

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

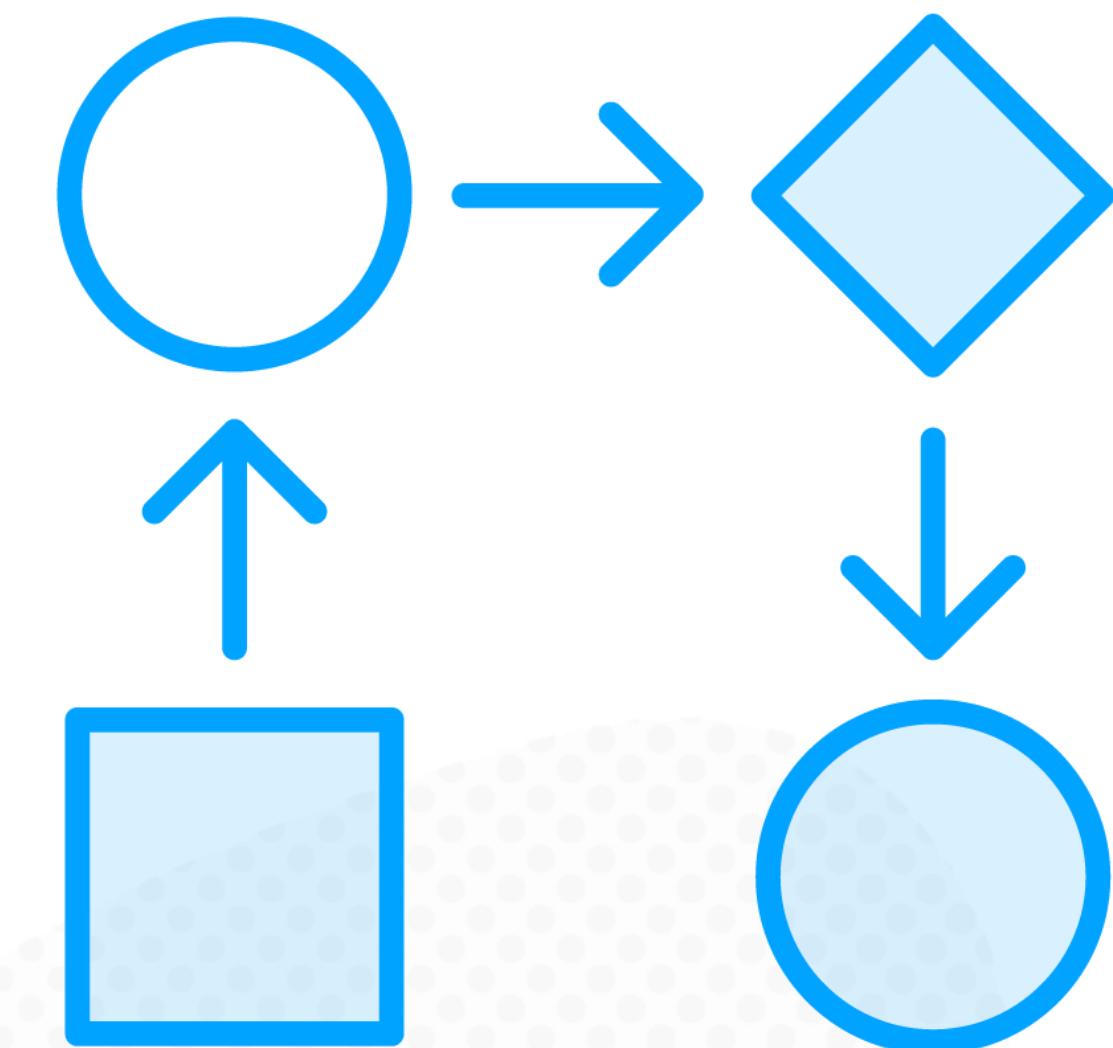


Security Orchestration Automated Response

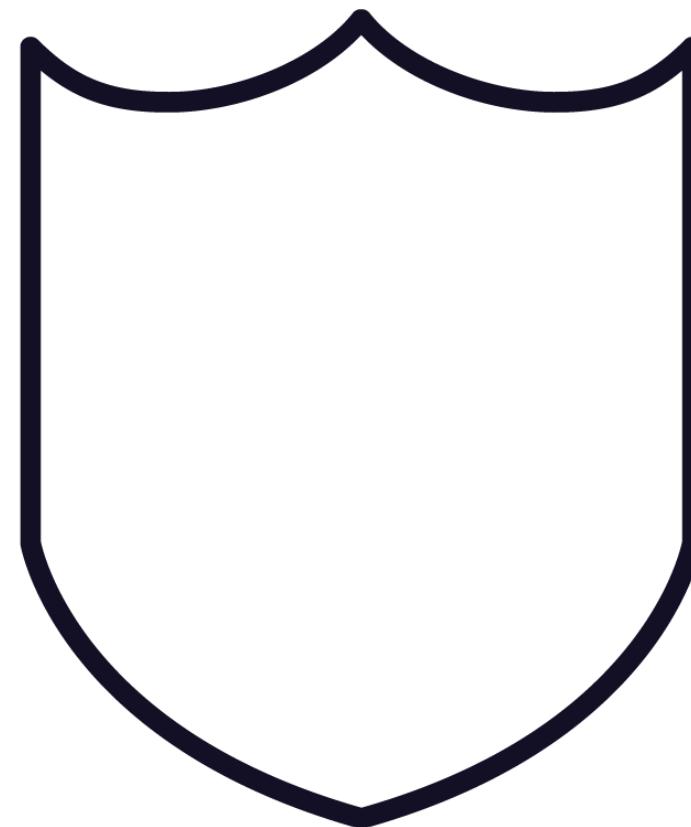
Collects data from many sources

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

SIEM

Microsoft Sentinel

SOAR

Microsoft Defender XDR
(formerly Microsoft 365 Defender)

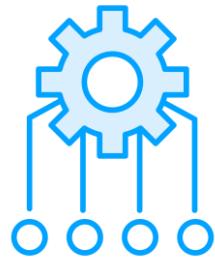
XDR



Microsoft Sentinel



Microsoft Sentinel Functionality



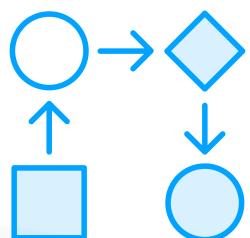
Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds



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



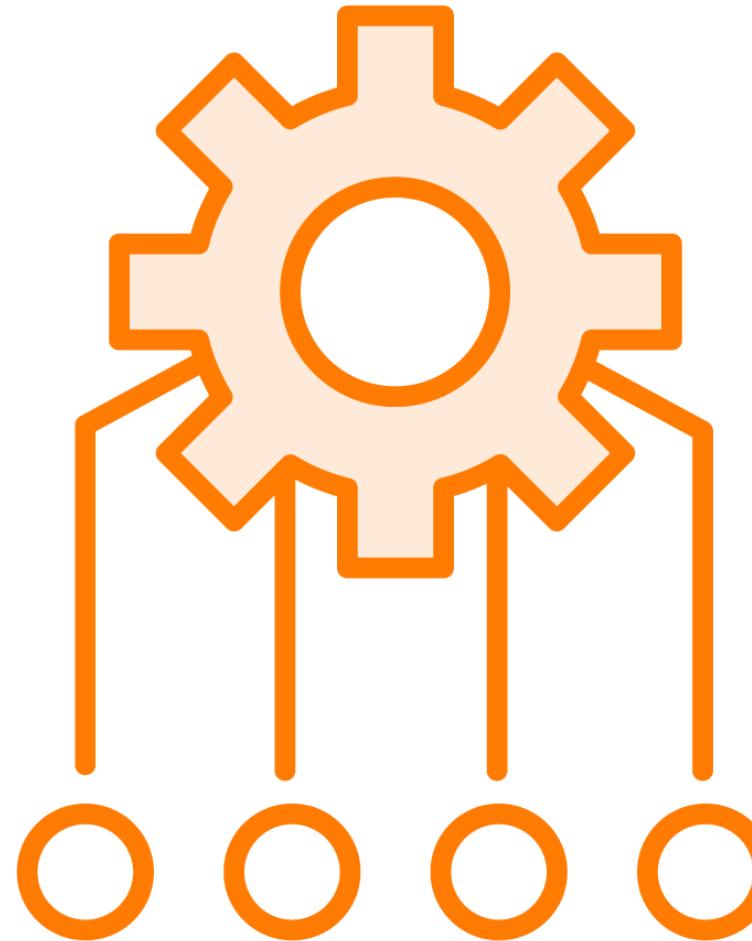
Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft



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



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

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >

Content hub

Refresh Install/Update Delete Guides & Feedback

Solutions 331 **Standalone contents** 272 **Installed** 0 **Updates** 0

<input type="checkbox"/> Content title	Content source	Provider	Support	Category	Status
<input checked="" type="checkbox"/> Amazon Web Services FEATURED	Solution	Amazon Web S...	Microsoft	Security - Cloud Security	
<input type="checkbox"/> Azure Activity FEATURED	Solution	Microsoft	Microsoft	IT Operations	
<input type="checkbox"/> Cisco Umbrella FEATURED	Solution	Cisco	Microsoft	Security - Automation (SOAR), Security - ...	
<input type="checkbox"/> Google Cloud Platform IAM FEATURED	Solution	Google	Microsoft	Cloud Provider, Identity	
<input type="checkbox"/> Microsoft Defender for Cloud FEATURED	Solution	Microsoft	Microsoft	Security - Threat Protection	
<input type="checkbox"/> Microsoft Defender XDR FEATURED	Solution	Microsoft	Microsoft	Security - Threat Protection	
<input type="checkbox"/> Microsoft Entra ID FEATURED	Solution	Microsoft	Microsoft	Identity, Security - Automation (SOAR)	
<input type="checkbox"/> Threat Intelligence FEATURED PREVIEW	Solution	Microsoft	Microsoft	Security - Threat Intelligence	

Search... Status : All Content type : Data connector (291) Support : All Provider : All Category : All Content sources : All

Amazon Web Services aws Amazon Web Services

Amazon Web Services Provider Microsoft Support Version 2.0.5

Description

Note: There may be [known issues](#) pertaining to this Solution, please refer to them before installing.

The Amazon Web Services solution for Microsoft Sentinel allows you to enable Security monitoring of AWS services by allowing ingestion of logs from the AWS CloudTrail platform, VPC Flow Logs, AWS GuardDuty and AWS CloudWatch.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 54, **Hunting Queries:** 36

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

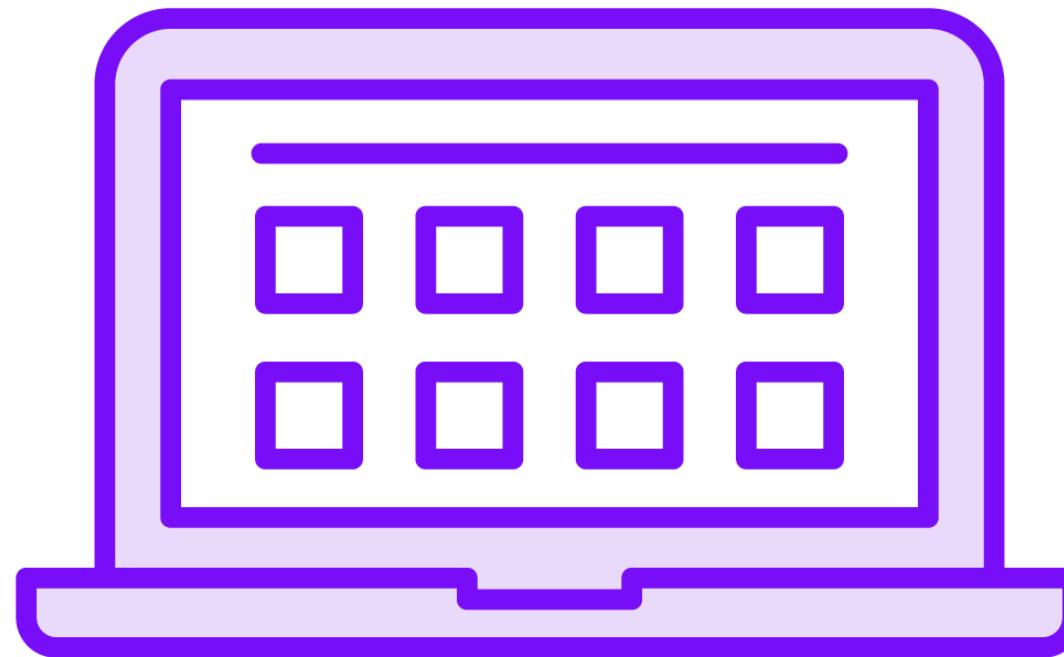
Content type ①

- Analytics rule 54
- Data connector 2
- Hunting query 36
- Workbook 2

Category ①

Install View details

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!

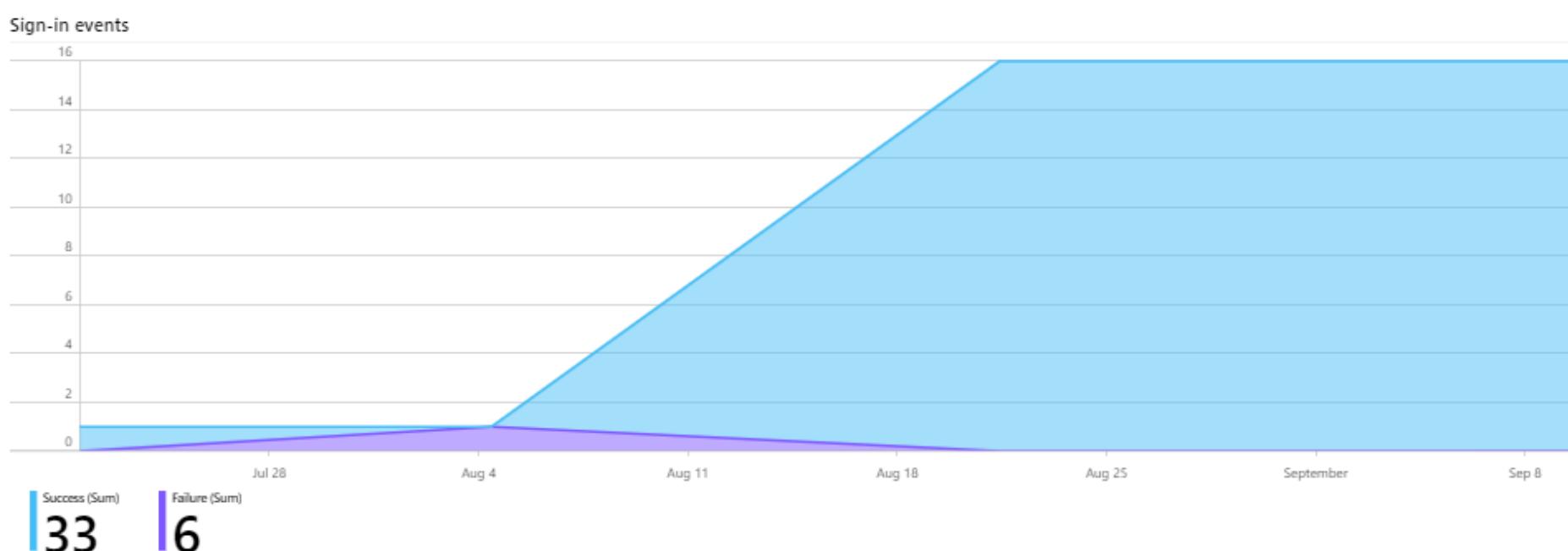


Workbook Example: AWS User Activities

AWS user activities

TimeRange: Last 60 days ▾

Signin and login events



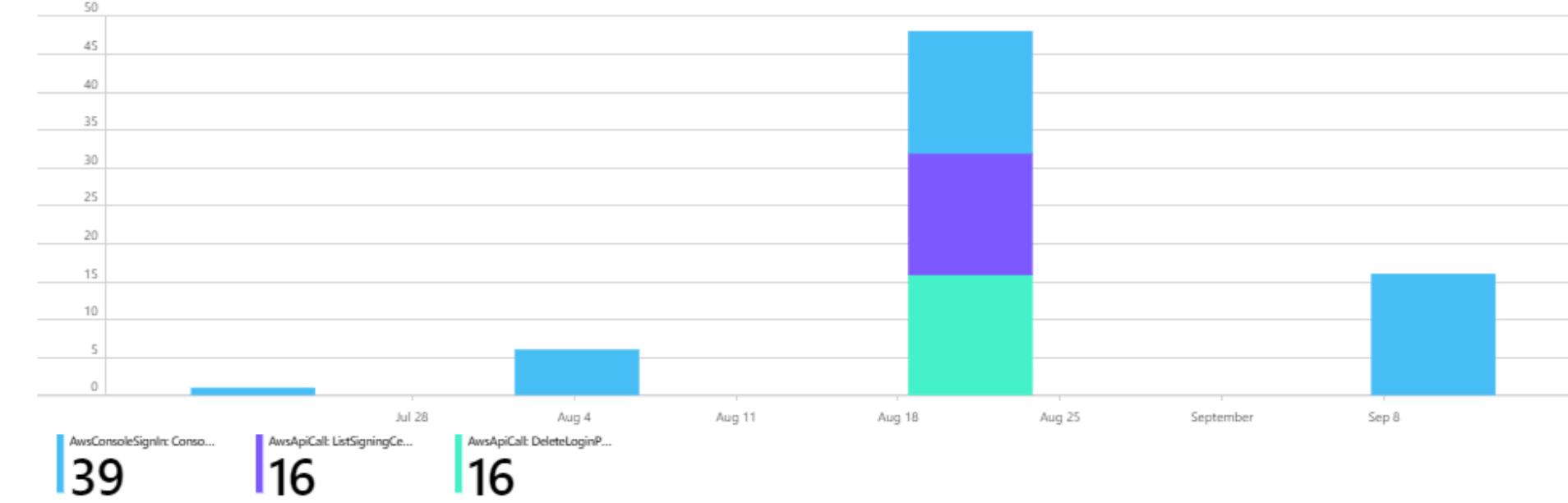
Sign-in events results

Name	Type	LoginResults Count	Trend
► ✓ Success	LoginResult	33	
► ✗ Failure	LoginResult	6	

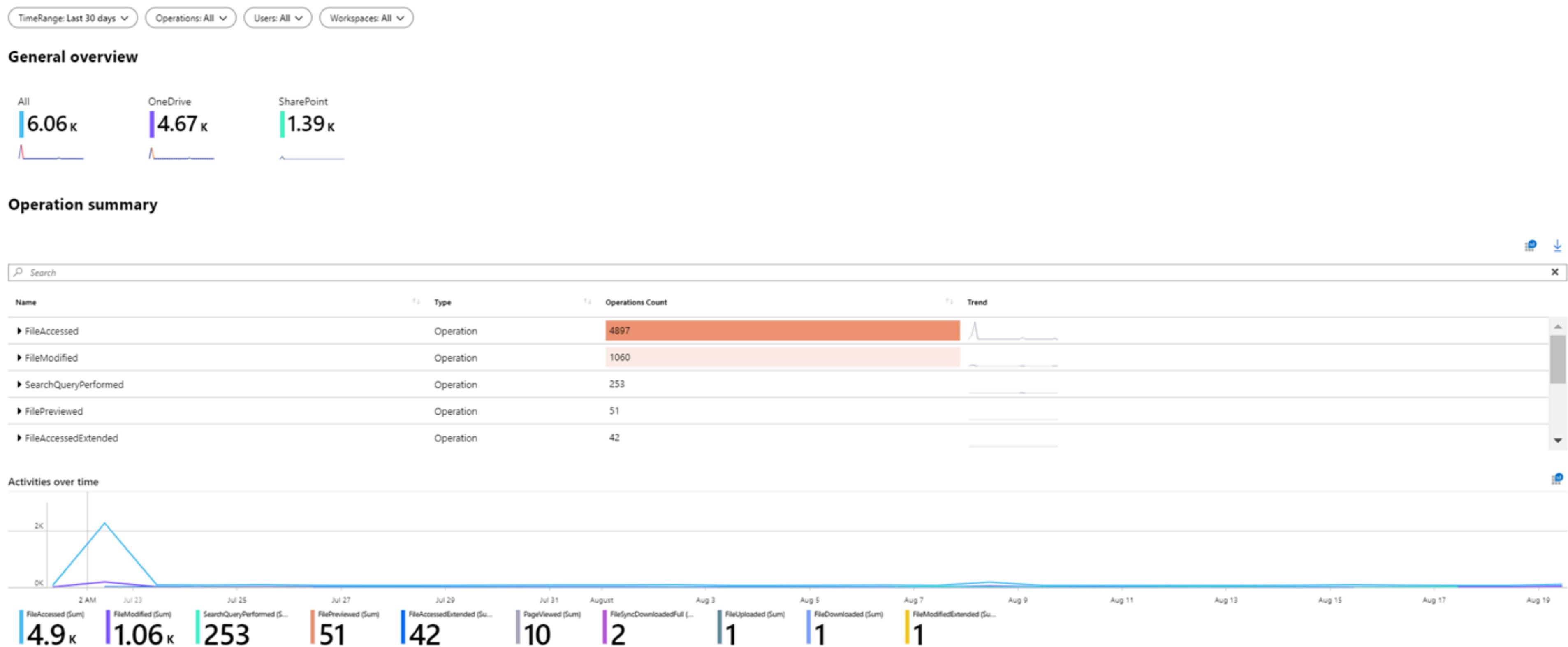
User sign-ins, by failure rate, and IP addresses

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

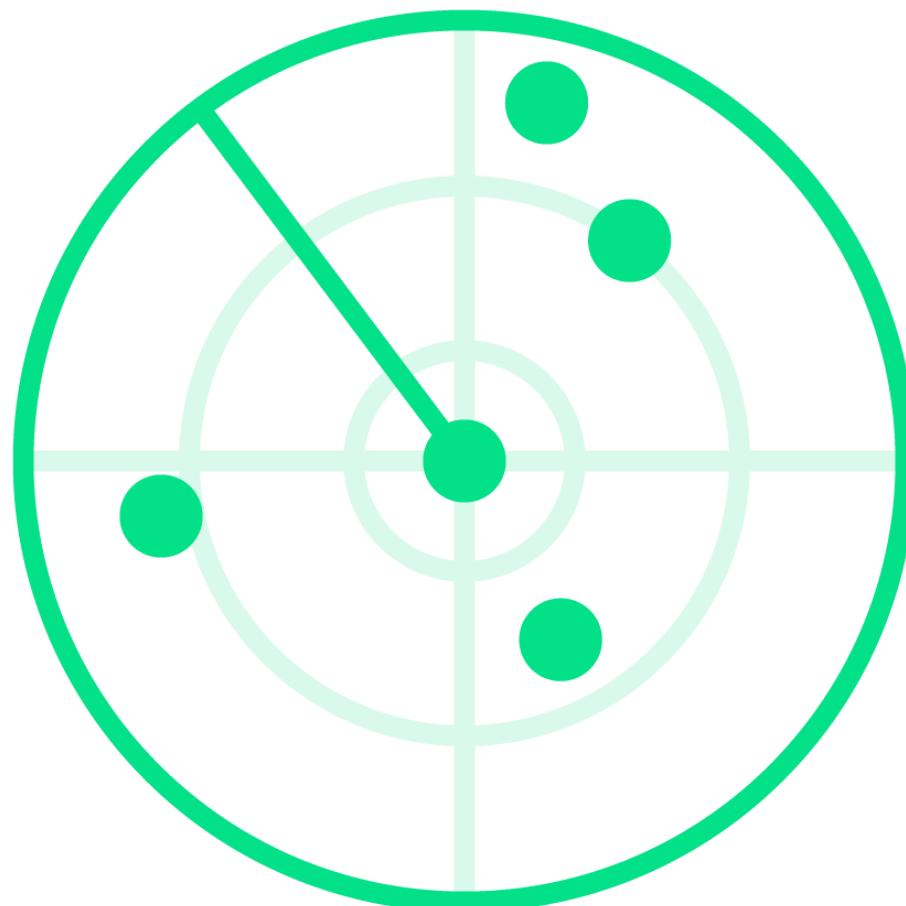
Console and API signin events over time



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

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents ... X

Selected workspace: 'Contoso'

Search (Ctrl+/Search by ID, title, tags, owner or product) Refresh Last 24 hours Actions Security efficiency workbook Columns Guides & Feedback

403 Open incidents 400 New incidents 3 Active incidents Open incidents by severity

High (82) Medium (95) Low (207) Informational (19)

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 possibl...	5	Microsoft Defender fo...	05/11/22, 11:52 AM
High	New	203425	Preview: Multiple alerts possibl...	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 loc...	2	Azure Active Directo...	05/11/22, 11:52 AM
High	New	203421	Preview: Suspicious PowerShell c...	2	Azure Active Directo...	05/11/22, 11:51 AM
High	New	203422	Preview: Multiple alerts possibl...	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

< Previous 1 - 50 Next >

Alerts

Authentication Methods Changed for Privileged Acc...
Incident ID: 203443

Owner: Unassigned | Status: New | Severity: High

Description: Identifies authentication methods being changed for a privileged account. This could be an indicator 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:

Events: 1 | Alerts: 1 | Bookmarks: 0

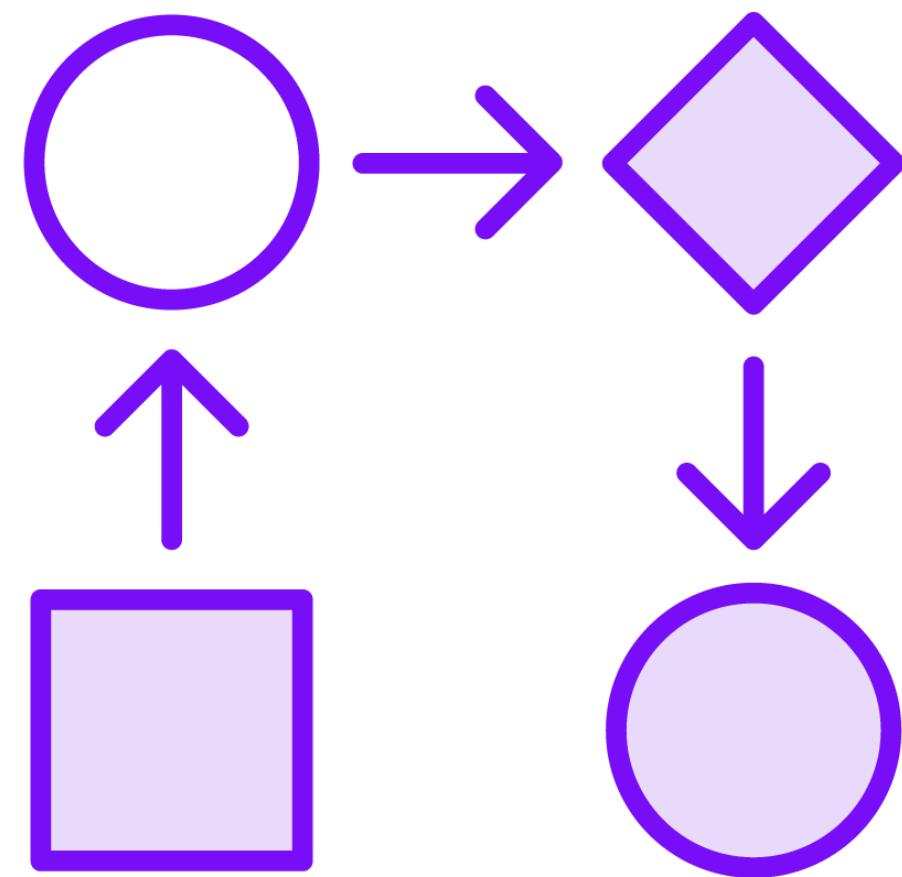
Last update time: 05/11/22, 12:50 PM | Creation time: 05/11/22, 12:49 PM

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

Tactics and techniques:

[View full details](#) [Actions](#)

Security Automation and Orchestration



Automation rules can help you be more productive in Microsoft Sentinel

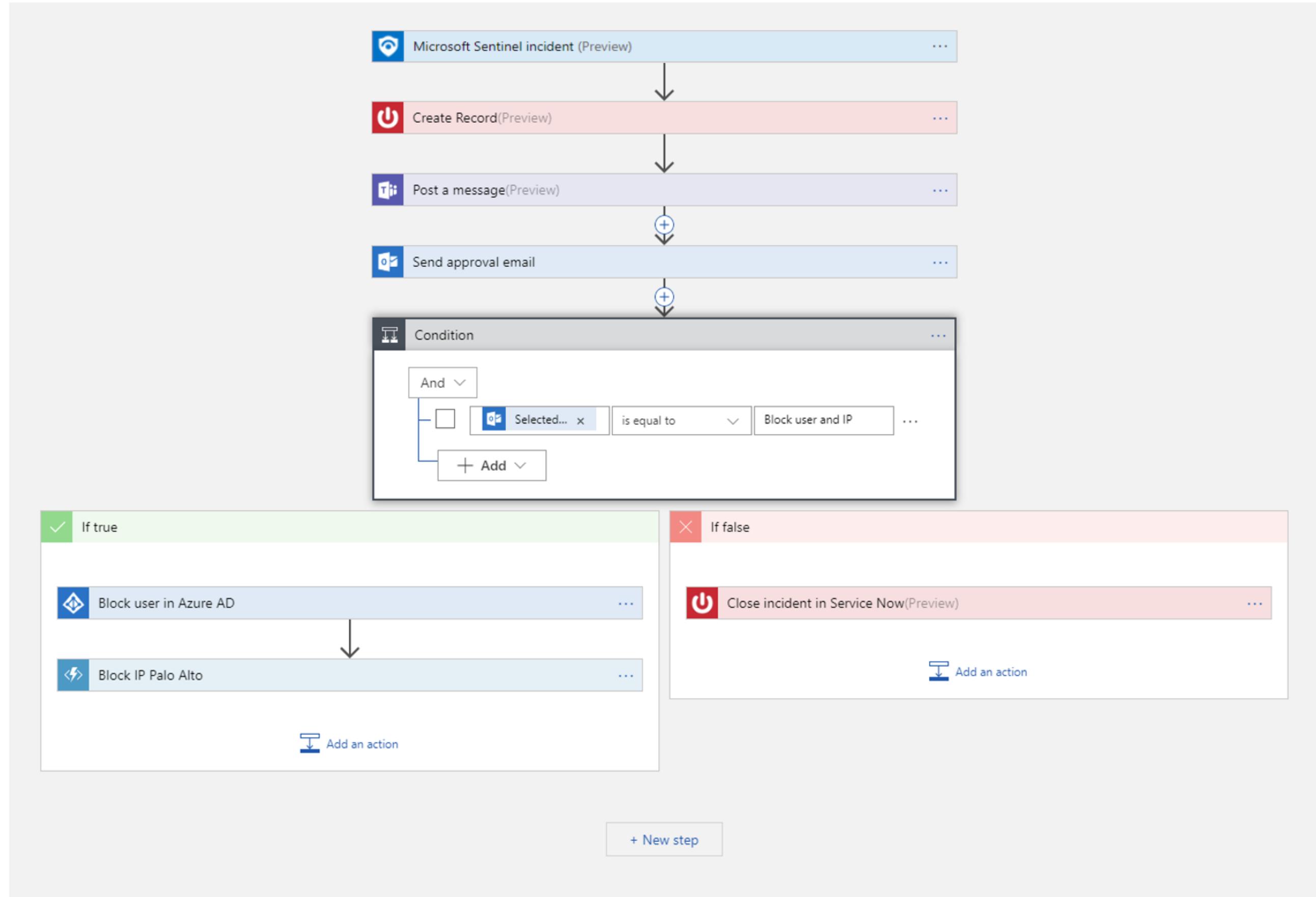
- Tag incidents
- Assign them to the right personnel
- Change severity
- Run playbooks

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



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

Home > Microsoft Sentinel > Microsoft Sentinel > Incident

Investigation

...

Undo Redo

ADFS DKM Master Key Export Incident

High Severity

New Status

Unassigned Owner

5/3/2021, 12:14:42 PM Last incident update time

The diagram illustrates a sequence of security events. It begins with an event from 'ADFS DKM Master K...' at 4/4/2021, 12:10:00 PM. This is followed by two more events from the same source at 5/2/2021, 12:10:01 PM. These events are labeled '+ 41 ADFS DKM Mas...'. A connection line links the first event to a node labeled 'VictimPC'. Another connection line links the second event to a node labeled 'VMADMIN'.

Timeline

»

- ADFS DKM Master Key Export**
4/4/2021, 12:10:00 PM
Identifies an export of the ADFS DKM Mast...
- ADFS DKM Master Key Export**
5/2/2021, 12:10:01 PM
Identifies an export of the ADFS DKM Mast...

Timeline

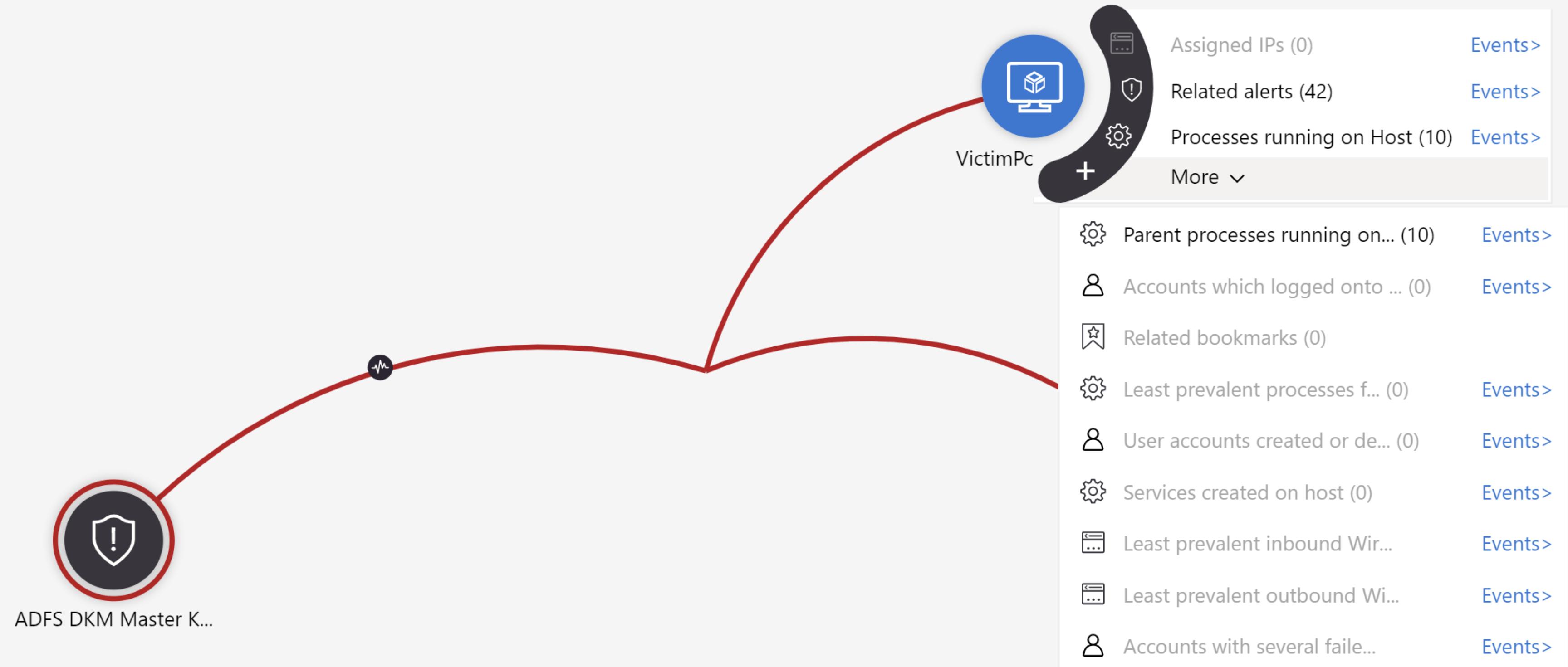
Info

Entities

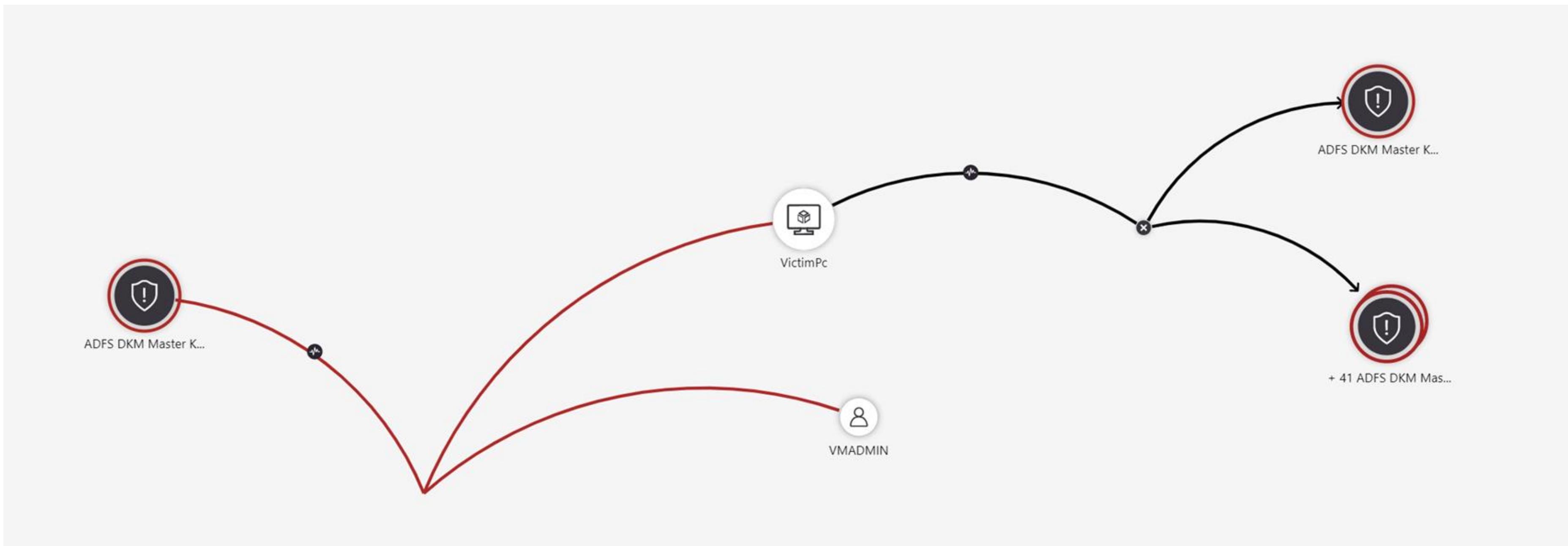
Insights

Help

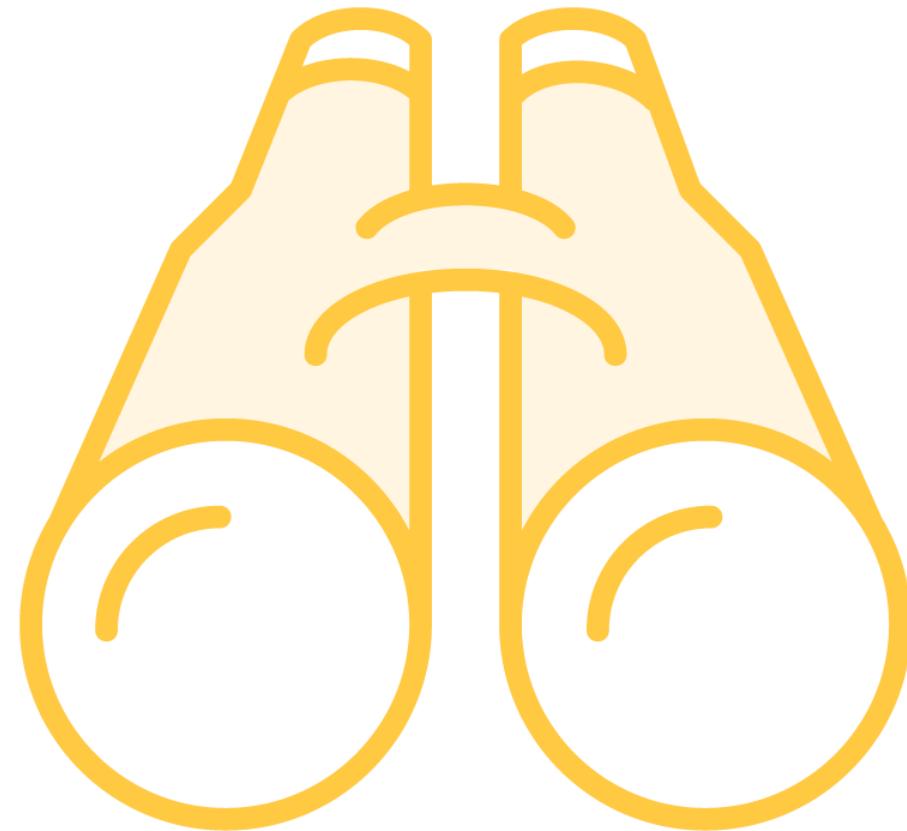
Microsoft Sentinel Investigation View: Exploration Queries



Microsoft Sentinel Investigation View: Related Alerts



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

Microsoft Sentinel - Hunting
Selected workspace: 'CyberSecurityDemo' - PREVIEW

General

- Overview
- Logs

Threat management

- Cases
- Dashboards
- User profiles (Coming soon)
- Hunting**

Configuration

- Getting started
- Data collection
- Security analytics
- Playbooks
- Community
- Workspace Settings

Queries

19 Total Queries | 106 Total Results

Search queries | FAVORITES : All | PROVIDER : All | DATA SOURCES : All | TACTICS : All

QUERY	DESCRIPTION	PROVIDER	DATA SO...	RE...	TACTICS
New processes observed in last 24 h...	Shows new processes observed in the last ...	Microsoft	SecurityEvent	103	
Azure AD signins from new locations	New AzureAD signin locations today versus...	Microsoft	SigninLogs	3	
Processes executed from binaries hid...	Process executed from binary hidden in Ba...	Microsoft	SecurityEvent	0	
Processes executed from base-encod...	Finding base64 encoded PE files header se...	Microsoft	SecurityEvent	0	
Anomalous Azure AD apps based on ...	This query over Azure AD sign-in activity h...	Microsoft	SigninLogs	0	
Summary of users creating new user ...	New user accounts may be an attacker pro...	Microsoft	OfficeActivity	--	
User and Group enumeration	The query finds attempts to list users or gr...	Microsoft	SecurityEvent	--	
Summary of failed user logons by rea...	A summary of failed logons can be used to...	Microsoft	SecurityEvent	--	
Hosts with new logons	Shows new accounts that have logged onto...	Microsoft	SecurityEvent	--	
Malware in the recycle bin	Finding attackers hiding malware in the re...	Microsoft	SecurityEvent	--	
Masquerading files	Malware writers often use windows system...	Microsoft	SecurityEvent	--	
Accounts and User Agents associated...	Summary of users/user agents associated ...	Microsoft	OfficeActivity	--	
Office365 authentications	Shows authentication volume by user age...	Microsoft	OfficeActivity	--	
Summary of users created using unc...	Summarizes users of uncommon & undocu...	Microsoft	SecurityEvent	--	
Powershell downloads	Finds PowerShell execution events that co...	Microsoft	SecurityEvent	--	
Script usage summary (cscript.exe)	Daily summary of vbs scripts run across th...	Microsoft	SecurityEvent	--	
Sharepoint downloads	Shows volume of documents uploaded to	Microsoft	OfficeActivity	--	

New processes observed in last 24 hours

Microsoft Provider	103 Results	SecurityEvent Data Source
Description		
Shows new processes observed in the last 24 hours versus the previous 30 days. These new processes could be benign new programs installed on hosts; however, especially in normally stable environments, these new processes could provide an indication of an unauthorized/malicious binary that has been installed and run. Reviewing the wider context of the logon sessions in which these binaries ran can provide a good starting point for identifying possible attacks.		
Query Information		
<pre>let start=datetime("2019-02-23T10:41:10.127Z"); let end=datetime("2019-02-24T10:41:10.127Z"); let processEvents=SecurityEvent where TimeGenerated > start and TimeGenerated < en where EventID==4688 project TimeGenerated, ComputerName=Computer, Acco</pre>		
View query result >		
Entities		
Tactics		
Execution		
The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system. read more...		

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

