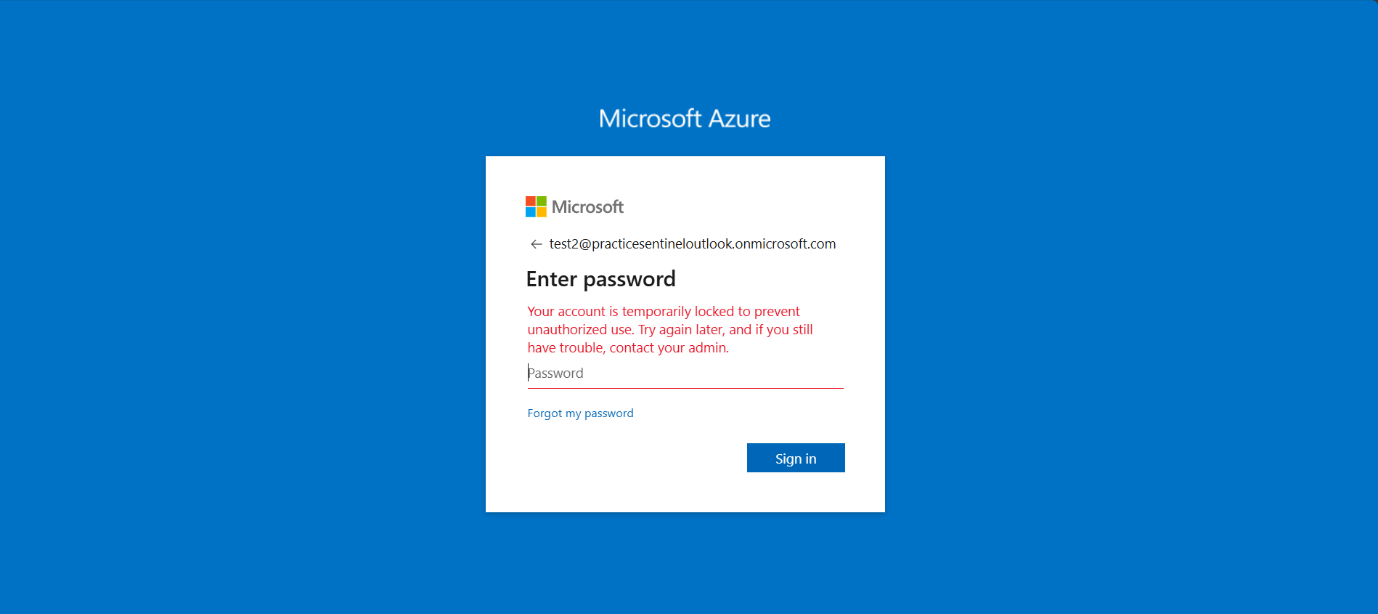
1. Configure Playbooks for automated incident response using Logic Apps.
2. Set up Workbooks for interactive visualization of security metrics.

**Detection Rules and Playbooks**

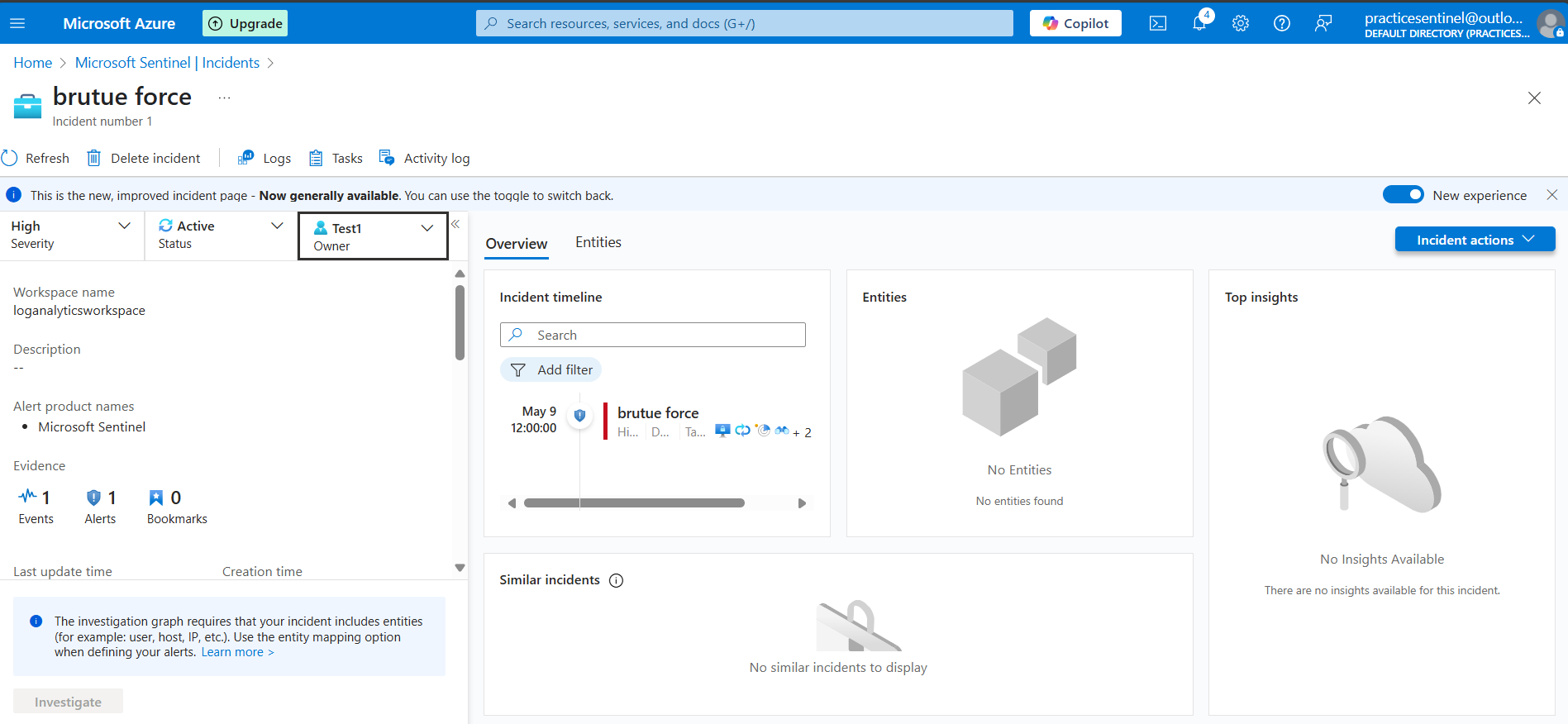
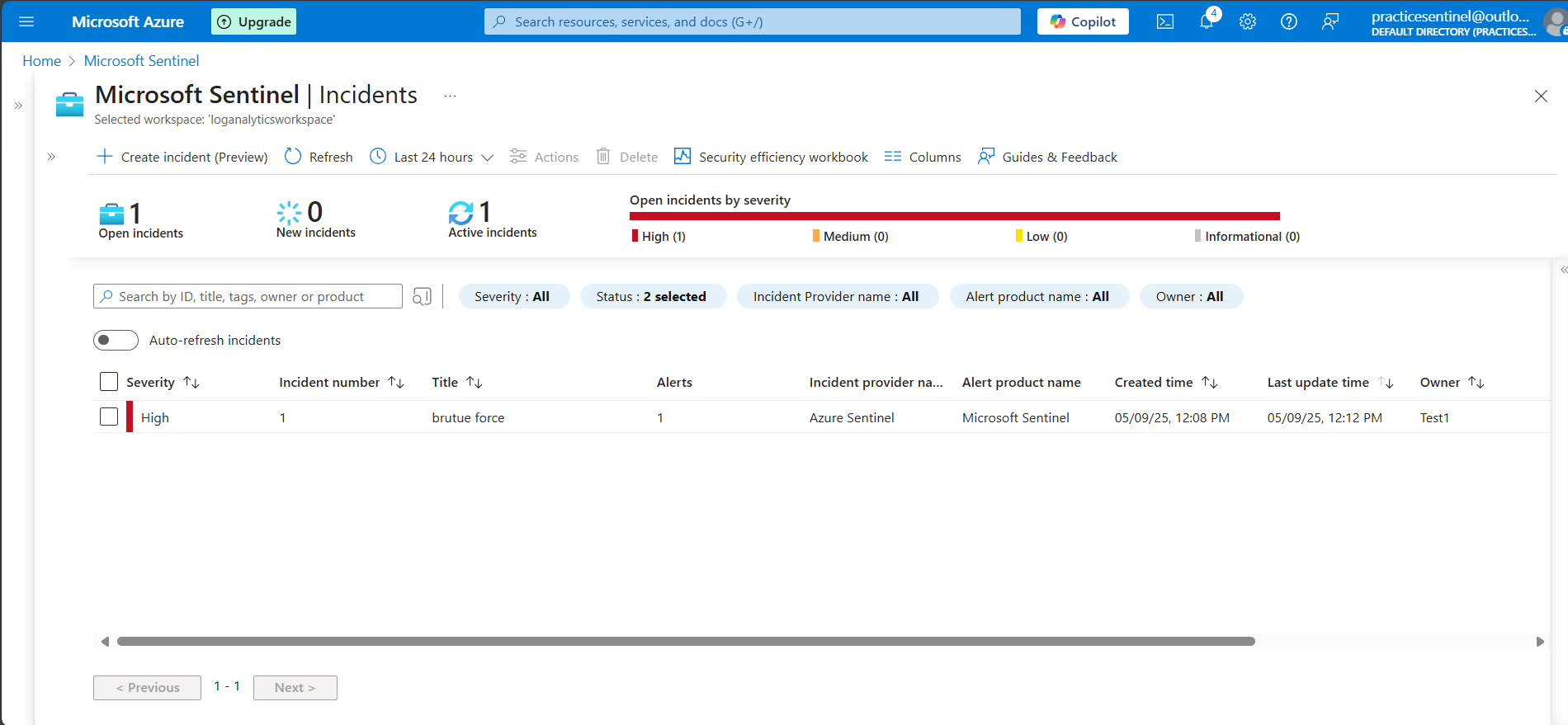
Detection Rules:

* Brute-force attempts on Azure AD





* + Unauthorized access from unknown IP addresses
  + Multiple failed login attempts within short time frames



**Detection Rules**

* Brute-force attempts on Azure AD
* Unauthorized login from unknown IPs
* Repeated login failures in a short span

KQL :

SigninLogs

where ResultType != 0

summarize FailedAttempts = count() by UserPrincipalName, IPAddress, bin(TimeGenerated, 5m)

where FailedAttempts > 5

**Playbooks:**

* + Lock out user accounts upon brute-force detection
  + Apply firewall rules to block malicious IP addresses
  + Send real-time alerts to the SOC team

**Incident Response Automation**

The incident response is fully automated to:

* Contain Threats: Lock compromised accounts and block IP addresses.
* Trigger Firewall Rules: Automatically update firewall policies based on threat detection.
* Notify Administrators: Immediate alerts sent to administrators via email and Microsoft Teams.

**Note**: ||||||||||||||||||||||||||||||||||||||||||||||||

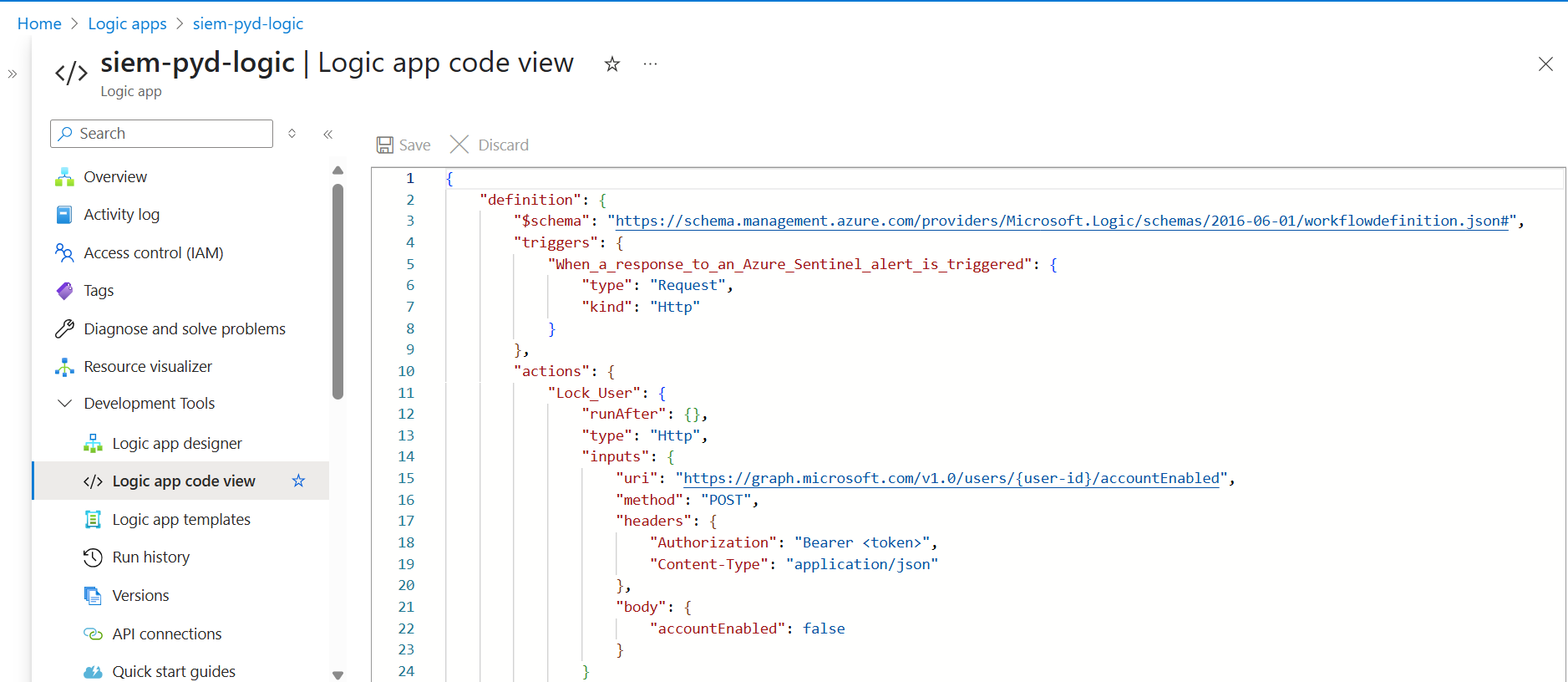
How to Import a Playbook JSON (Manually)

1. In your Logic App, go to the left sidebar and click:

Logic app code view (just below "Logic app designer")

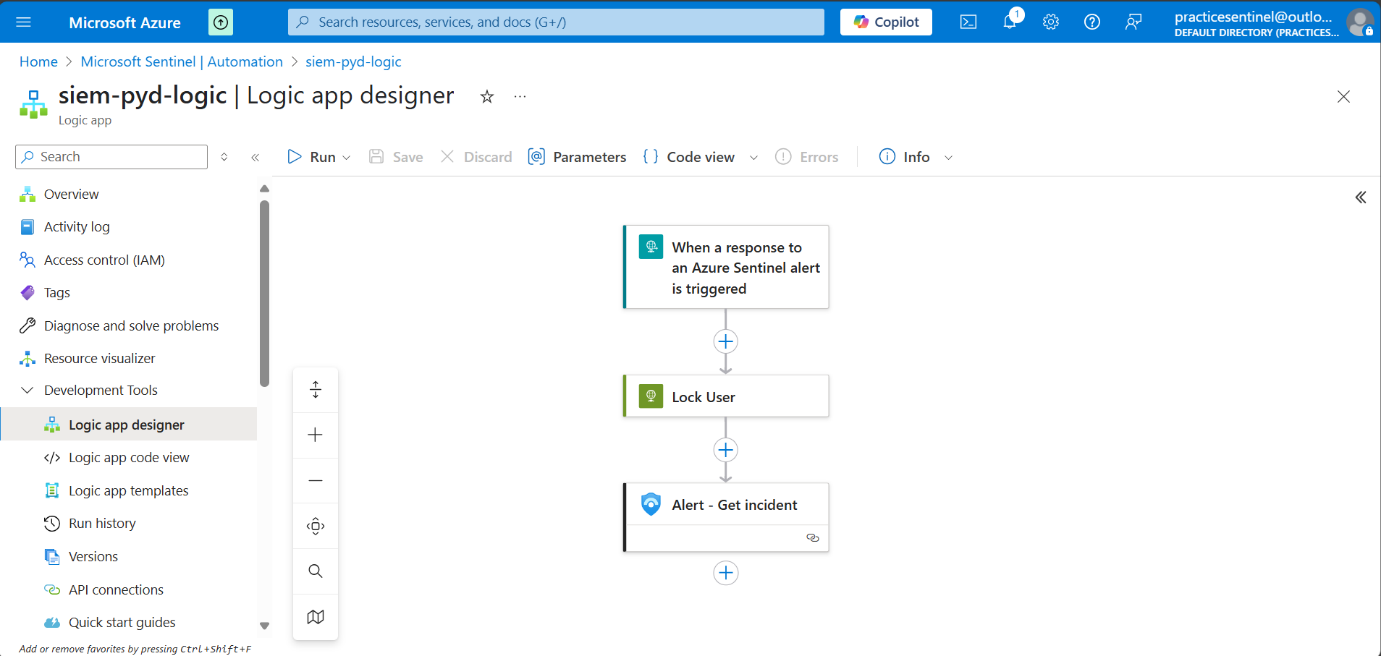
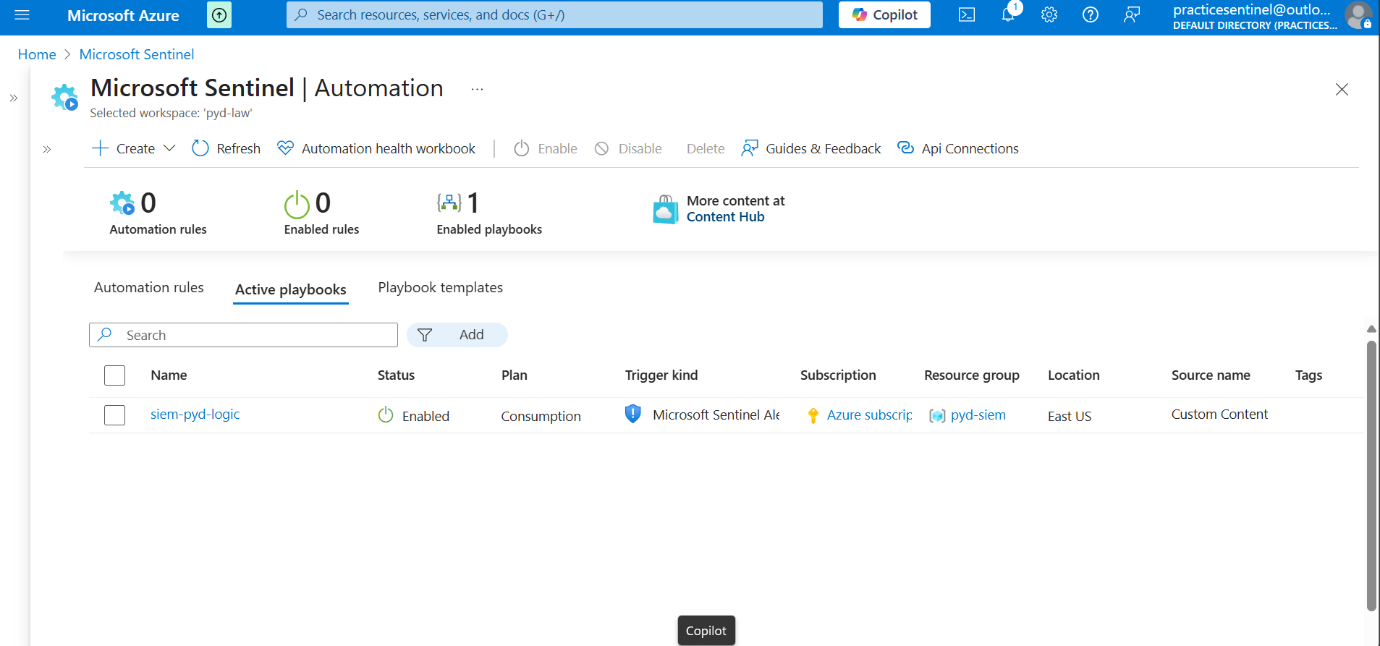
1. Delete everything in the existing code (if this is a new Logic App).
2. Paste the entire JSON content from one of the playbook files:
   * Download playbook-lock-user.json
   * Download playbook-alert-teams.json
3. Click Save (top menu).
4. Now go back to Logic app designer, and you’ll see the full workflow diagrammatically.
5. Click “Create” → “Automation rule”  
   (This starts the creation of a rule that can trigger your existing Logic App)
6. Fill in the rule details:
   * Name: e.g., Brute Force Alert Auto-Response
   * Conditions: Set based on the analytics rule (or leave default for now)
   * Actions:
     1. Select “Run playbook”
     2. Choose your Logic App from the list (e.g., siem-pyd-logic)
7. Click Create to save the automation rule.

This will connect the existing Logic App (your playbook) to Sentinel without needing “+ Add existing” explicitly. |||||||||||||||||||||||||||||||||||||||||||||||||||||



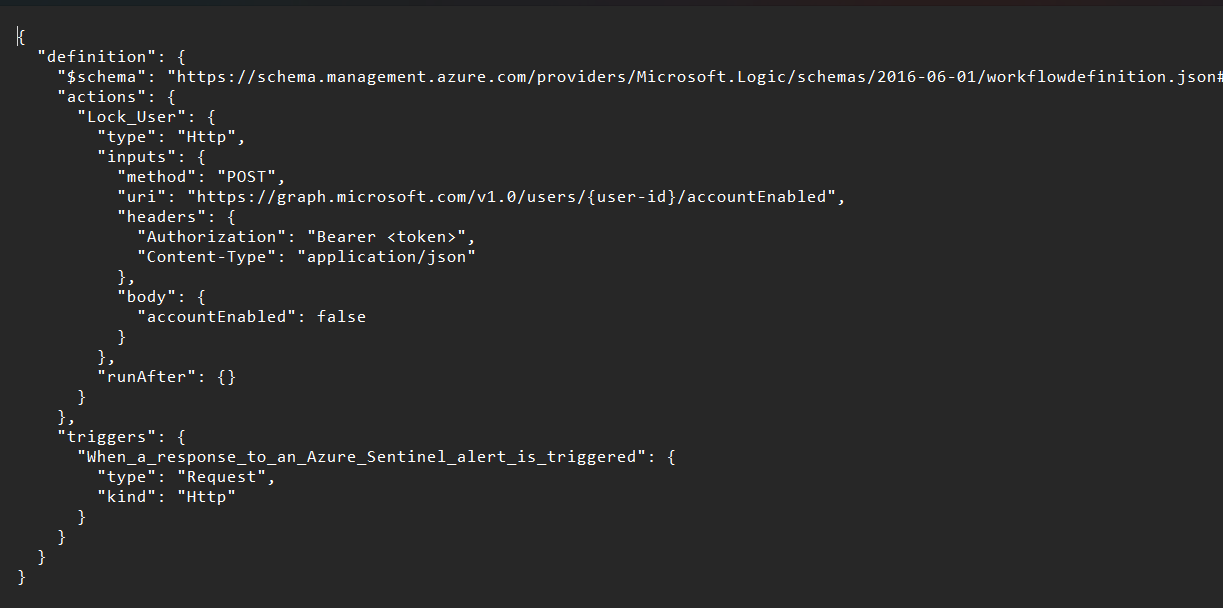
Top of Form

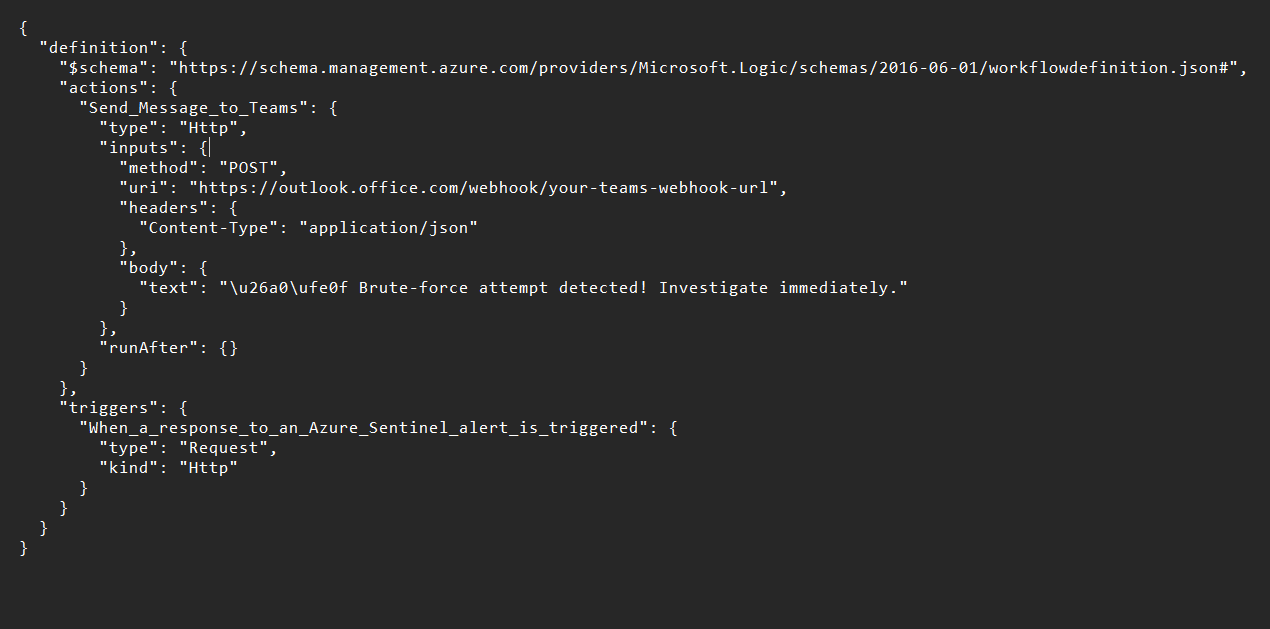
Bottom of Form



* Download detection-rule-brute-force.kql
* Download playbook-lock-user.json
* Download playbook-alert-teams.json

**Playbook-Lock-User**

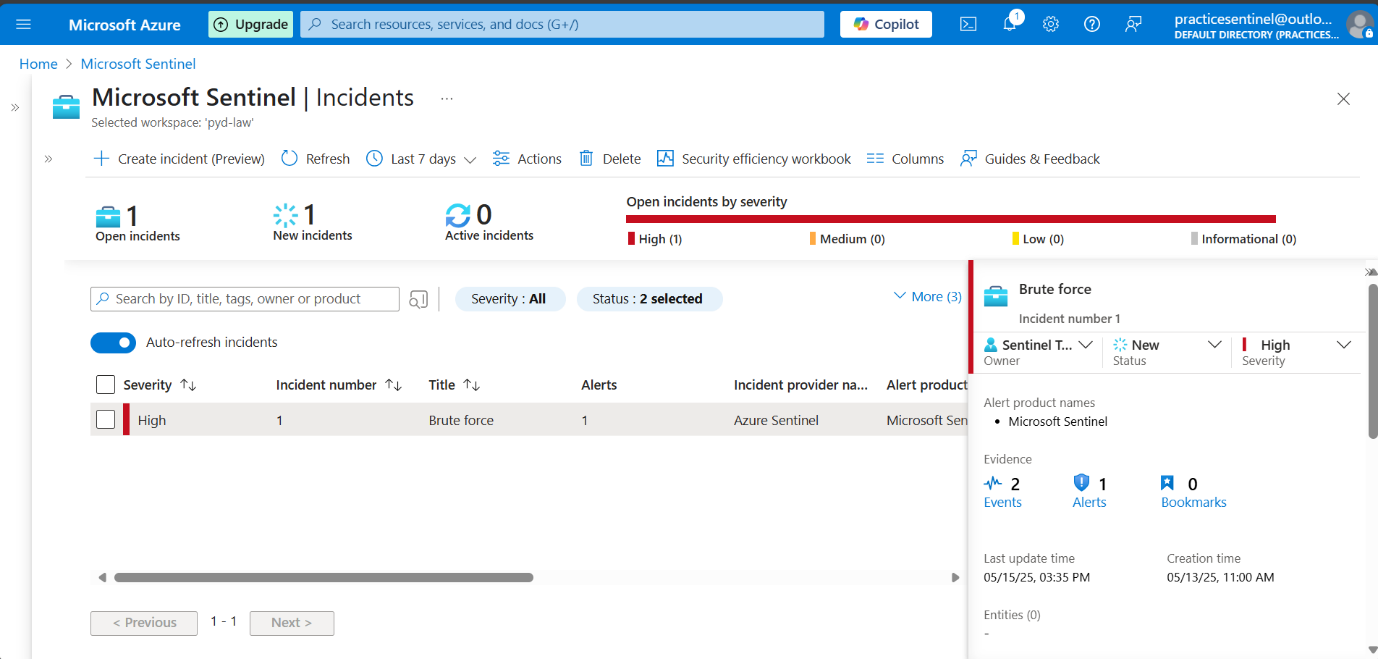


**Playbook-alert-teams**

**Visualization and Dashboards**

Interactive Dashboards:

* Overview of brute-force attempts
* Geographic distribution of attack origins
* Incident response timelines and resolutions



**Future Enhancements**

* Integration with External Threat Intelligence for proactive defense
* Machine Learning-based Anomaly Detection for advanced threat hunting
* Multi-cloud Support for AWS and GCP environments

**Contributing Guidelines**

Contributions are welcome. Please follow the guidelines for pull requests and include detailed descriptions of your changes.

**License and Acknowledgements**

MIT License. Special thanks to Microsoft for their documentation and the cybersecurity community for sharing best practices and insights.