Microsoft Sentinel

Gain visibility across your enterprise to detect and respond to threats before they can cause damage

Workshop contents

P2	Introduction
P3	About Slalom
P7	About Microsoft Sentinel
P16	Our Approach
P18	Next Steps

About Slalom

WHAT WE DO

Slalom is a purpose-led, global business and technology consulting company.

From strategy to implementation, our approach is fiercely human. We deeply understand our customers–and their customers–to deliver practical, end-to-end solutions that drive meaningful impact.

Microsoft & Slalom achieve more together.

Our business was built on Microsoft, and for nearly two decades, we've delivered innovation together. It starts with our shared purpose: realizing greater impact through collaboration and enabling every person and organization on the planet to achieve more.

We're partnering with change-making clients to shape the future around Microsoft technology—that's because as we look to the next two decades and beyond, we know the future will be built on Microsoft, too.

slalom | Microsoft

Microsoft Gold Partner

2022 US Analytics Partner of the Year

350+
Microsoft clients served in 2021

53
Microsoft Partner Awards

Microsoft Solutions

Cloud architecture and migration

Product engineering

Enterprise application strategy and deployment

Artificial Intelligence and machine learning

Data architecture

DevOps

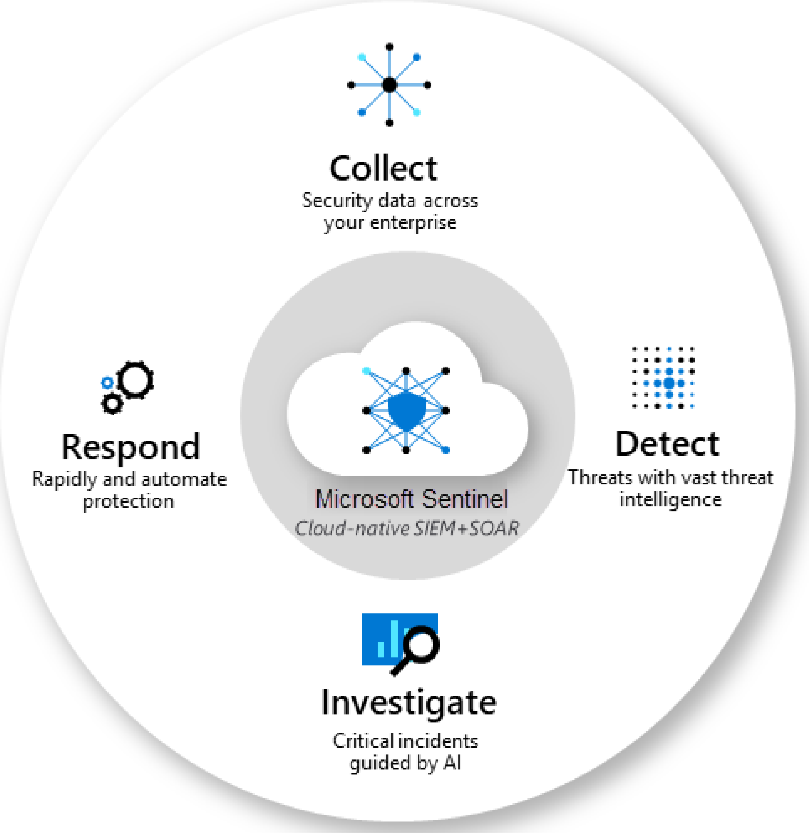
Data visualization and storytelling

Microsoft Sentinel is a scalable, cloud-native solution that provides:

Security information and event management (SIEM)

Security orchestration, automation, and response (SOAR)

Microsoft Sentinel natively incorporates proven Azure services, like Log Analytics and Logic Apps.


Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Microsoft Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

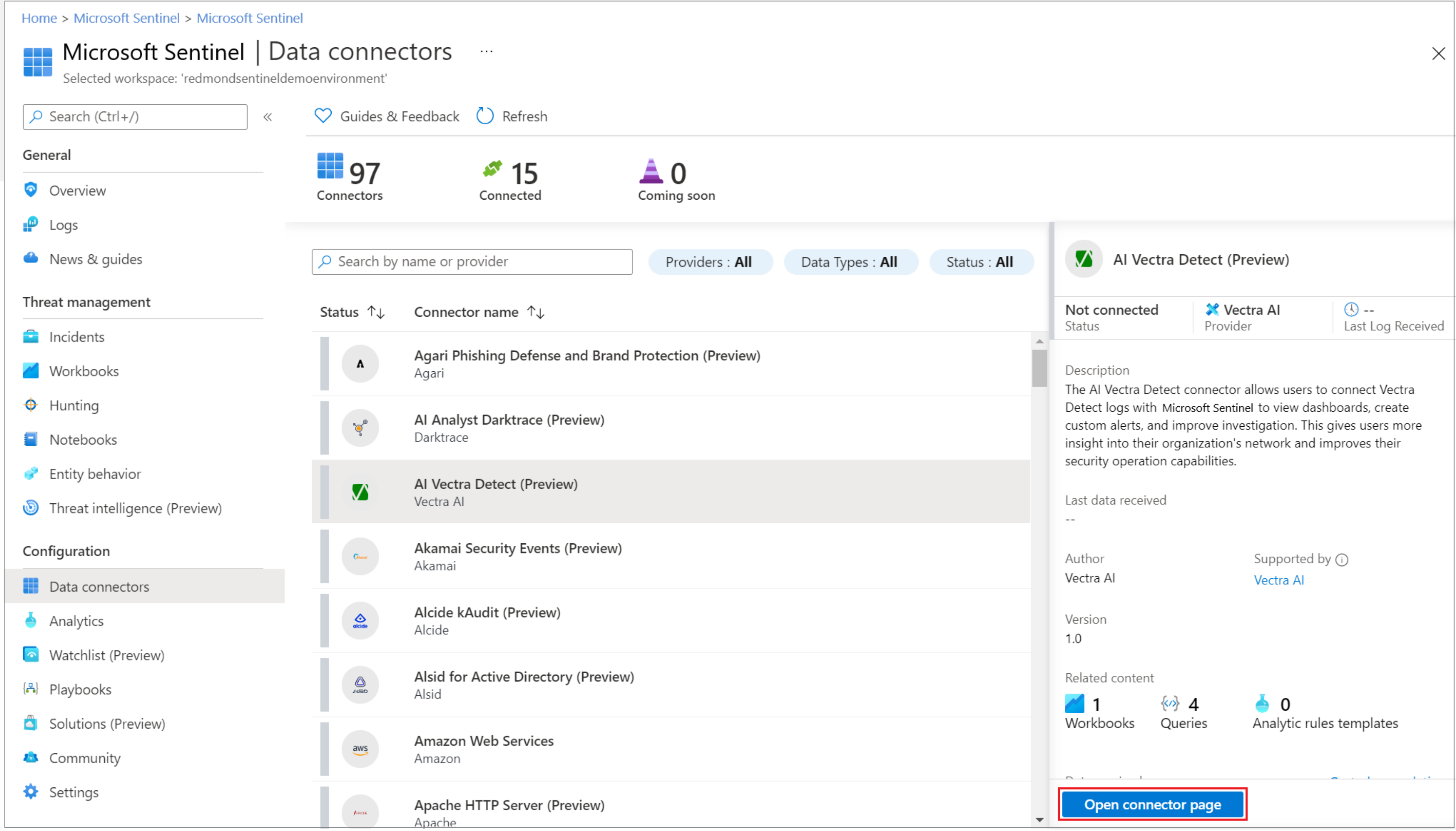
Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-prem and in multiple clouds.

Detect previously undetected threats and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

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

Collect data by using data connectors



Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Data connectors ...

Selected workspace: 'redmondsentineldemoenvironment'

97 Connectors

15 Connected

0 Coming soon

Providers : **All** Data Types : **All** Status : **All**

Status	Connector name
	Agari Phishing Defense and Brand Protection (Preview) Agari
	AI Analyst Darktrace (Preview) Darktrace
	AI Vectra Detect (Preview) Vectra AI
	Akamai Security Events (Preview) Akamai
	Alcide kAudit (Preview) Alcide
	Alsid for Active Directory (Preview) Alsid
	Amazon Web Services Amazon
	Apache HTTP Server (Preview) Apache

AI Vectra Detect (Preview)

Not connected
Status

Vectra AI
Provider

--
Last Log Received

Description

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.

Last data received

--

Author
Vectra AI

Supported by
Vectra AI

Version
1.0

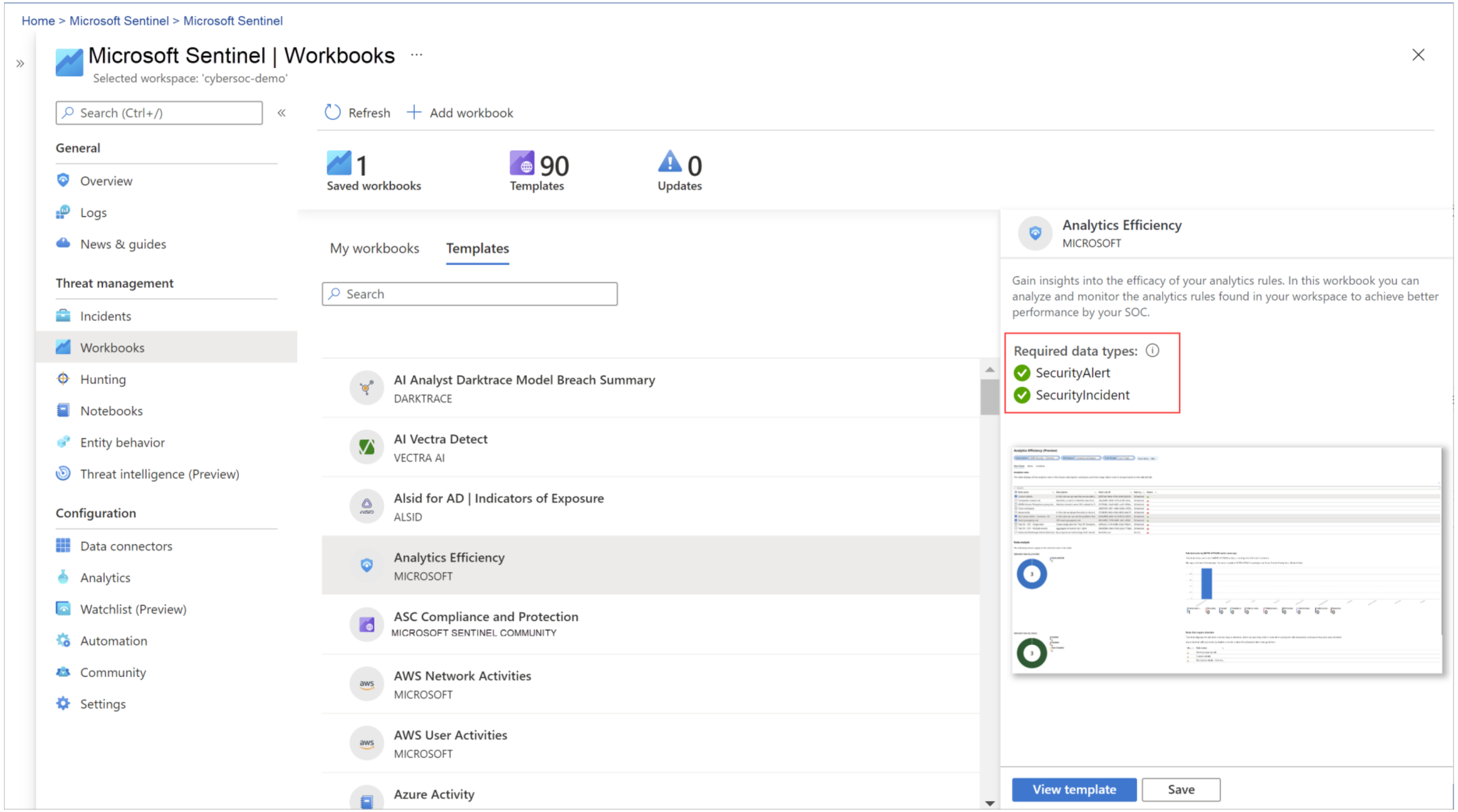
Related content

1 Workbooks

4 Queries

0 Analytic rules templates

Create interactive reports by using workbooks



AI Analyst Darktrace Model Breach Summary
DARKTRACE

AI Vectra Detect
VECTRA AI

Alsid for AD | Indicators of Exposure
ALSID

Analytics Efficiency
MICROSOFT

ASC Compliance and Protection
MICROSOFT SENTINEL COMMUNITY

AWS Network Activities
MICROSOFT

AWS User Activities
MICROSOFT

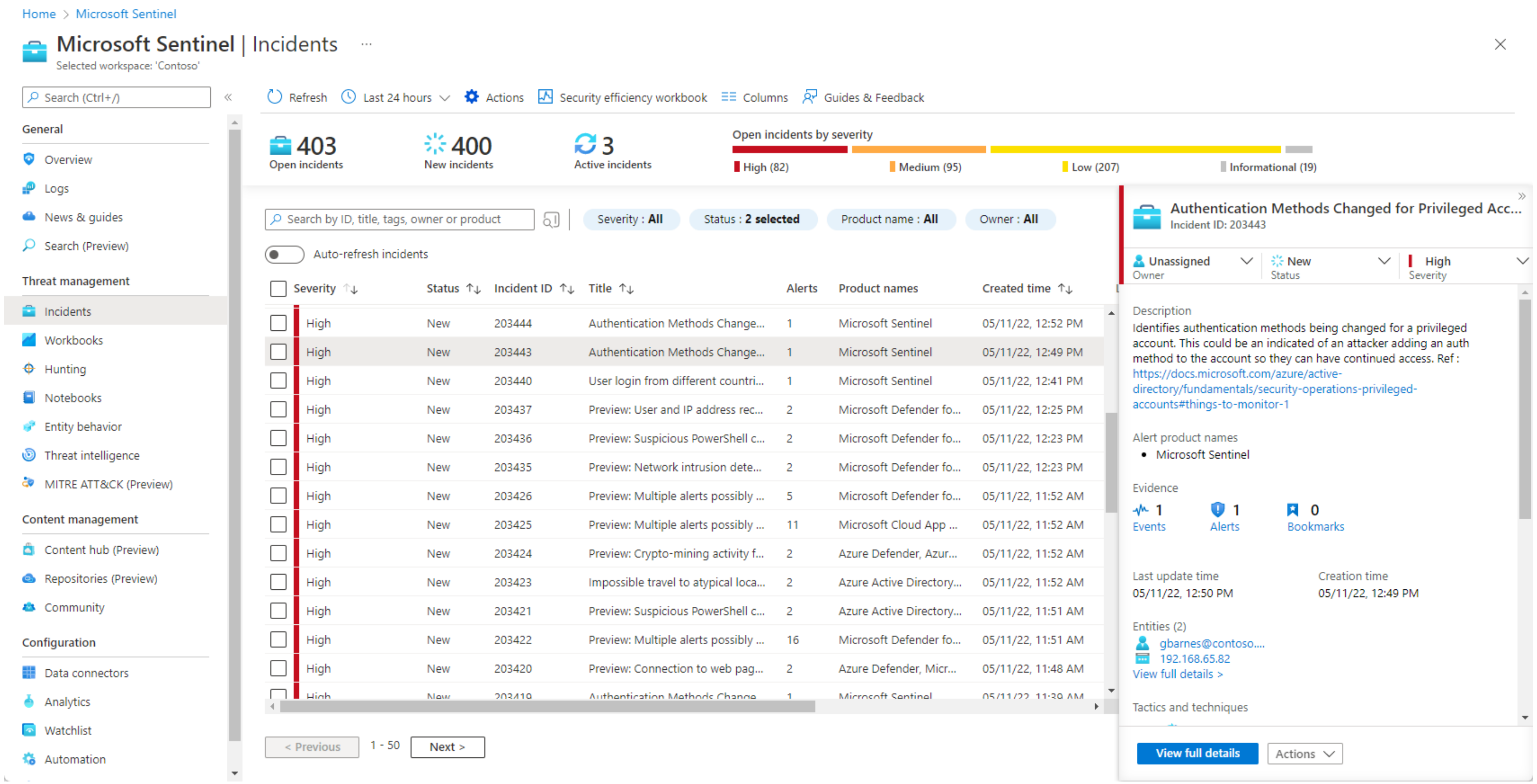
Azure Activity

Analytics Efficiency
MICROSOFT

Gain insights into the efficacy of your analytics rules. In this workbook you can analyze and monitor the analytics rules found in your workspace to achieve better performance by your SOC.

Required data types:
- ✓ SecurityAlert
- ✓ SecurityIncident

Correlate alerts into incidents by using analytics rules



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**

	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

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 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

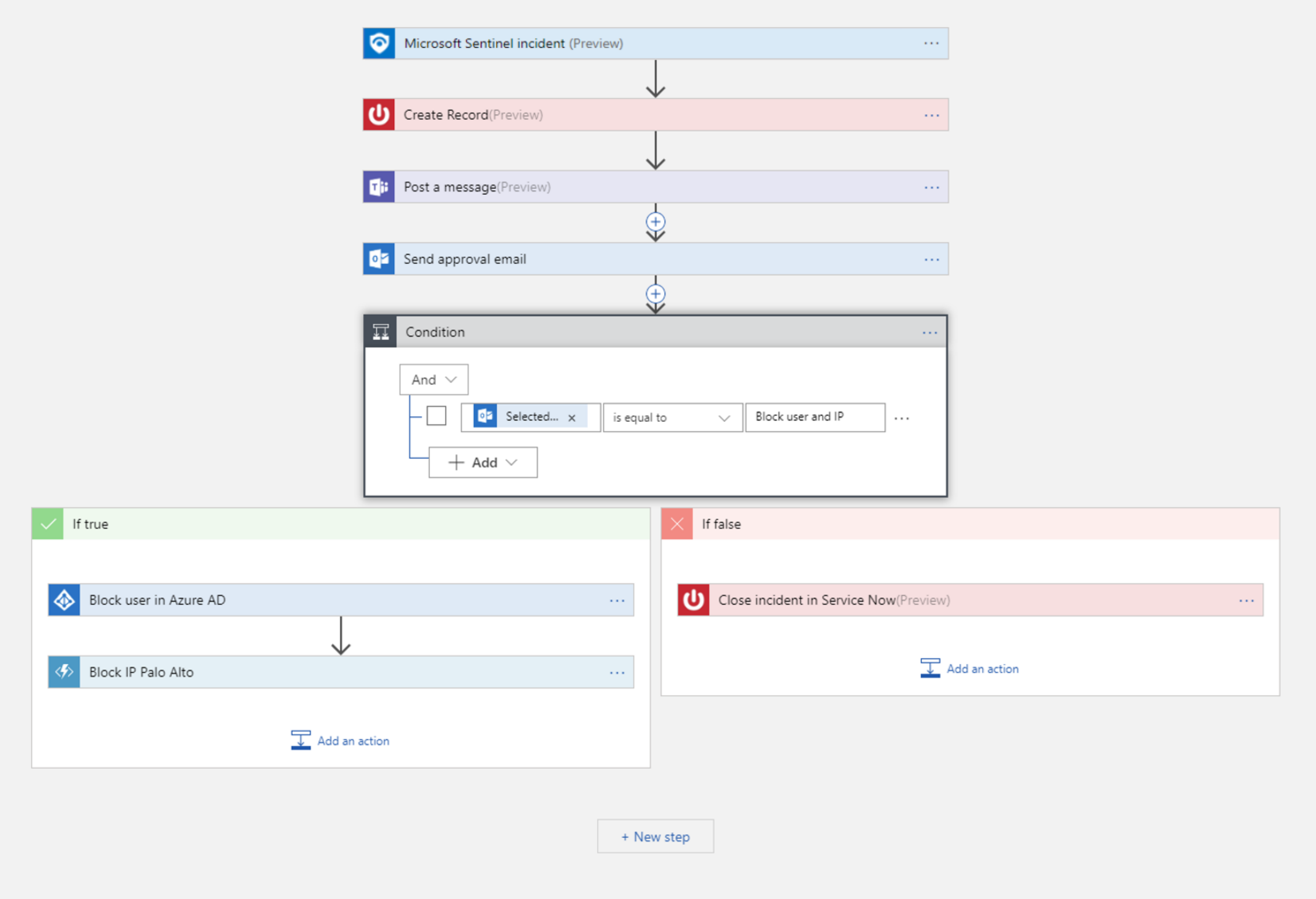
Evidence
1 Events · 1 Alerts · 0 Bookmarks

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

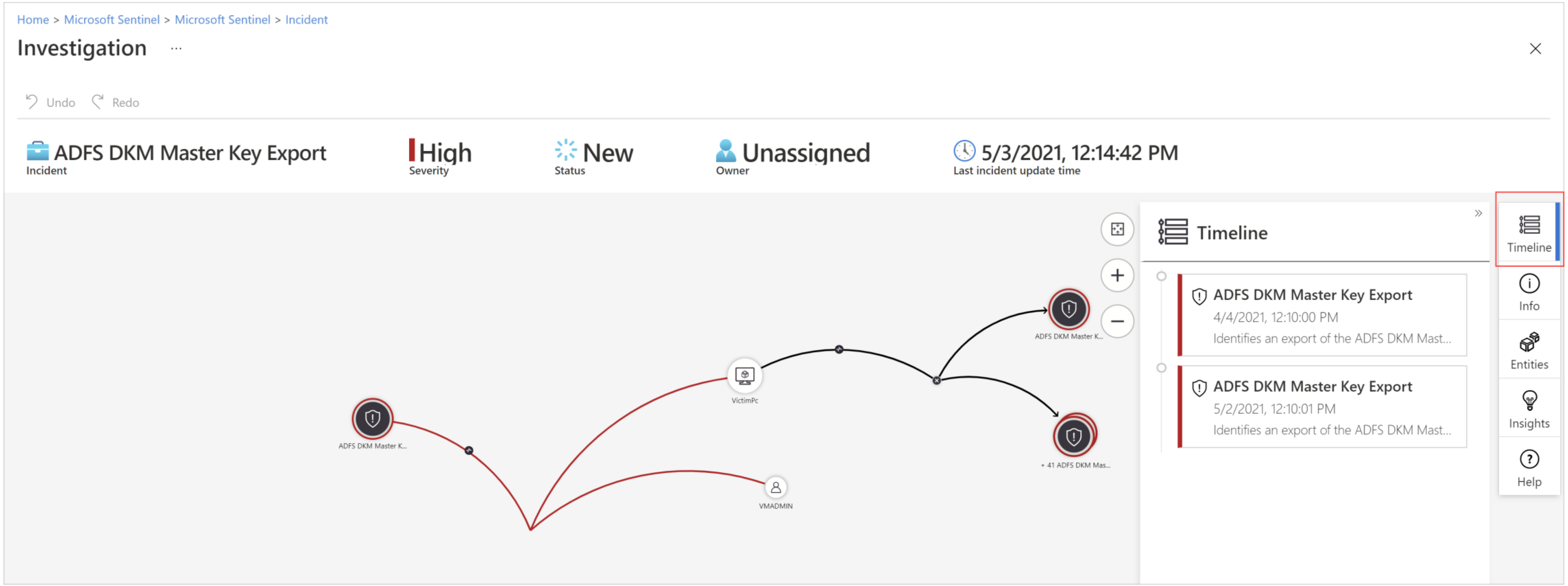
Entities (2)
gbarnes@contoso....
192.168.65.82
View full details >

Tactics and techniques

Automate and orchestrate common tasks by using playbooks



Investigate the scope and root cause of security threats



Home > Microsoft Sentinel > Microsoft Sentinel > Incident

Investigation ···

Undo Redo

ADFS DKM Master Key Export
Incident

High
Severity

New
Status

Unassigned
Owner

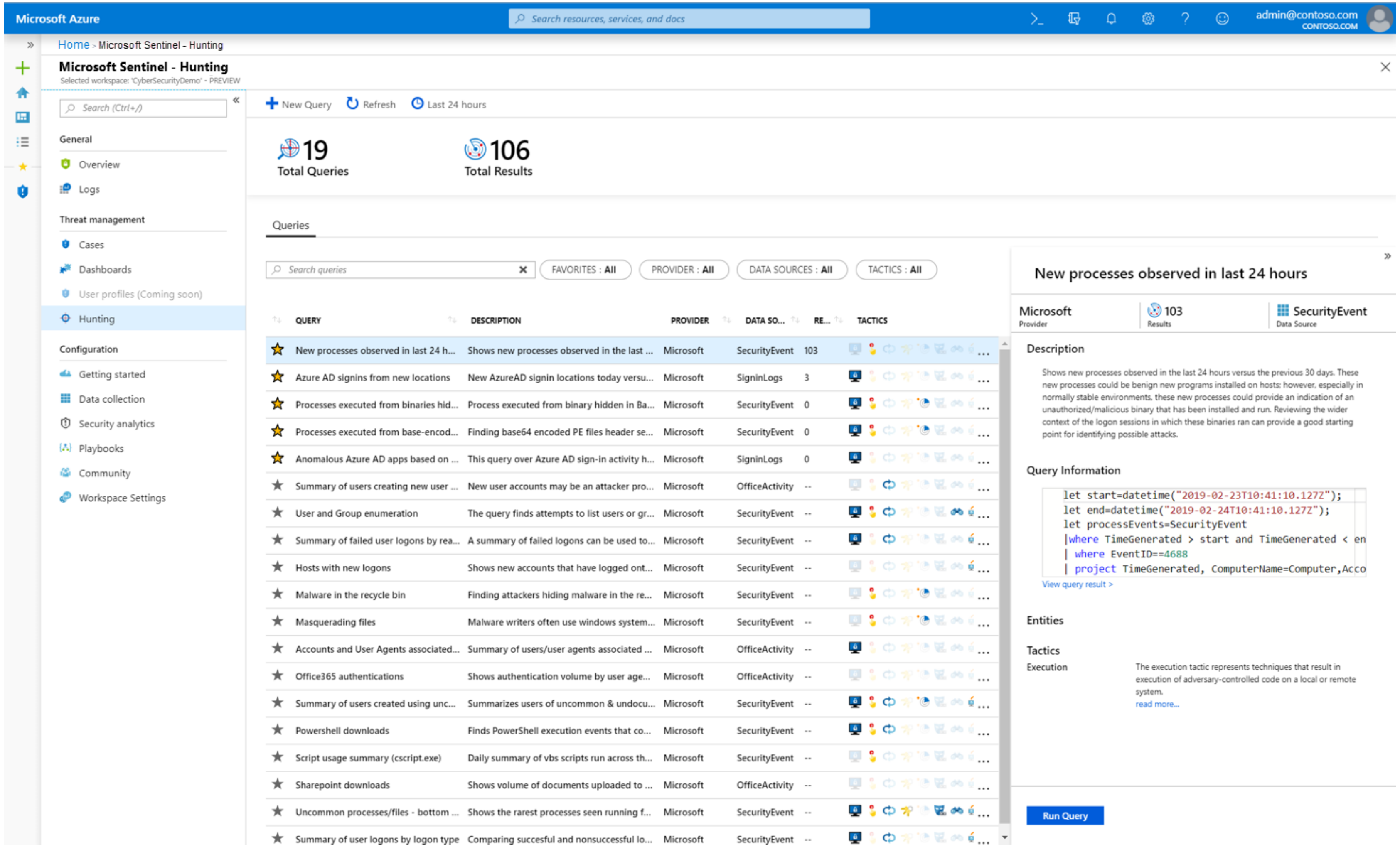
5/3/2021, 12:14:42 PM
Last incident update time

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...

Hunt for security threats by using built-in queries



Microsoft Sentinel - Hunting

Selected workspace: 'CyberSecurityDemo' - PREVIEW

19 Total Queries

106 Total Results

	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 versu...	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 ont...	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	--	...
★	Uncommon processes/files - bottom ...	Shows the rarest processes seen running f...	Microsoft	SecurityEvent	--	...
★	Summary of user logons by logon type	Comparing succesful and nonsuccessful lo...	Microsoft	SecurityEvent	--	...

New processes observed in last 24 hours

Microsoft	103	SecurityEvent
Provider	Results	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

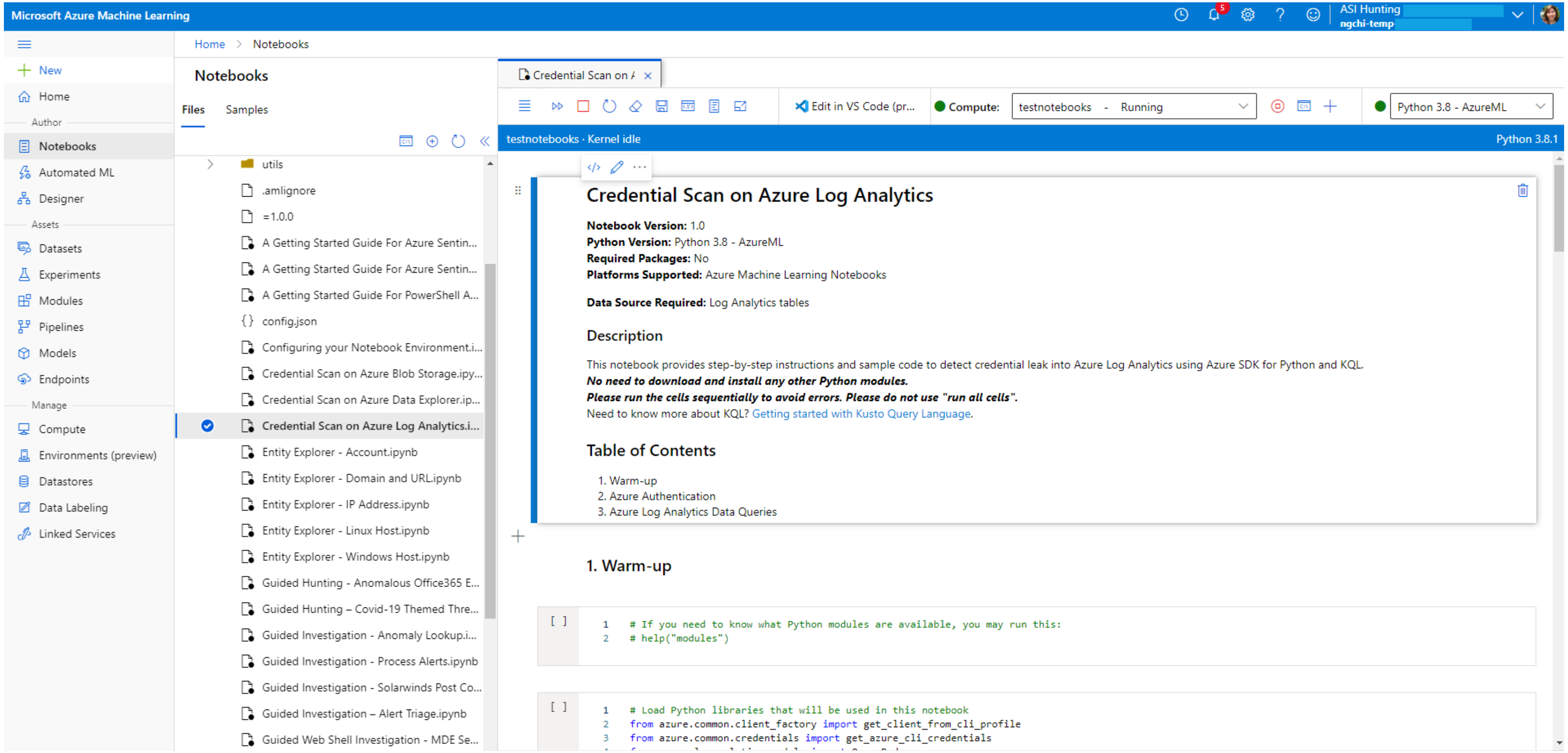
```
let start=datetime("2019-02-23T10:41:10.127Z");
let end=datetime("2019-02-24T10:41:10.127Z");
let processEvents=SecurityEvent
|where TimeGenerated > start and TimeGenerated < en
| where EventID==4688
| project TimeGenerated, ComputerName=Computer,Acco
```

Entities

Tactics

Execution — The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.

Enhance your threat hunting with notebooks



Microsoft Azure Machine Learning
ASI Hunting [redacted]
ngchi-temp [redacted]
Home > Notebooks
New
Home
Author
Notebooks
Automated ML
Designer
Assets
Datasets
Experiments
Modules
Pipelines
Models
Endpoints
Manage
Compute
Environments (preview)
Datastores
Data Labeling
Linked Services
Notebooks
Files
Samples
utils
.amlignore
=1.0.0
A Getting Started Guide For Azure Sentin...
A Getting Started Guide For Azure Sentin...
A Getting Started Guide For PowerShell A...
config.json
Configuring your Notebook Environment.i...
Credential Scan on Azure Blob Storage.ipy...
Credential Scan on Azure Data Explorer.ip...
Credential Scan on Azure Log Analytics.i...
Entity Explorer - Account.ipynb
Entity Explorer - Domain and URL.ipynb
Entity Explorer - IP Address.ipynb
Entity Explorer - Linux Host.ipynb
Entity Explorer - Windows Host.ipynb
Guided Hunting - Anomalous Office365 E...
Guided Hunting – Covid-19 Themed Thre...
Guided Investigation - Anomaly Lookup.i...
Guided Investigation - Process Alerts.ipynb
Guided Investigation - Solarwinds Post Co...
Guided Investigation – Alert Triage.ipynb
Guided Web Shell Investigation - MDE Se...
Credential Scan on A
Edit in VS Code (pr...
Compute:
testnotebooks - Running
Python 3.8 - AzureML
testnotebooks · Kernel idle
Python 3.8.1

Credential Scan on Azure Log Analytics

Notebook Version: 1.0
Python Version: Python 3.8 - AzureML
Required Packages: No
Platforms Supported: Azure Machine Learning Notebooks

Data Source Required: Log Analytics tables

Description

This notebook provides step-by-step instructions and sample code to detect credential leak into Azure Log Analytics using Azure SDK for Python and KQL.
No need to download and install any other Python modules.
Please run the cells sequentially to avoid errors. Please do not use "run all cells".
Need to know more about KQL? Getting started with Kusto Query Language.

Table of Contents

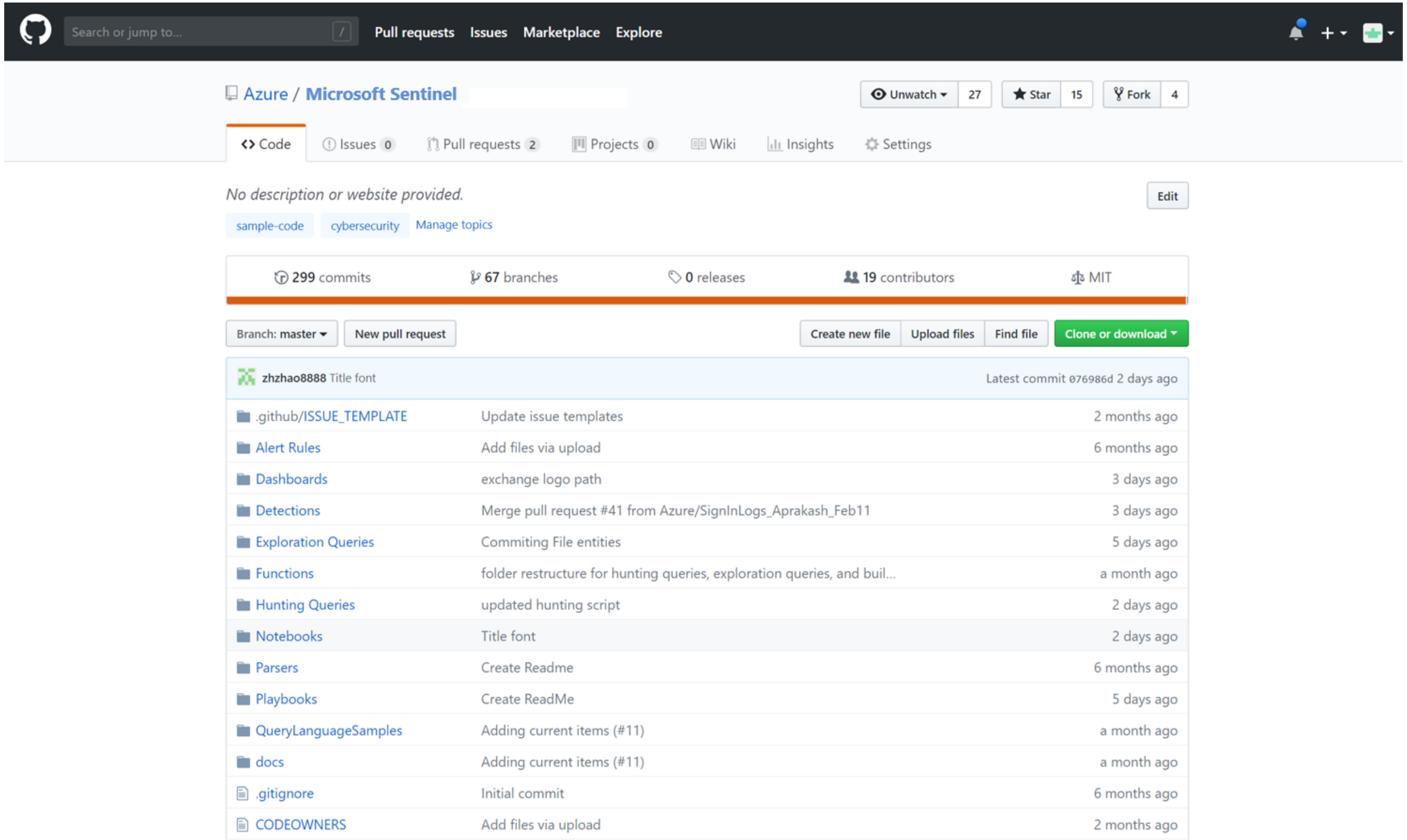
1. Warm-up
2. Azure Authentication
3. Azure Log Analytics Data Queries

1. Warm-up

```
[ ]
# If you need to know what Python modules are available, you may run this:
# help("modules")
```

```
[ ]
# Load Python libraries that will be used in this notebook
from azure.common.client_factory import get_client_from_cli_profile
from azure.common.credentials import get_azure_cli_credentials
```

Download security content from the community



Azure / **Microsoft Sentinel**

No description or website provided.

sample-code cybersecurity

299 commits · 67 branches · 0 releases · 19 contributors · MIT

zhzhao8888 Title font — Latest commit 076986d 2 days ago

.github/ISSUE_TEMPLATE	Update issue templates	2 months ago
Alert Rules	Add files via upload	6 months ago
Dashboards	exchange logo path	3 days ago
Detections	Merge pull request #41 from Azure/SignInLogs_Aprakash_Feb11	3 days ago
Exploration Queries	Commiting File entities	5 days ago
Functions	folder restructure for hunting queries, exploration queries, and buil…	a month ago
Hunting Queries	updated hunting script	2 days ago
Notebooks	Title font	2 days ago
Parsers	Create Readme	6 months ago
Playbooks	Create ReadMe	5 days ago
QueryLanguageSamples	Adding current items (#11)	a month ago
docs	Adding current items (#11)	a month ago
.gitignore	Initial commit	6 months ago
CODEOWNERS	Add files via upload	2 months ago

Our Approach

Technology that empowers your business

Security in harmony with your business

People First

We aren't just here to implement technology; we are here to implement technology that works for you.

We work alongside your teams to bring business process and technology together.

Impactful Delivery

Leverage our industry and product expertise to quickly navigate everchanging compliance and regulatory requirements

Enable flexibility with solutions and policies tailored to your unique needs

Long Term Planning

Set you up for a successful future, drive meaningful impact, and limit business disruption.

What’s next for you?

Connect with us to schedule a:

- 1:1 Demo for you and your team
- Proof of concept in your environment
- Customized Strategy Session
- Requirements Gathering and Implementation Roadmap

slalom | Microsoft