Threat Detection and Mitigation with Microsoft Sentinel

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Introduction to SIEM, SOAR, and XDR

Microsoft Sentinel

Introduction to SIEM, SOAR, and XDR

Set of Security Tools

SIEM — Security Incident and Event Management

SOAR — Security Orchestration Automated Response

XDR — Extended Detection and Response

Security Incident and Event Management

Collect data from your digital estate

- Infrastructure
- Software
- Applications

Analyzes data and looks for correlations or anomalies

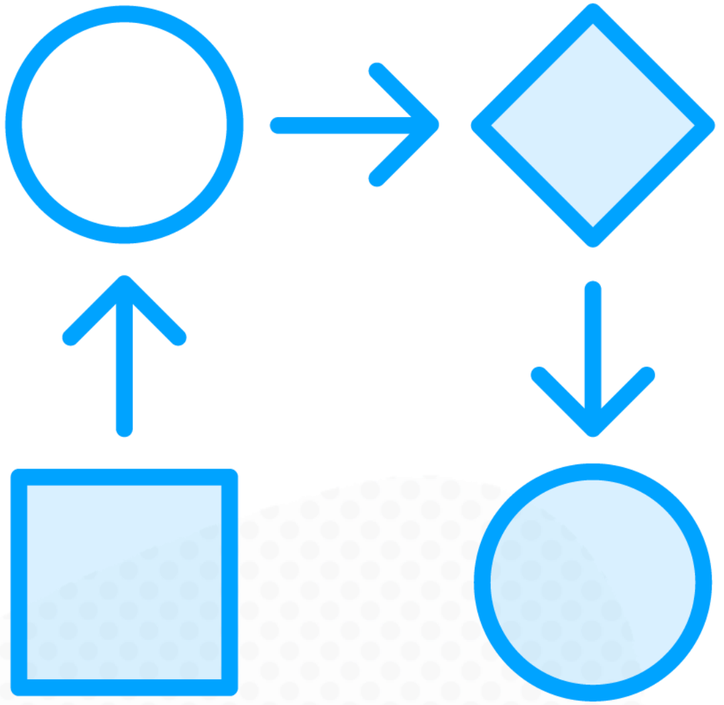
- Generates alerts and incidents

Security Orchestration Automated Response

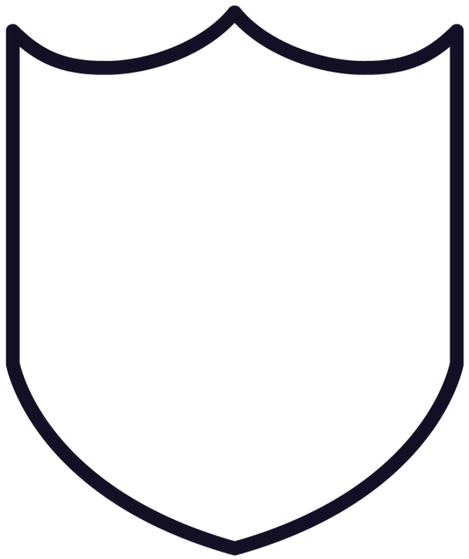
Collects data from many sources

Similar to a SIEM system

Able to trigger automated workflows to mitigate the issue



Extended Detection and Response



Security threat detection and incident response tool

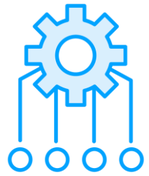
- Identities
- Endpoints
- Applications
- E-mail
- Infrastructure

Microsoft Products

Microsoft Sentinel	Microsoft Sentinel	Microsoft Defender XDR *(formerly Microsoft 365 Defender)*
SIEM	SOAR	XDR

Microsoft Sentinel

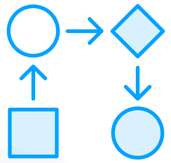
Microsoft Sentinel Functionality



Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence

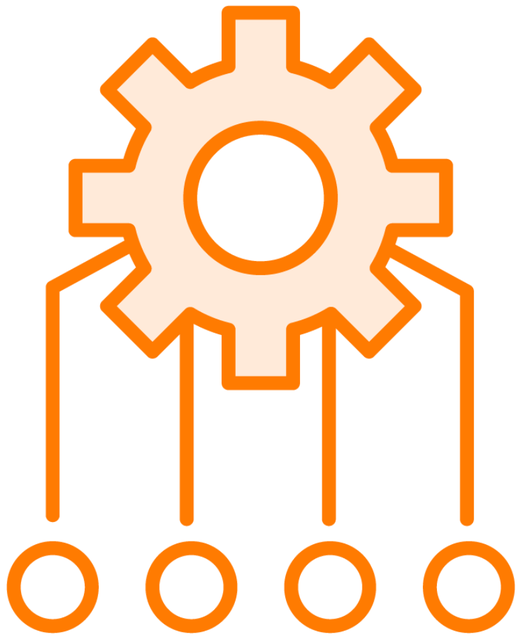
Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft



Respond to incidents rapidly with built-in orchestration and automation of common security tasks

https://learn.microsoft.com/en-us/azure/sentinel/overview

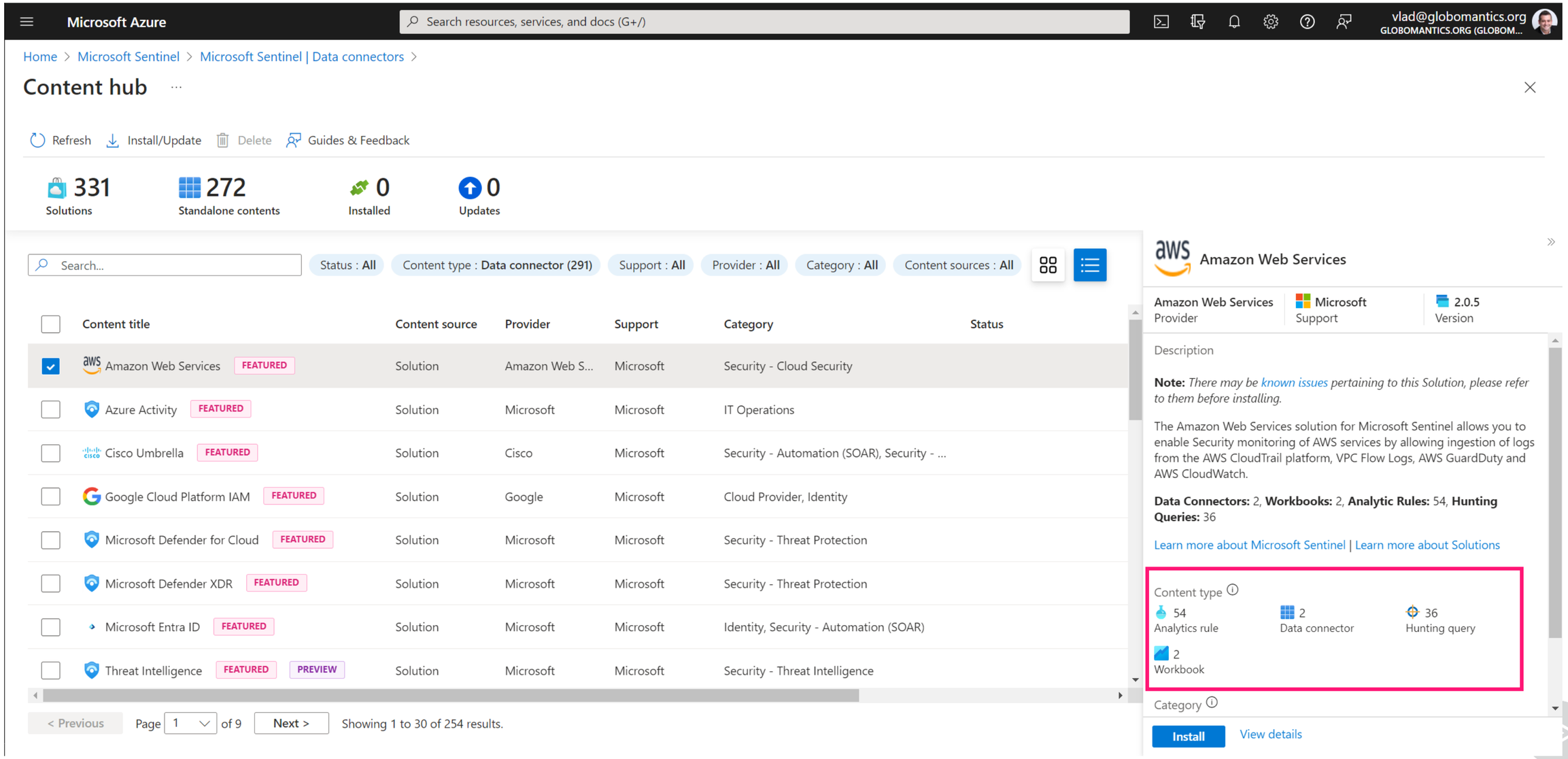
Connect to All Your Data



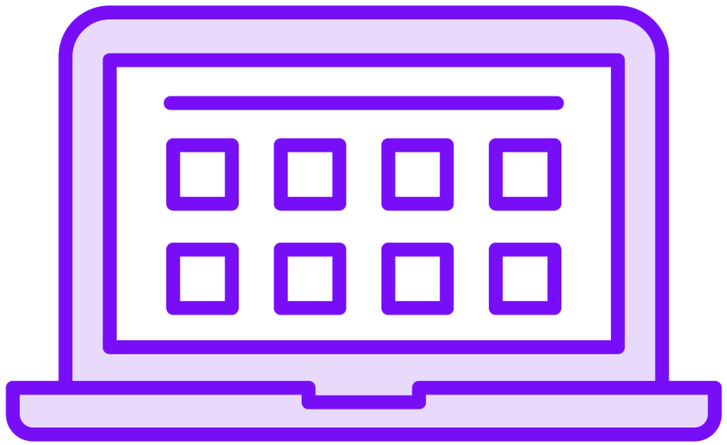
Great number of built-in data connectors

- Microsoft services
  - Entra ID
  - Microsoft Defender XDR
  - Office 365
- External solutions
  - F5 BIG-IP
  - Okta SSO
  - Google Workspace

Over 250 Data Connectors Built-in



Workbooks



Sentinel integrates with Azure Monitor Workbooks

- Flexible canvas for data analysis and rich visual reports in the Azure portal

Built-in workbooks with most data connectors

- You can also create your own!

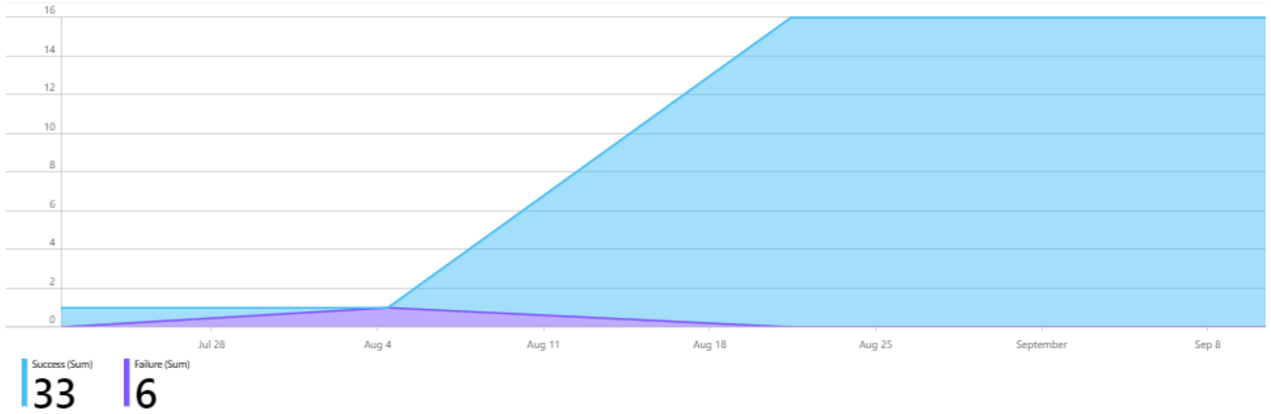
Workbook Example: AWS User Activities

AWS user activities

TimeRange: Last 60 days

Signin and login events

Sign-in events



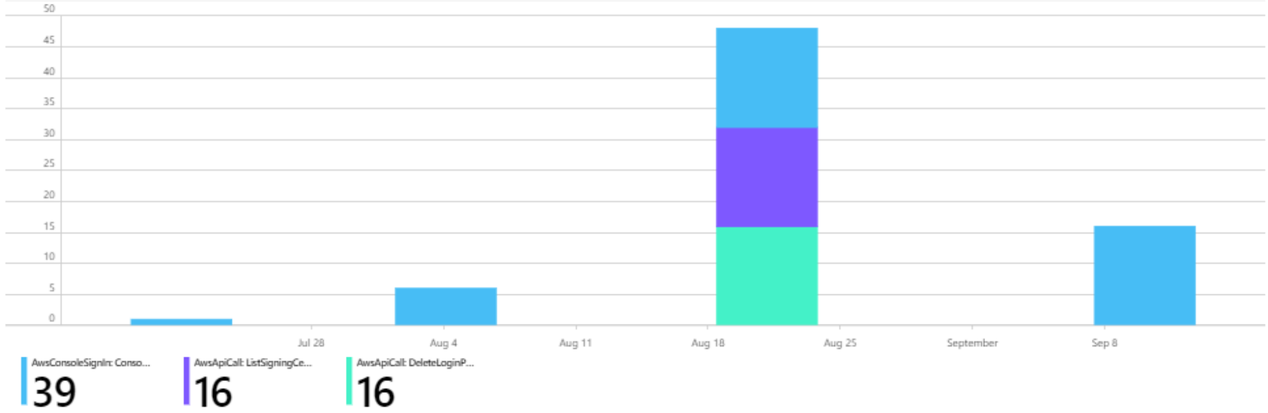
Sign-in events results

Name	Type	LoginResults Count	Trend
Success	LoginResult	33	
Failure	LoginResult	6	

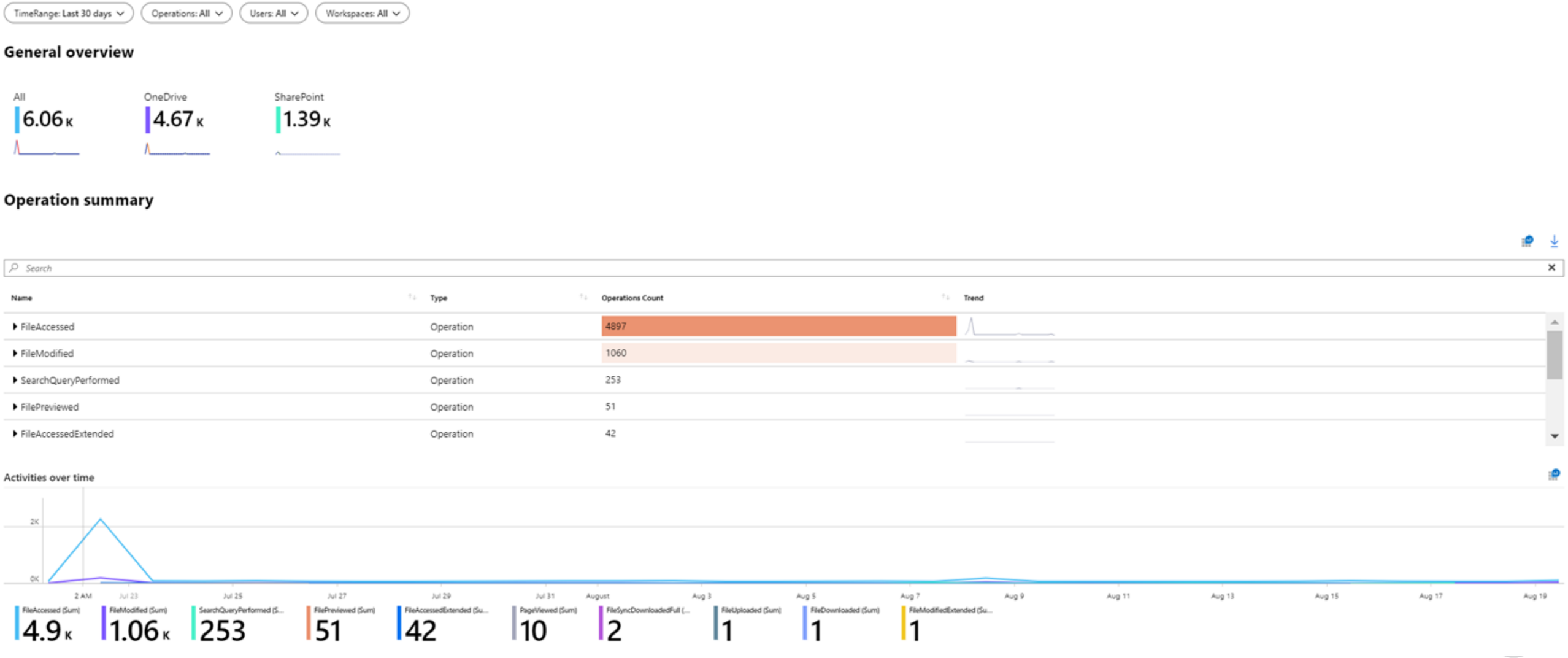
User sign-ins, by failure rate, and IP addresses

UserIdentityUserName	UserIdentityAccountId	SourceIpAddress	EventName	Success	Failure
moshabi	1	1	1	0	6
None	1	2	1	32	0
mahhasan	1	1	1	1	0

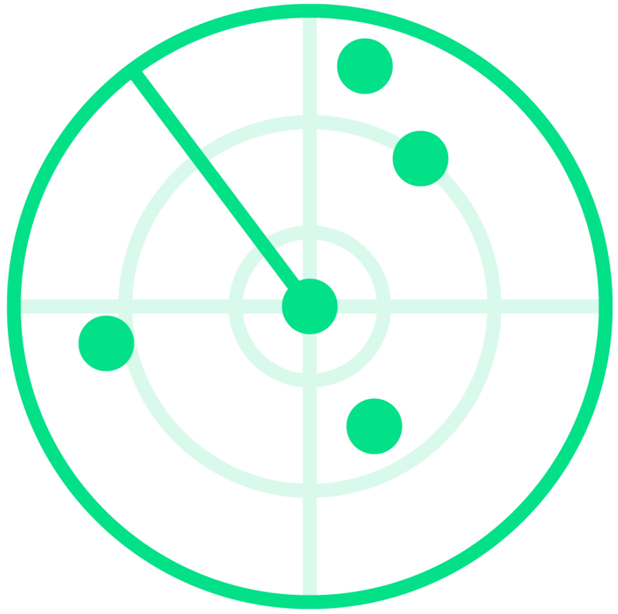
Console and API signin events over time



Workbook Example: SharePoint and OneDrive



Analytics and Incidents



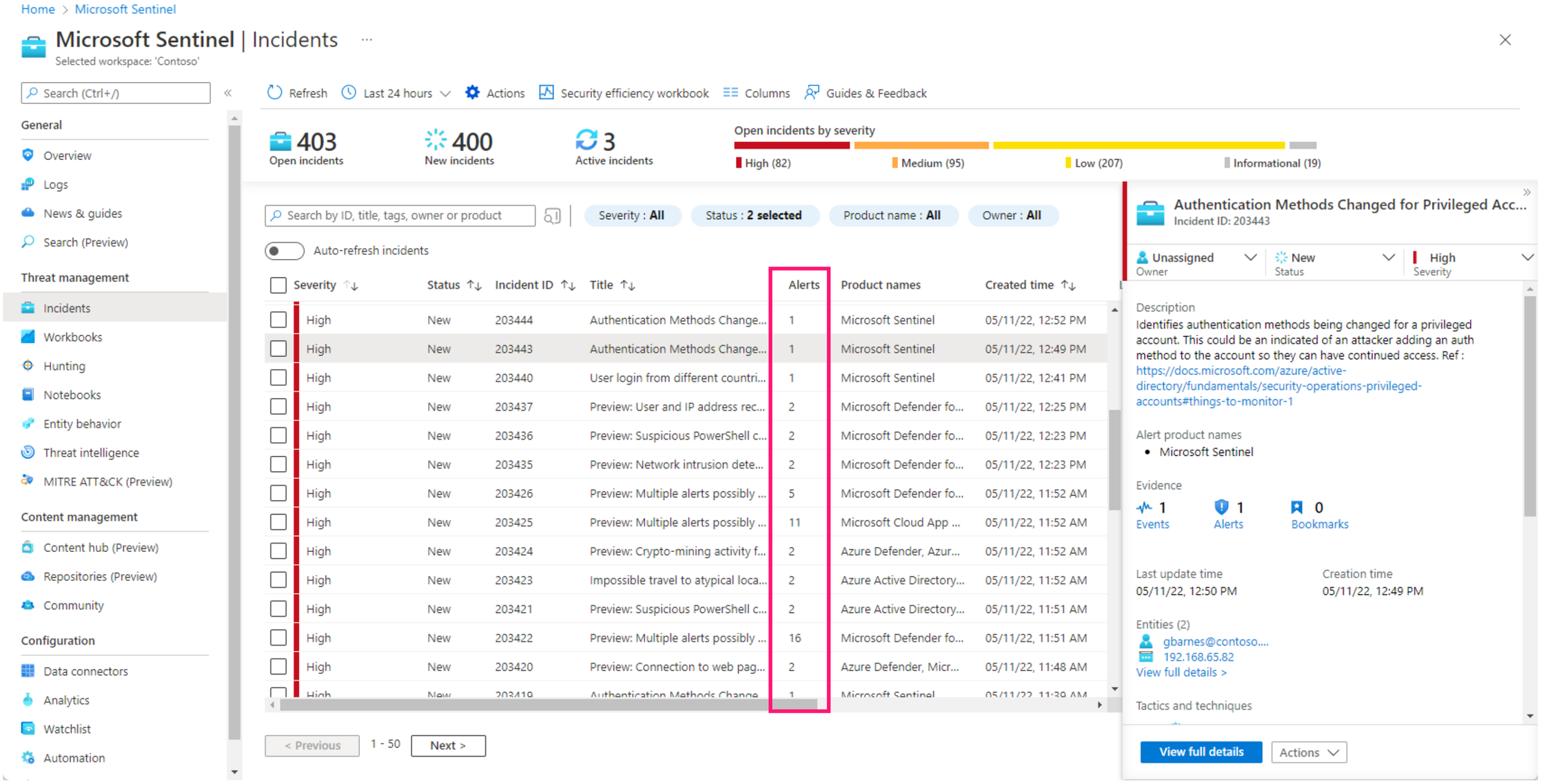
Built-in analytics templates for most connectors

- Get notified when anything suspicious occurs

Sentinel can correlate alerts into incidents

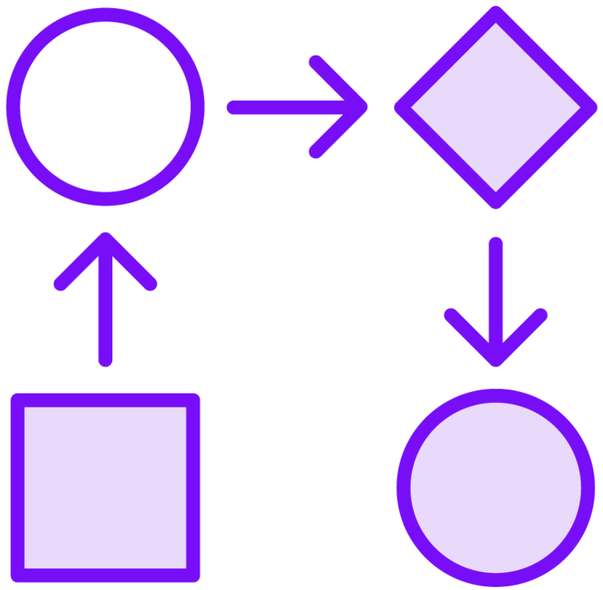
- Built-in correlation rules/create your own

Microsoft Sentinel Incidents



Source: https://learn.microsoft.com/en-us/azure/sentinel/overview

Security Automation and Orchestration



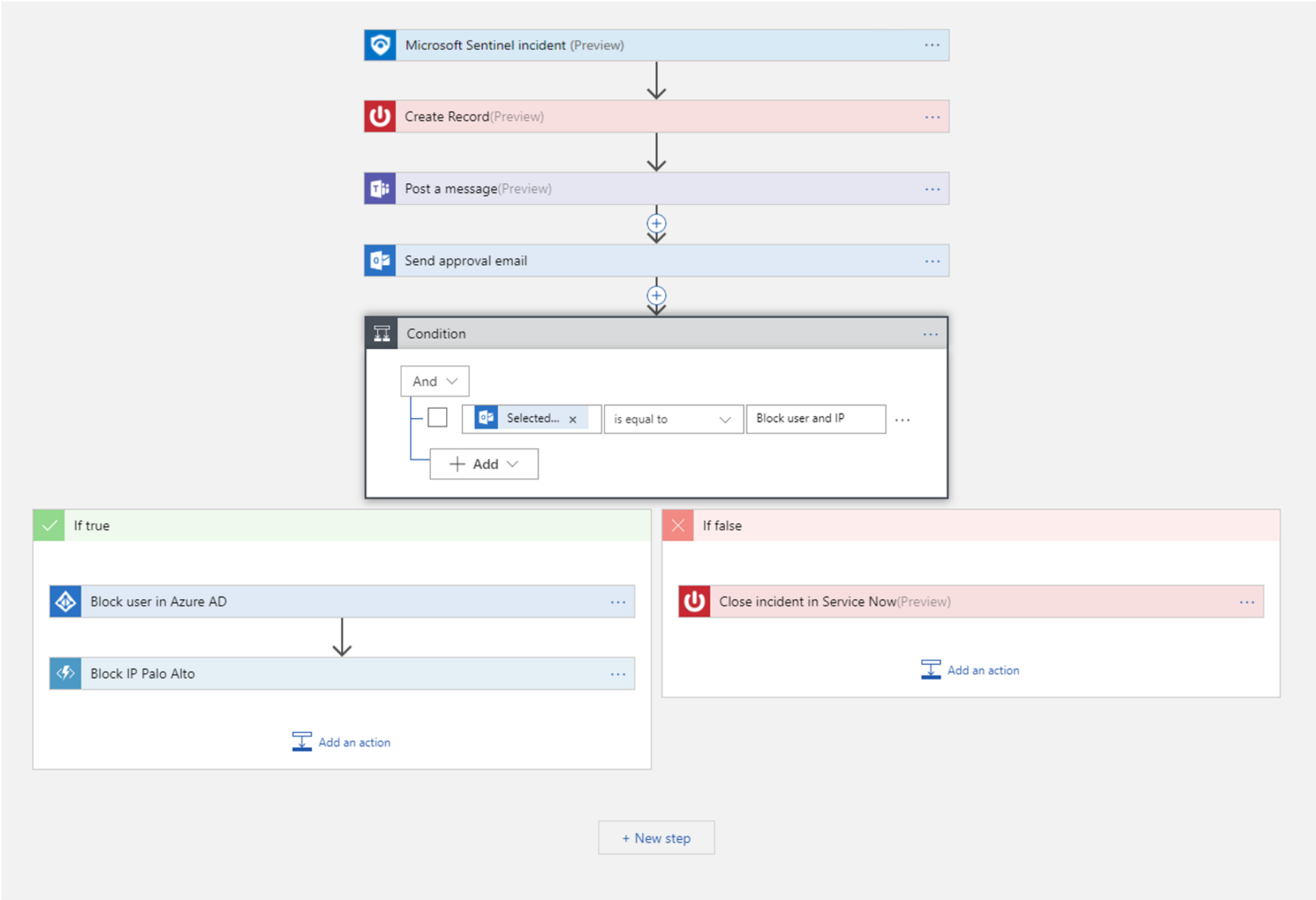
Automation rules can help you be more productive in Microsoft Sentinel

- Tag incidents
- Assign them to the right personnel
- Change severity
- Run playbooks

Playbooks are collections of procedures that can be run

- Based on workflows built with Azure Logic Apps
- Over 500 connectors built in for your own custom logic

Microsoft Sentinel Playbook Example



Source: https://learn.microsoft.com/en-us/azure/sentinel/overview

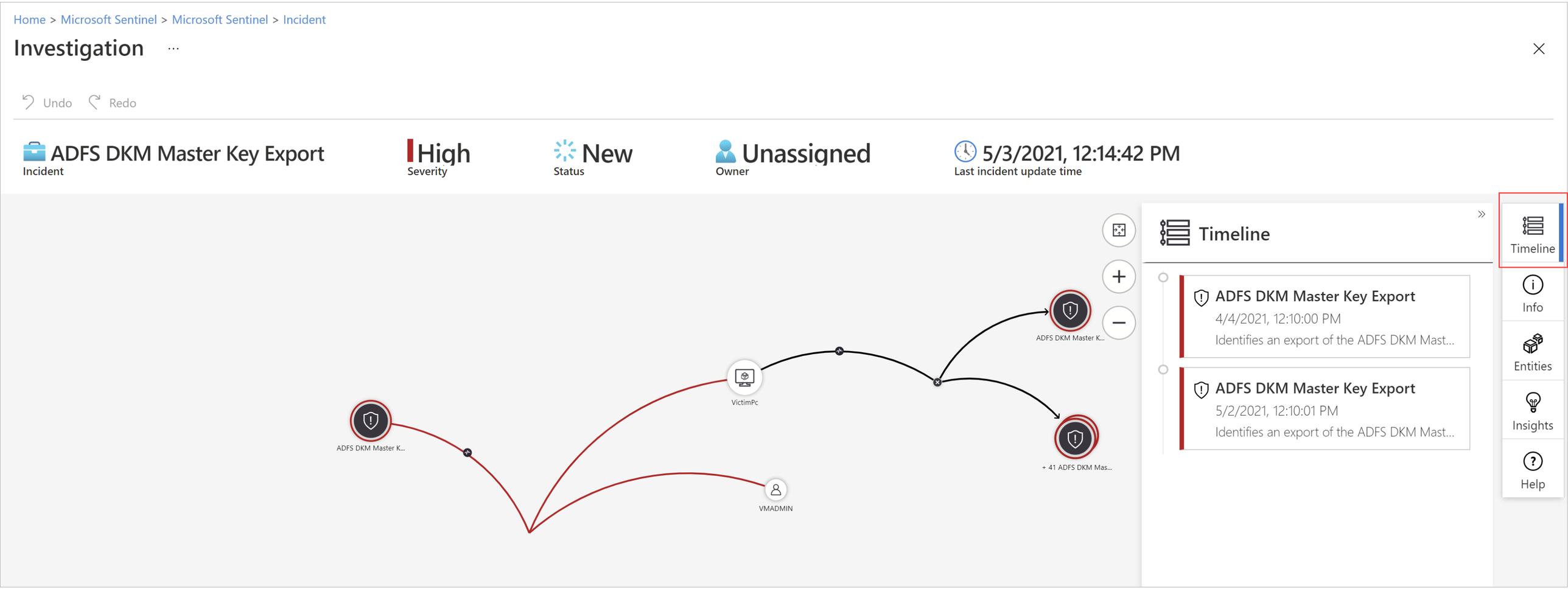
Investigation

Understand the scope and find the root cause of a security threat

Multiple ways to view information

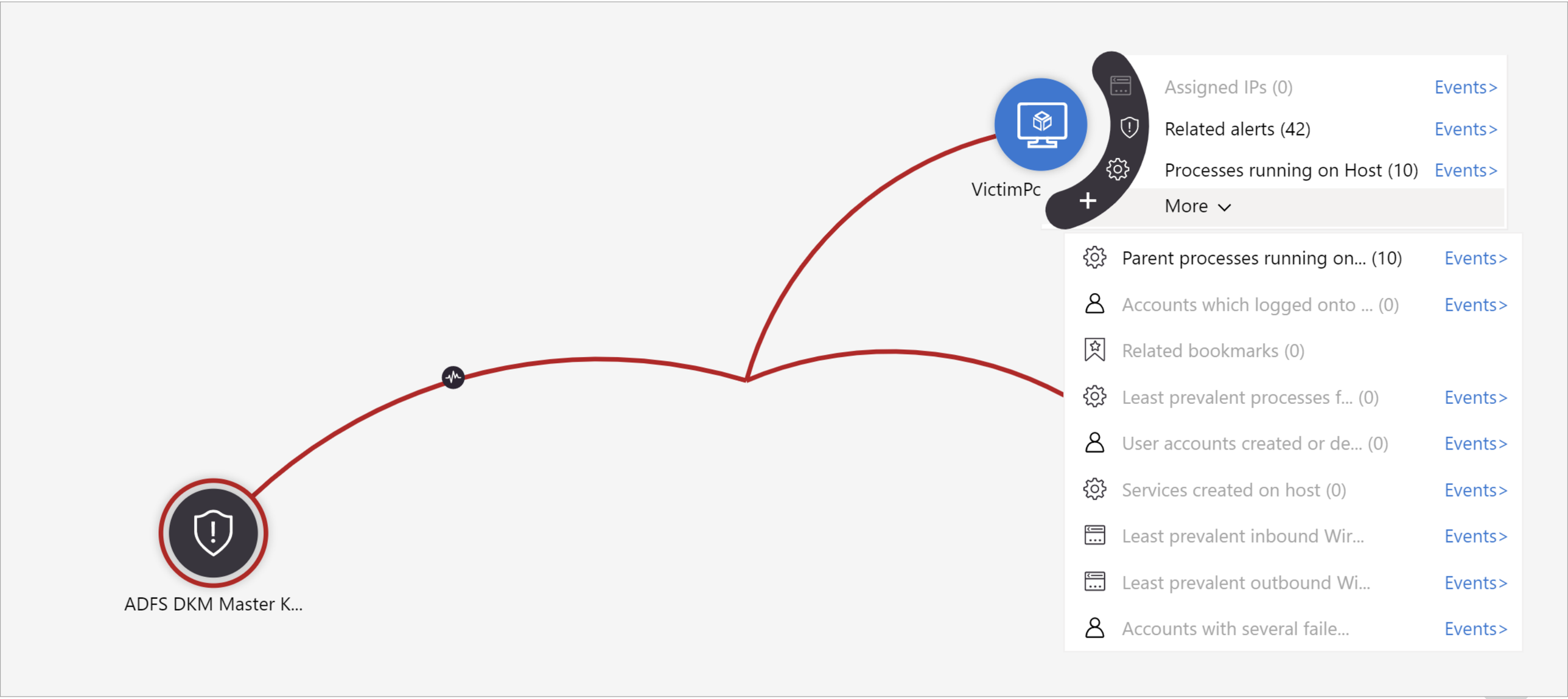
- Timeline
- Related alerts
- Exploration queries

Microsoft Sentinel Investigation View: Timeline



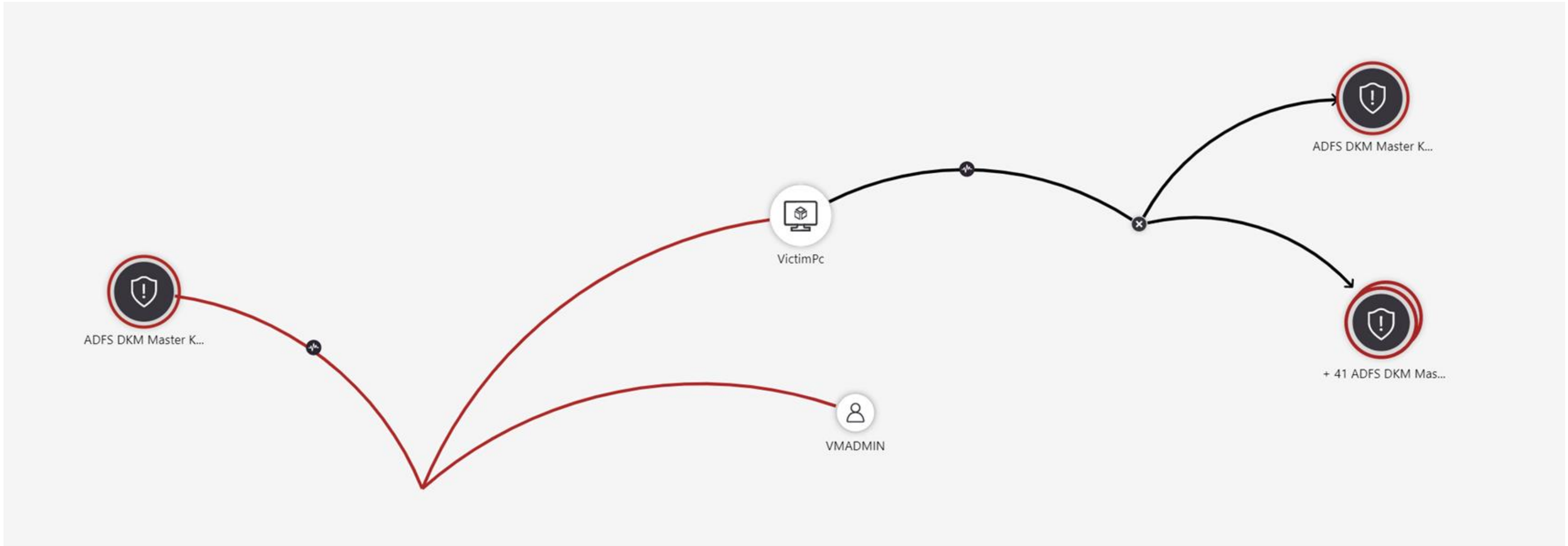
Source: https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases

Microsoft Sentinel Investigation View: Exploration Queries



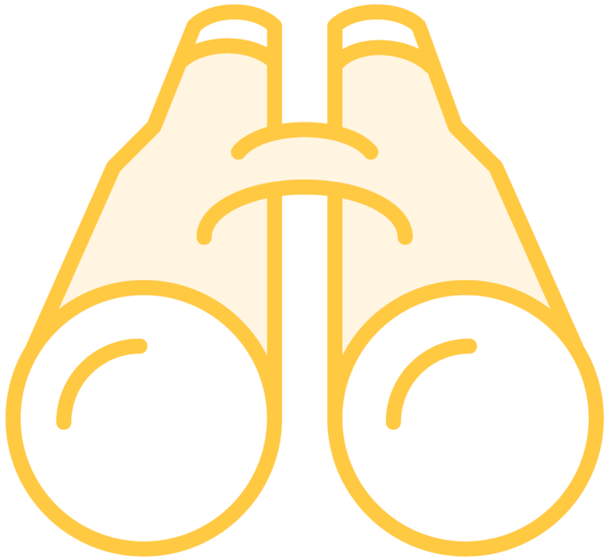
Source: https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases

Microsoft Sentinel Investigation View: Related Alerts



Source: https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases

Hunting



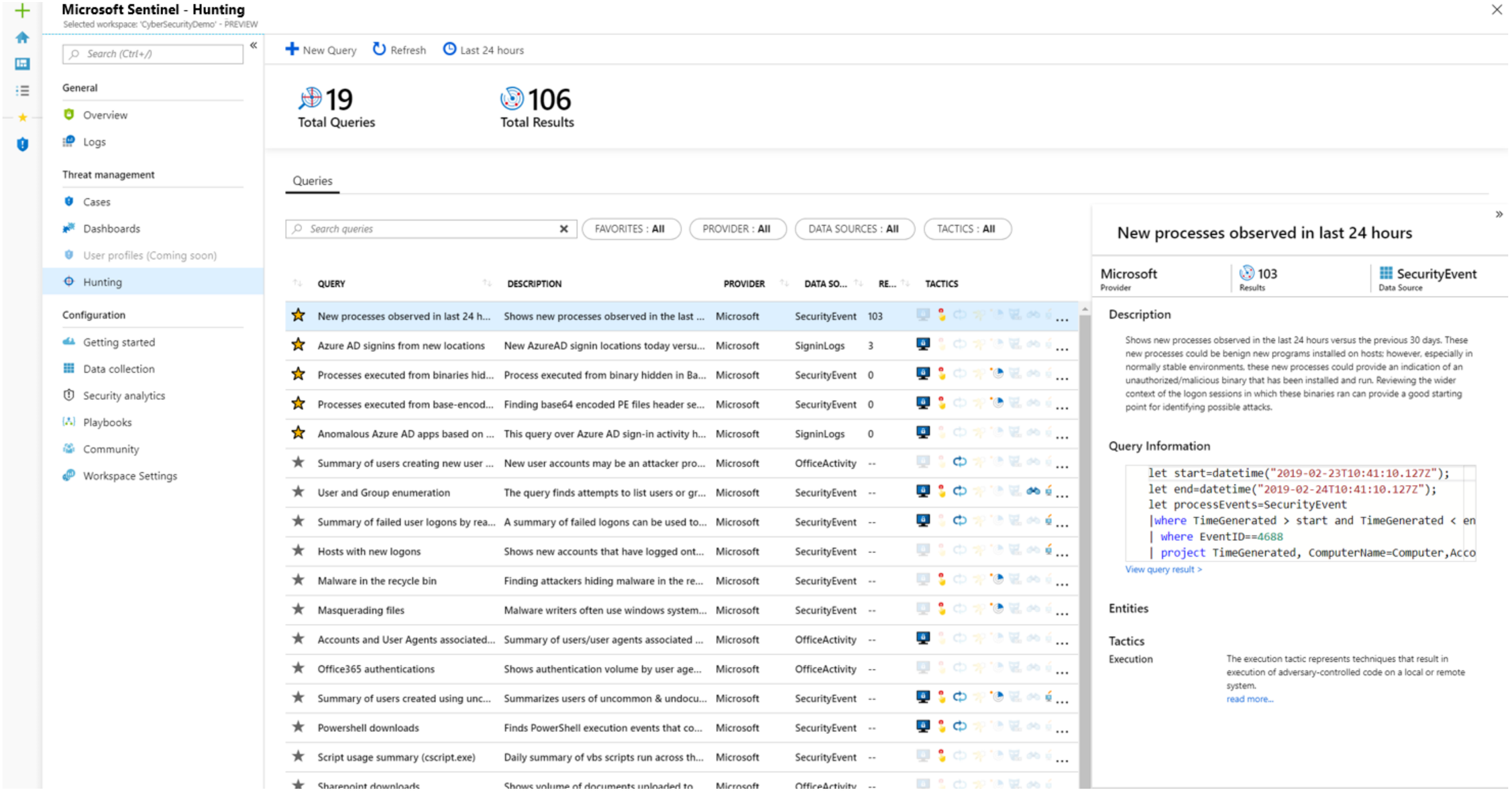
Search-and-query tools to proactively hunt security threats

- That weren't detected in your security apps/ scheduled analytics

Create custom detection rules based on your queries

- Surface them as alerts in the future

Microsoft Sentinel Hunting Dashboard



Source: https://learn.microsoft.com/en-us/azure/sentinel/overview

Module Conclusion

Introduction to SIEM, SOAR, and XDR

- Security Incident and Event Management
- Security Orchestration Automated Response
- Extended Detection and Response

Microsoft Sentinel

- Connect to all your data
- Workbooks
- Analytics and incidents
- Security automation and orchestration
  - Playbooks
- Investigation
- Hunting

Up Next:

Introduction to Microsoft Defender XDR