



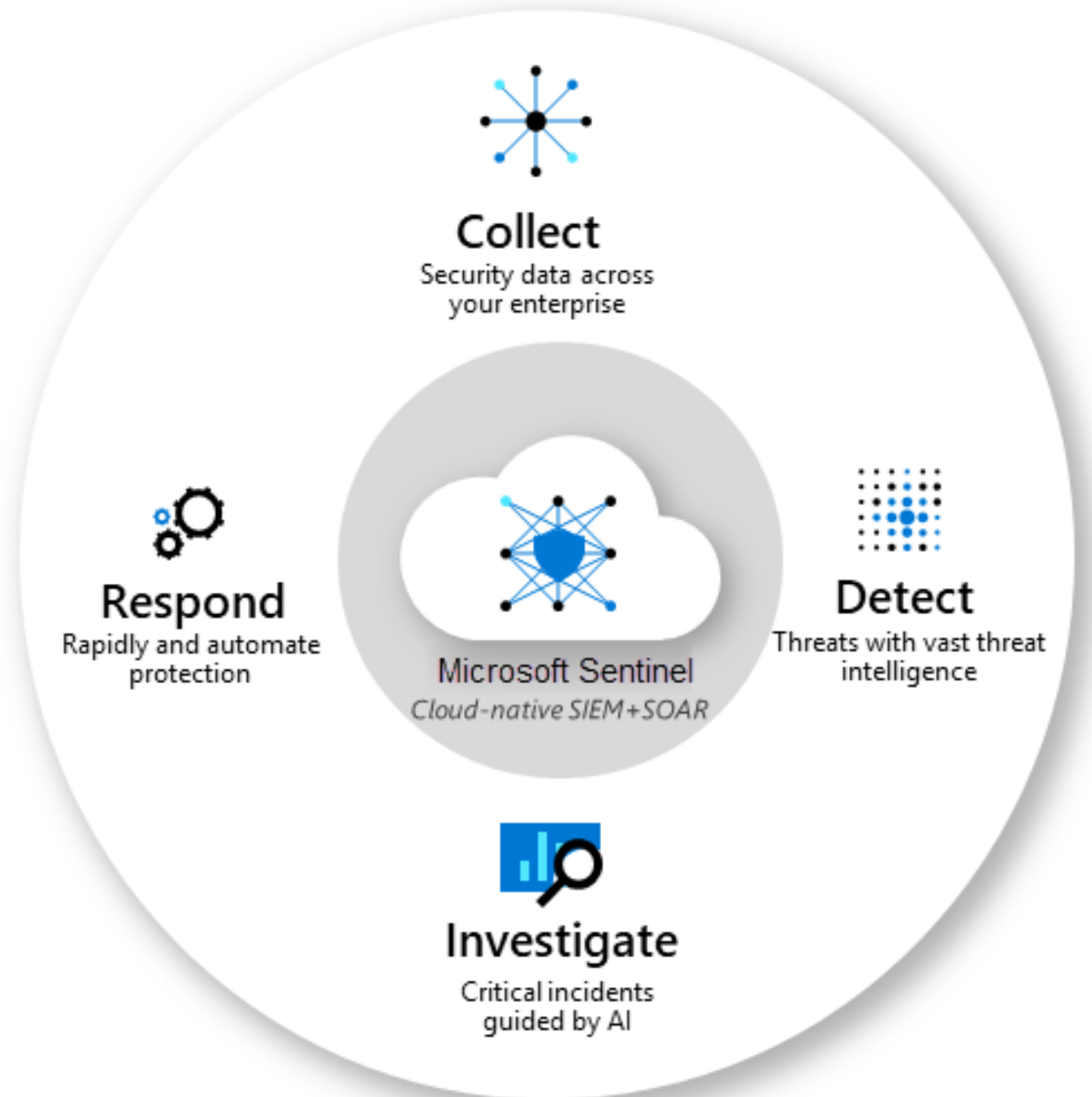
Microsoft Sentinel

KlayyTech Security Radar

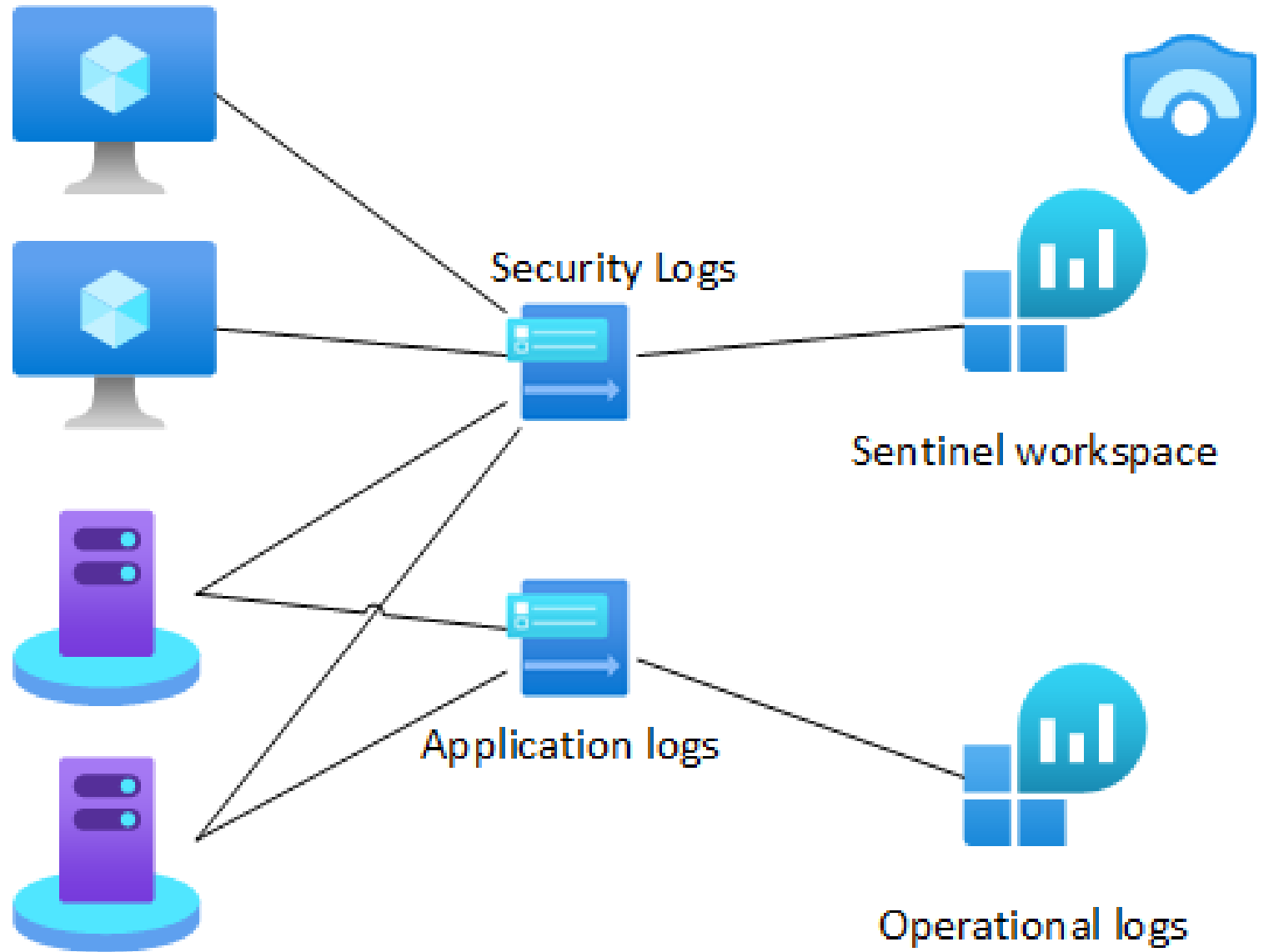
What is KlayyTech Security Radar

It's Based on Microsoft Sentinel with a lot of custom features as follows:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR) with a lot of automatic response.

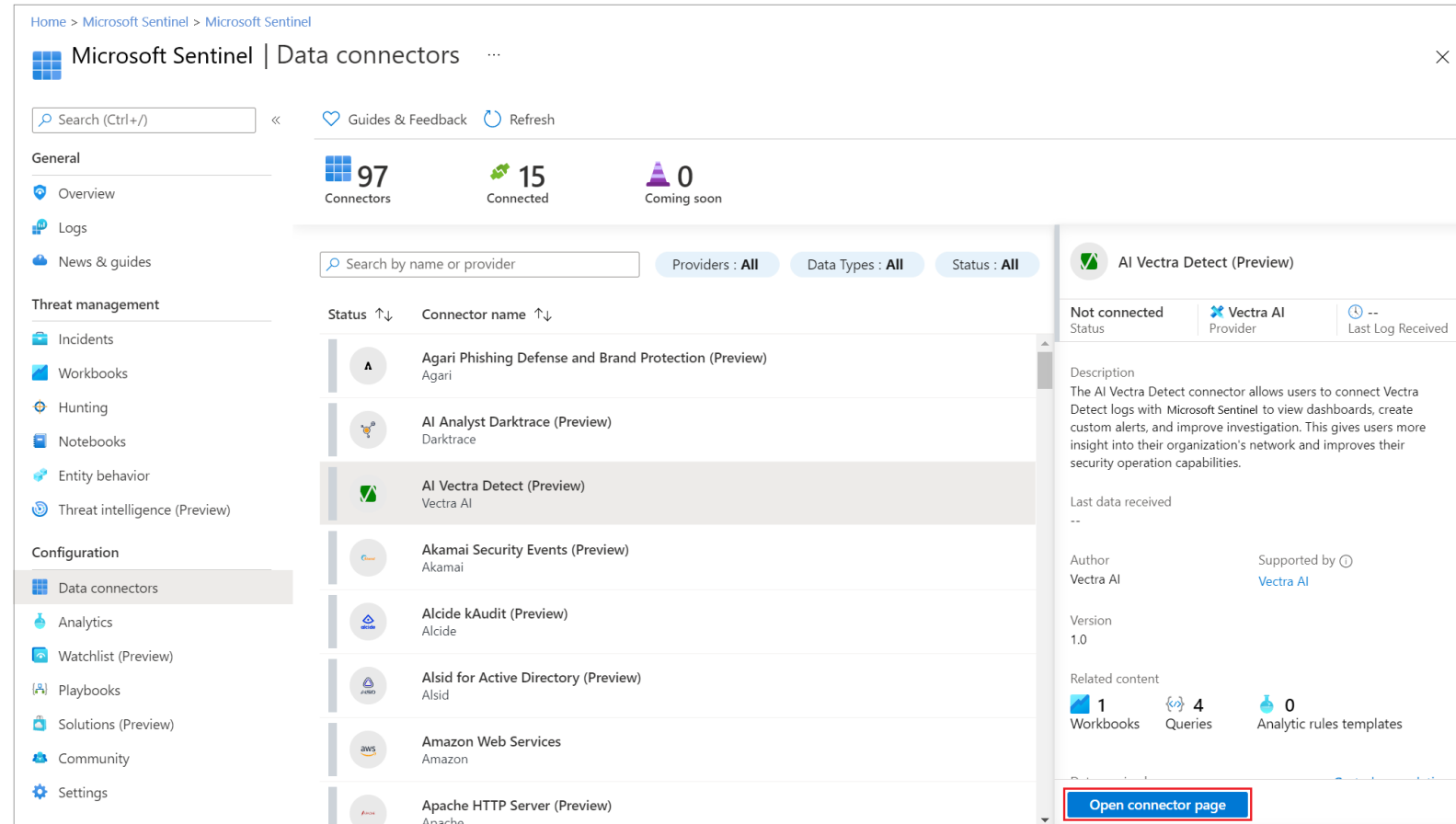


collect



Collect data by using data connectors

- Microsoft sources like Microsoft 365 Defender, Microsoft Defender for Cloud, Office 365, Microsoft Defender for IoT, and more.
- Azure service sources like Azure Active Directory, Azure Activity, Azure Storage, Azure Key Vault, Azure Kubernetes service, and more.



The screenshot displays the Microsoft Sentinel Data connectors interface. The top navigation bar shows the breadcrumb path: Home > Microsoft Sentinel > Microsoft Sentinel. The main header is "Microsoft Sentinel | Data connectors". Below the header, there is a search bar and navigation options like "Guides & Feedback" and "Refresh".

The interface is divided into two main sections: a left-hand navigation menu and a main content area. The navigation menu includes sections for "General" (Overview, Logs, News & guides), "Threat management" (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence (Preview)), and "Configuration" (Data connectors, Analytics, Watchlist (Preview), Playbooks, Solutions (Preview), Community, Settings). The "Data connectors" option is currently selected.

The main content area displays a summary of connectors: 97 Connectors, 15 Connected, and 0 Coming soon. Below this, there is a search bar and filter buttons for "Providers: All", "Data Types: All", and "Status: All". A table lists the connectors with columns for "Status" and "Connector name". The "AI Vectra Detect (Preview)" connector is highlighted.










Status	Connector name
Not connected	Agari Phishing Defense and Brand Protection (Preview) Agari
Not connected	AI Analyst Darktrace (Preview) Darktrace
Connected	AI Vectra Detect (Preview) Vectra AI
Not connected	Akamai Security Events (Preview) Akamai
Not connected	Alcide kAudit (Preview) Alcide
Not connected	Alsid for Active Directory (Preview) Alsid
Not connected	Amazon Web Services Amazon
Not connected	Apache HTTP Server (Preview) Apache

The details panel for "AI Vectra Detect (Preview)" is open on the right. It shows the status as "Not connected" and the provider as "Vectra AI". The description states: "The AI Vectra Detect connector allows users to connect Vectra Detect logs with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation. This gives users more insight into their organization's network and improves their security operation capabilities." It also shows the last data received as "--", the author as "Vectra AI", and the version as "1.0". There are 1 Workbook, 4 Queries, and 0 Analytic rules templates related to this connector. A red box highlights the "Open connector page" button at the bottom.

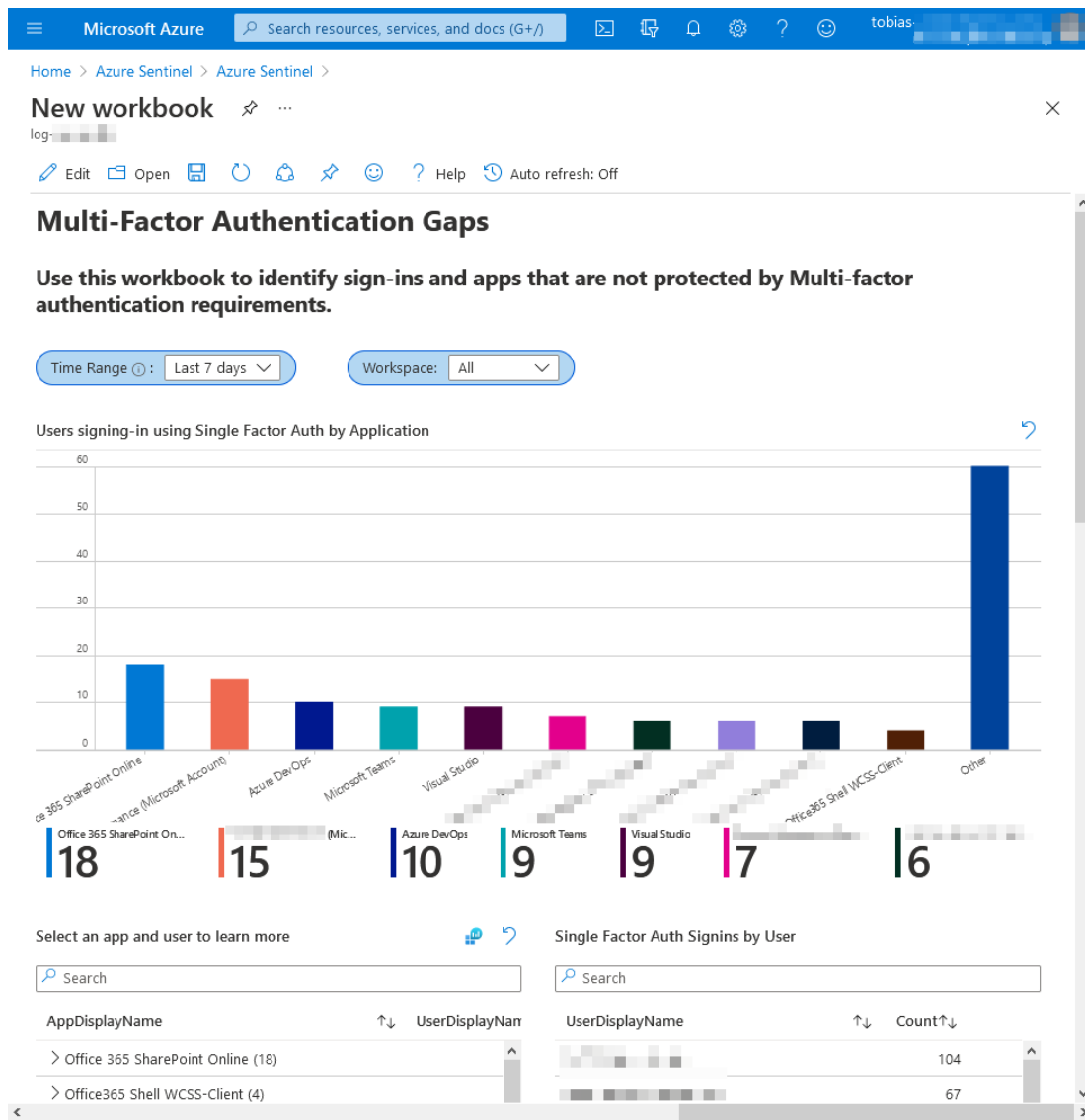
Connectors

127 Connectors 11 Connected More content at Content hub

Search by name or provider Providers : All Data Types : All **Status : Connected**

Status	Connector name ↑
	 Azure Active Directory Microsoft
	 Azure Activity Microsoft
	 Azure Key Vault Microsoft
	 Barracuda Web Application Firewall Barracuda
	 Microsoft 365 Defender Microsoft
	 Microsoft Defender for Cloud Microsoft
	 Network Security Groups Microsoft
	 Office 365 Microsoft
	 Security Events via Legacy Agent Microsoft

Custom Visualization



Create Custom interactive reports by using workbooks

Microsoft Sentinel allows you to create custom workbooks across your data. Microsoft Sentinel also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source

The screenshot displays the Microsoft Sentinel Workbooks interface. The top navigation bar shows 'Home > Microsoft Sentinel > Microsoft Sentinel'. The main header is 'Microsoft Sentinel | Workbooks' with a sub-header 'Selected workspace: 'cybersoc-demo''. Below the header, there is a search bar and a 'Refresh + Add workbook' button. The interface is divided into three main sections: 'General', 'Threat management', and 'Configuration'. The 'General' section shows '1 Saved workbooks', '90 Templates', and '0 Updates'. The 'Threat management' section includes 'Overview', 'Logs', 'News & guides', 'Incidents', 'Workbooks', 'Hunting', 'Notebooks', 'Entity behavior', and 'Threat intelligence (Preview)'. The 'Configuration' section includes 'Data connectors', 'Analytics', 'Watchlist (Preview)', 'Automation', 'Community', and 'Settings'. The 'Workbooks' section is currently selected, showing a list of templates. The 'Analytics Efficiency' template by MICROSOFT is highlighted. A red box highlights the 'Required data types' section, which lists 'SecurityAlert' and 'SecurityIncident' with green checkmarks. Below the list, there is a preview of the 'Analytics Efficiency' workbook, which includes a bar chart and a table. At the bottom right, there are 'View template' and 'Save' buttons.

Correlate alerts into incidents by using analytics rules

To help you reduce noise and minimize the number of alerts you have to review and investigate, Microsoft Sentinel uses analytics to correlate alerts into incidents

The screenshot displays the Microsoft Sentinel 'Incidents' dashboard. At the top, it shows 403 Open incidents, 400 New incidents, and 3 Active incidents. A bar chart indicates the distribution of incidents by severity: High (82), Medium (95), Low (207), and Informational (19). The main table lists incidents with columns for Severity, Status, Incident ID, Title, Alerts, Product names, and Created time. The selected incident, ID 203443, is titled 'Authentication Methods Changed for Privileged Acc...'. The detailed view on the right shows the incident description, alert product names (Microsoft Sentinel), evidence (1 Events, 1 Alerts, 0 Bookmarks), last update time (05/11/22, 12:50 PM), and creation time (05/11/22, 12:49 PM). The interface also includes a search bar, filters for Severity, Status, Product name, and Owner, and a navigation pane on the left with categories like General, Threat management, Content management, Configuration, and Automation.

Severity	Status	Incident ID	Title	Alerts	Product names	Created time
High	New	203444	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 12:52 PM
High	New	203443	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 12:49 PM
High	New	203440	User login from different countri...	1	Microsoft Sentinel	05/11/22, 12:41 PM
High	New	203437	Preview: User and IP address rec...	2	Microsoft Defender fo...	05/11/22, 12:25 PM
High	New	203436	Preview: Suspicious PowerShell c...	2	Microsoft Defender fo...	05/11/22, 12:23 PM
High	New	203435	Preview: Network intrusion dete...	2	Microsoft Defender fo...	05/11/22, 12:23 PM
High	New	203426	Preview: Multiple alerts possibly ...	5	Microsoft Defender fo...	05/11/22, 11:52 AM
High	New	203425	Preview: Multiple alerts possibly ...	11	Microsoft Cloud App ...	05/11/22, 11:52 AM
High	New	203424	Preview: Crypto-mining activity f...	2	Azure Defender, Azur...	05/11/22, 11:52 AM
High	New	203423	Impossible travel to atypical loca...	2	Azure Active Directory...	05/11/22, 11:52 AM
High	New	203421	Preview: Suspicious PowerShell c...	2	Azure Active Directory...	05/11/22, 11:51 AM
High	New	203422	Preview: Multiple alerts possibly ...	16	Microsoft Defender fo...	05/11/22, 11:51 AM
High	New	203420	Preview: Connection to web pag...	2	Azure Defender, Micr...	05/11/22, 11:48 AM
High	New	203419	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 11:39 AM

Custom analytic rules

The screenshot shows the Microsoft Sentinel Analytics dashboard. At the top, there is a search bar and navigation icons for 'Create', 'Refresh', and 'Analytics workbook'. A dropdown menu is open under the 'Create' button, listing options: 'Scheduled query rule' (highlighted with a red box), 'NRT query rule (Preview)', and 'Microsoft incident creation rule'. Below the menu, there is a summary bar for 'Active rules' with a red bar indicating 'High (102)', an orange bar for 'Medium (43)', a yellow bar for 'Low (5)', and a grey bar for 'Informational'. The 'Active rules' tab is selected at the bottom.

Analytics rule wizard - Create a new scheduled rule

General **Set rule logic** Incident settings Automated response Review and 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.

```
SecurityAlert
| where ProviderName == 'MicrosoftNetworkProtection' and AlertType == 'AnomalousNetworkTraffic'
```

[View query results >](#)

Alert enrichment

Custom created rules

- Login to disabled account
- Account lock
- Failed logins for the same account more than 5 times in an hour
- Signing in using single factor authentication
- Signing in outside geographical location
- Suspicious access to sensitive servers
- Sign in outside of working hours
- Deleting server logs
- Unusual DNS queries
- Failed SQL database access attempts
- Unusual VPN logins

Incidents

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'Contoso'

Search (Ctrl+/) Refresh Last 24 hours Actions Security efficiency workbook Columns Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors
- Analytics
- Watchlist
- Automation

403 Open Incidents 400 New incidents 3 Active incidents

Open incidents by severity: High (82) Medium (95) Low (207) Informational (19)

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

Auto-refresh incidents

Severity	Status	Incident ID	Title	Alerts	Product names	Created time
High	New	203444	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 12:52 PM
High	New	203443	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 12:49 PM
High	New	203440	User login from different countri...	1	Microsoft Sentinel	05/11/22, 12:41 PM
High	New	203437	Preview: User and IP address rec...	2	Microsoft Defender fo...	05/11/22, 12:25 PM
High	New	203436	Preview: Suspicious PowerShell c...	2	Microsoft Defender fo...	05/11/22, 12:23 PM
High	New	203435	Preview: Network intrusion dete...	2	Microsoft Defender fo...	05/11/22, 12:23 PM
High	New	203426	Preview: Multiple alerts possibly ...	5	Microsoft Defender fo...	05/11/22, 11:52 AM
High	New	203425	Preview: Multiple alerts possibly ...	11	Microsoft Cloud App ...	05/11/22, 11:52 AM
High	New	203424	Preview: Crypto-mining activity f...	2	Azure Defender, Azur...	05/11/22, 11:52 AM
High	New	203423	Impossible travel to atypical loca...	2	Azure Active Directory...	05/11/22, 11:52 AM
High	New	203421	Preview: Suspicious PowerShell c...	2	Azure Active Directory...	05/11/22, 11:51 AM
High	New	203422	Preview: Multiple alerts possibly ...	16	Microsoft Defender fo...	05/11/22, 11:51 AM
High	New	203420	Preview: Connection to web pag...	2	Azure Defender, Micr...	05/11/22, 11:48 AM
High	New	203410	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 11:30 AM

Authentication Methods Changed for Privileged Account
Incident ID: 203443

Owner: Unassigned Status: New Severity: High

Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref: <https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1>

Alert product names
• Microsoft Sentinel

Evidence
1 Events 1 Alerts 0 Bookmarks

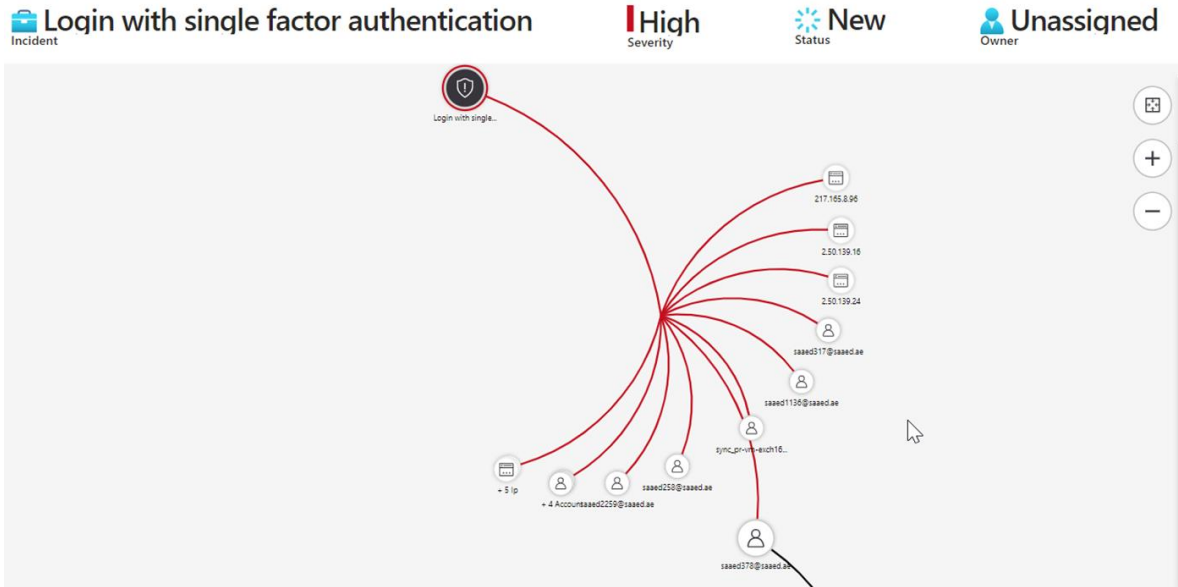
Last update time: 05/11/22, 12:50 PM Creation time: 05/11/22, 12:49 PM

Entities (2)
gbarnes@contoso...
192.168.65.82
[View full details >](#)

Tactics and techniques

[View full details](#) Actions

Incident investigations



This is the new, improved incident page (currently in preview). You can use the toggle to switch back.

High Severity | New Status | Unassigned Owner

Workspace name: saaed-defender

Description: --

Alert product names: Microsoft Sentinel

Evidence: 2.1K Events | 1 Alerts | 0 Bookmarks

Last update time: 5/21/2023, 12:26:32 PM | Creation time: 5/21/2023, 12:26:32 PM

Entities (18): 217.165.8.96 IP, 2.50.139.16 IP, 2.50.139.24 IP, saaed317@saaed.ae

Investigate

Overview | Entities

Incident timeline

Search

Add filter

May 21 06:21:27 | Login with single factor ... | Hi... Detected by Mi... Ta...

Entities

Search | Type: All

217.165.8.96 IP

2.50.139.16 IP

2.50.139.24 IP

Similar incidents (Preview)

Severity	Incident ID	Title	Last update time	Status
Medium	330	Successful logon from IP and fail...	5/17/2023, 01:54 PM	New
Medium	300	SharePointFileOperation via previ...	5/15/2023, 01:57 PM	New

Top insight: Last 24 h | IP a 5/20 | Di | Tc | AI | See | IP a 5/20

Automation

To send email whenever incident is created

The screenshot shows the Microsoft Sentinel Automation interface. The left sidebar contains a navigation menu with the following items: Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), Content management (Content hub (Preview), Repositories (Preview), Community), Configuration (Workspace manager (Preview), Data connectors, Analytics, Watchlist, Automation), and Settings. The 'Automation' item is highlighted with a red box. The main content area displays a list of automation rules with a search bar and action buttons (Create, Refresh, Automation health workbook, Edit, Enable, Move up, Move down). The list includes: Automation rule, Playbook with incident trigger (highlighted with a red box), Playbook with alert trigger, Playbook with entity trigger, and Blank playbook. A 'No automation rules were found' message is displayed below the list, accompanied by a play button icon. The message includes sections for 'What is it?' (Automation rules allow you to centrally manage all the automation of incident handling...), 'How does it work?' (Automation rules are triggered by the creation of incidents...), and 'What does it do for you?' (Automate incident, Trigger playbooks for).