



"I finally master Azure's products, acronyms, and concepts! It was a breeze!"

François, 26 years old



SIEM

Ms SENTINEL

● SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

● Combines SIM and SEM to provide real-time analysis of security alerts generated by network hardware and applications.



SIM

LOG MANAGEMENT

Focus on simple collection and storage of log messages and audit trails.

SECURITY INFORMATION MANAGEMENT (SIM)

Long-term storage as well as analysis and reporting of log data.



SEM

EVENT LOGS

Systems and applications generate events which are kept in event logs. Lists of activities that occurred, with records of new events being appended to the end of the logs as they occur.

SECURITY EVENT MANAGEMENT (SEM)

Real-time monitoring, correlation of events, notifications, and console views.



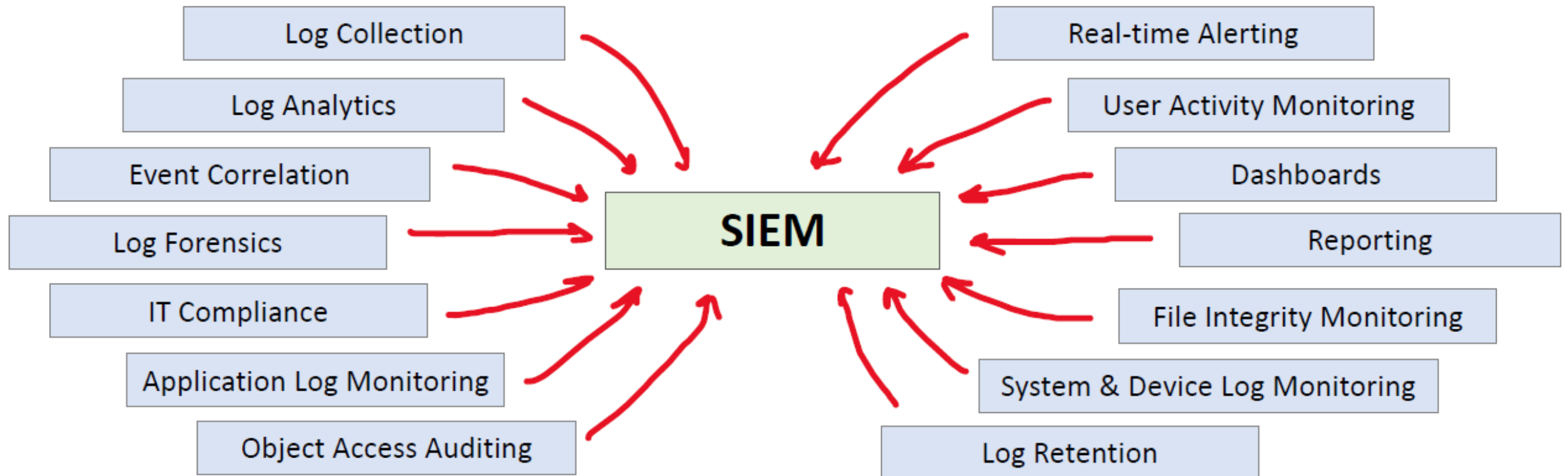
(STRUCTURED) LOGS VS EVENT LOGS

- All events can be represented as structured logs, but not all structured logs are events.
- Unlike logs, events describe a unit of work, meaning they contain all the information about what it took for a service to perform a certain job.
- Not every log is an event in its entirety.
- Logs are usually only portions of events.
- A group of logs can compose a single event.

SIM + SEM = SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Combines SIM and SEM to **provides real-time analysis of security alerts** generated by network hardware and applications



Microsoft Sentinel

TO GET STARTED WITH MICROSOFT SENTINEL, YOU NEED A SUBSCRIPTION TO MICROSOFT AZURE.

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

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)



Microsoft Sentinel uses built-in AI to help you quickly analyze large volumes of data across an enterprise. Microsoft Sentinel aggregates data from various sources, including users, applications, servers, and devices running on-premises or in any cloud, letting you reason over millions of records in a few seconds. With Microsoft Sentinel, you can:

- **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 Microsoft's 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 tasks.



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 by using data connectors

Home > Microsoft Sentinel > Microsoft Sentinel



Microsoft Sentinel | Data connectors

Selected workspace: 'contoso-sentinel-workspace'

Search Refresh Guides & Feedback

- 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

137
Connectors

12
Connected

More content at
Content hub

Search by name or provider

Providers : All

Data Types : All

Status : All

Status Connector name ↑



Azure Active Directory

Microsoft



Azure Active Directory Identity Protection

Microsoft



Azure Activity

Microsoft



Azure Data Lake Storage Gen1

Microsoft



Azure Active Directory

Connected
Status

Microsoft
Provider

35 Min...
Last Log Rec...

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app

[Open connector page](#)

Create interactive reports by using workbooks

Home > Microsoft Sentinel > Microsoft Sentinel



Microsoft Sentinel | Workbooks

Selected workspace: 'cybersoc-demo'

Search (Ctrl+/)



Refresh



Add workbook

General



Overview



Logs



News & guides

Threat management



Incidents



Workbooks



Hunting



Notebooks



Entity behavior



Threat intelligence (Preview)

Configuration



Data connectors



Analytics



Watchlist (Preview)



Automation



Community



Settings



1

Saved workbooks



90

Templates



0

Updates

My workbooks

Templates



Search



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



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.

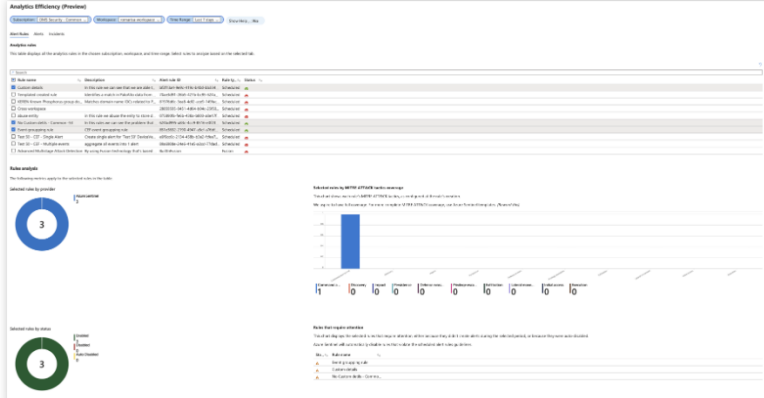
Required data types: ⓘ



SecurityAlert



SecurityIncident



Correlate alerts into incidents by using analytics rules

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

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

< Previous

1 - 50

Next >

Authentication Methods Changed for Privileged Acc...

Incident ID: 203443

Unassigned
Owner

New
Status

High
Severity

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)

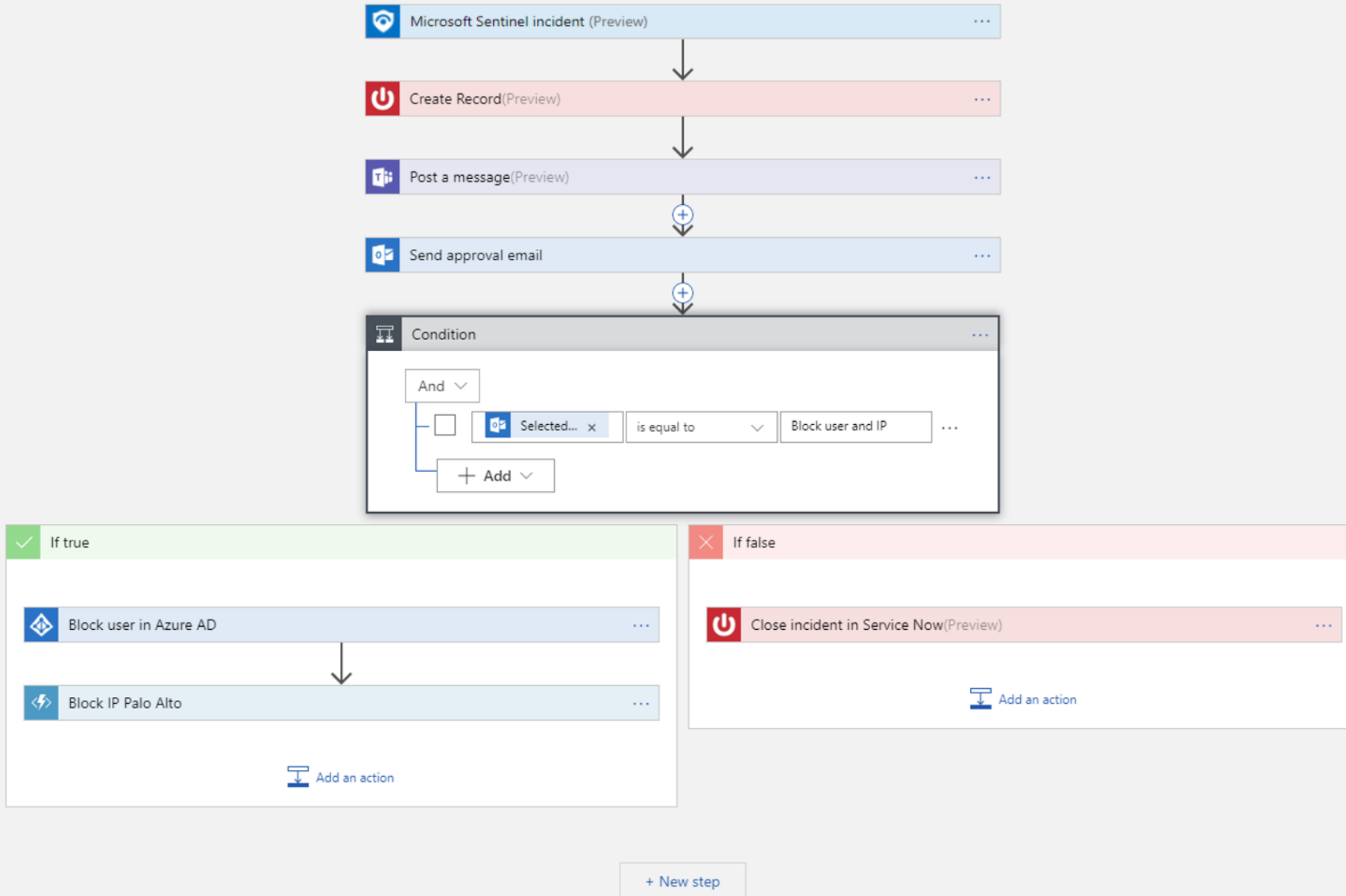
[gbarnes@contoso...](#)
[192.168.65.82](#)
[View full details >](#)

Tactics and techniques

View full details

Actions

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

ADFS DKM Master K...

VictimPc

VMADMIN

ADFS DKM Master K...

+ 41 ADFS DKM Mas...

+

-

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

Hunt for security threats by using built-in queries

Microsoft Azure

Search resources, services, and docs

admin@contoso.com

Home - Microsoft Sentinel - Hunting

Microsoft Sentinel - Hunting

Selected workspace: 'CyberSecurityDemo' - PREVIEW

Search (Ctrl+/)

General

Overview

Logs

Threat management

Cases

Dashboards

User profiles (Coming soon)

Hunting

Configuration

Getting started

Data collection

Security analytics

Playbooks

Community

Workspace Settings

New Query

Refresh

Last 24 hours

19

Total Queries

106

Total Results

Queries

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 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

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

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
[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...](#)

Run Query

Enhance your threat hunting with notebooks

The screenshot displays the Microsoft Azure Machine Learning web interface. The top navigation bar includes the 'Microsoft Azure Machine Learning' logo, a home icon, a 'Home' link, and a 'Notebooks' link. The left sidebar contains a 'New' button and a list of resources: Home, Author, Notebooks, Automated ML, Designer, Assets, Datasets, Experiments, Modules, Pipelines, Models, Endpoints, Manage, Compute, Environments (preview), Datastores, Data Labeling, and Linked Services. The main content area is divided into a file explorer on the left and a notebook editor on the right. The file explorer shows a directory structure with a 'utils' folder and several files, including 'Credential Scan on Azure Log Analytics.ipynb', which is selected. The notebook editor shows the title 'Credential Scan on Azure Log Analytics' and a table of contents with three sections: '1. Warm-up', '2. Azure Authentication', and '3. Azure Log Analytics Data Queries'. The '1. Warm-up' section is expanded, showing two code cells. The first code cell contains a comment and a call to help for the 'modules' module. The second code cell contains a comment and imports for 'get_client_from_cli_profile' and 'get_azure_cli_credentials' from the 'azure.common' module.

Microsoft Azure Machine Learning

Home > Notebooks

Notebooks

Files Samples

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




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

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


Download security content from the community



[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

[Azure](#) / [Microsoft Sentinel](#)

[Unwatch](#) 27 [Star](#) 15 [Fork](#) 4

[Code](#) [Issues](#) [Pull requests](#) [Projects](#) [Wiki](#) [Insights](#) [Settings](#)

No description or website provided.

[sample-code](#) [cybersecurity](#) [Manage topics](#)

[299](#) commits [67](#) branches [0](#) releases [19](#) contributors [MIT](#)

Branch: master [New pull request](#) [Create new file](#) [Upload files](#) [Find file](#) [Clone or download](#)

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	Committing 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