



Understanding Azure Sentinel

examlabpractice.com



<https://t.me/learningnets>



What is Azure Sentinel?

Azure Sentinel is a scalable, cloud based, security information event management (SIEM) and security orchestration automated response (SOAR) product. Sentinel delivers intelligent security analytics and threat intelligence solution, providing a centralized point for alert detection, threat visibility, proactive hunting, and threat response.

Purposes of Sentinel

Azure Sentinel is your eye in the sky for viewing across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution timeframes.

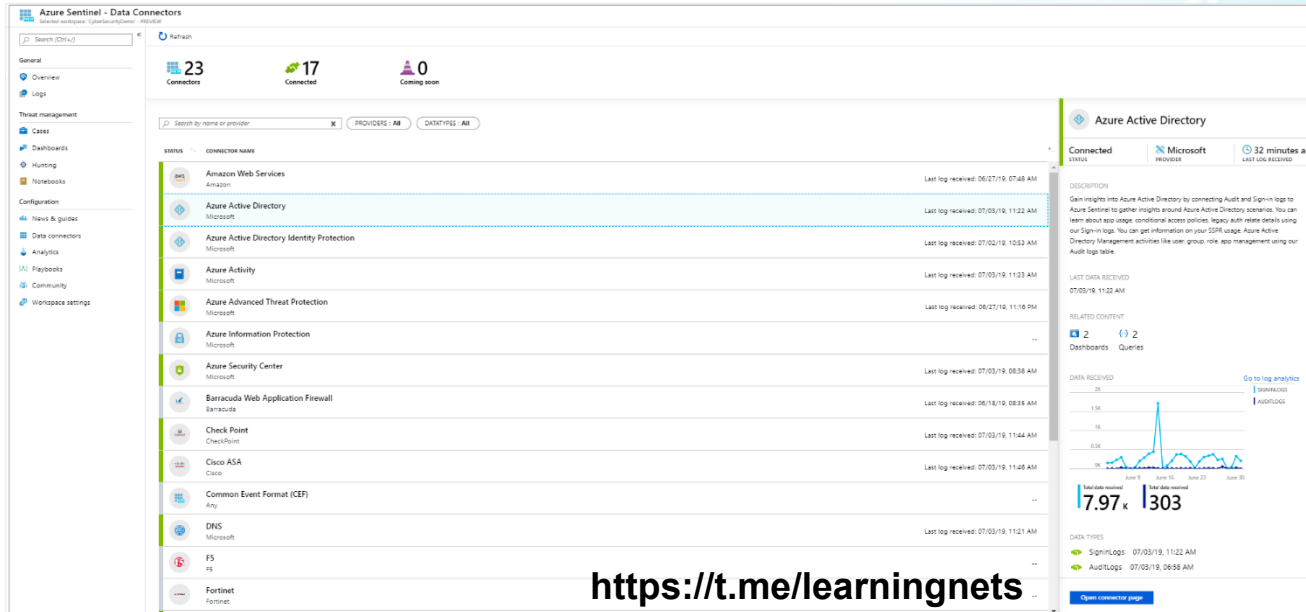
- Data collection at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in the cloud.
- Find previously undetected threats, and minimize false positives using Microsoft's analytics and threat intelligence.
- Investigate threats with artificial intelligence, and hunt for suspicious activities, tapping into years of cyber security work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks

<https://t.me/learningnets>



Connect With All Of Your Data

Azure Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft Threat Protection solutions, and Microsoft 365 sources, including Office 365, Azure AD, Azure ATP, and Microsoft Cloud App Security, and more.



The screenshot displays the Azure Sentinel Data Connectors interface. On the left, a navigation pane includes sections for General, Threat management, Configuration, and Workspace settings. The main area shows a list of connectors with columns for status, name, provider, and last log received. The 'Azure Active Directory' connector is highlighted, and its details are shown in a right-hand pane. This pane includes a description of the connector, a 'LAST DATA RECEIVED' timestamp, a 'RELATED CONTENT' section with links to dashboards and queries, and a 'DATA RECEIVED' line chart showing activity over time. Below the chart, there are two large numbers: 7.97k and 1303, representing data volume. At the bottom of the interface, there is a link to 'Open connector page'.

STATUS	CONNECTION NAME	PROVIDERS	DATA TYPES	LAST LOG RECEIVED
Connected	Amazon Web Services	Amazon		06/27/19, 07:48 AM
Connected	Azure Active Directory	Microsoft		07/03/19, 11:22 AM
Connected	Azure Active Directory Identity Protection	Microsoft		07/02/19, 10:53 AM
Connected	Azure Activity	Microsoft		07/03/19, 11:23 AM
Coming soon	Azure Advanced Threat Protection	Microsoft		06/27/19, 11:16 PM
Coming soon	Azure Information Protection	Microsoft		--
Connected	Azure Security Center	Microsoft		07/03/19, 08:38 AM
Connected	Barracuda Web Application Firewall	Barracuda		06/18/19, 08:33 AM
Connected	Check Point	CheckPoint		07/03/19, 11:44 AM
Connected	Cisco ASA	Cisco		07/03/19, 11:45 AM
Coming soon	Common Event Format (CEF)	Any		--
Connected	DNS	Microsoft		07/03/19, 11:21 AM
Coming soon	F5	F5		--
Coming soon	Fortinet	Fortinet		--

Azure Active Directory
Connected status | Microsoft provider | 32 minutes ago | Last log received

DESCRIPTION
Get insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure 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 SSPR usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

LAST DATA RECEIVED
07/03/19, 11:22 AM

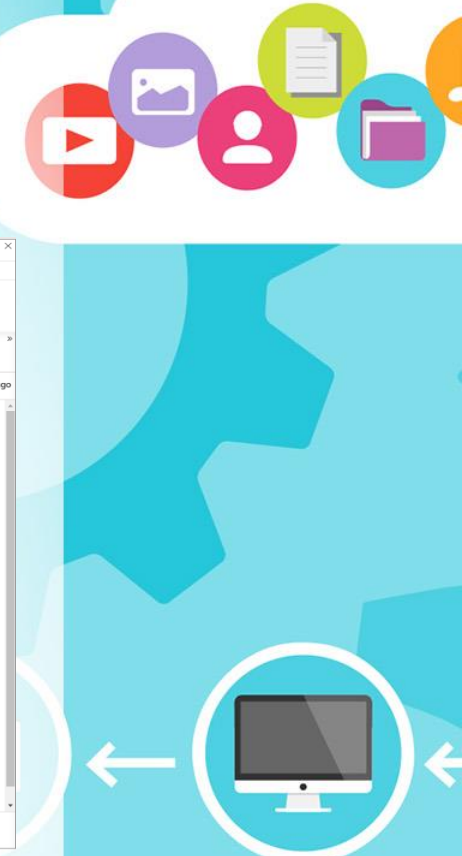
RELATED CONTENT
2 Dashboards | 2 Queries

DATA RECEIVED
7.97k | 1303

DATA TYPES
SignLogs: 07/03/19, 11:22 AM
AuditLogs: 07/03/19, 06:56 AM

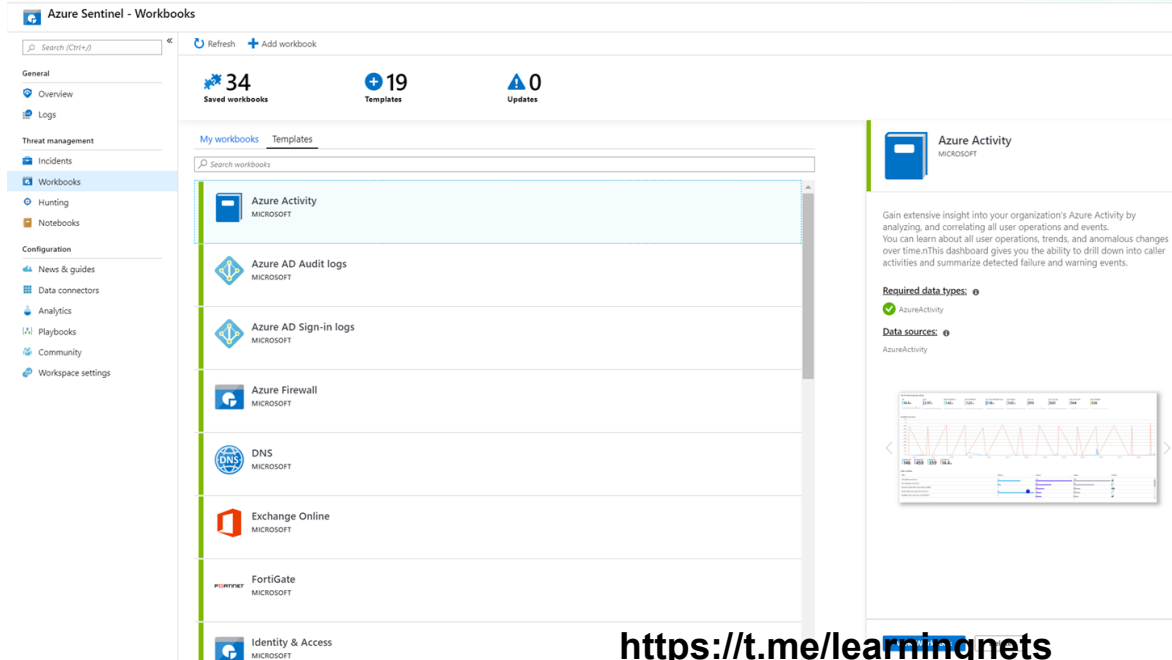
[Open connector page](#)

<https://t.me/learningnets>



Workbooks

Azure Sentinel, you can monitor the data using the Azure Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks.



<https://t.me/learningnets>



Analytics

To help you reduce noise and minimize the number of alerts you have to review and investigate, Azure Sentinel uses analytics to correlate alerts into incidents. Incidents are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve.



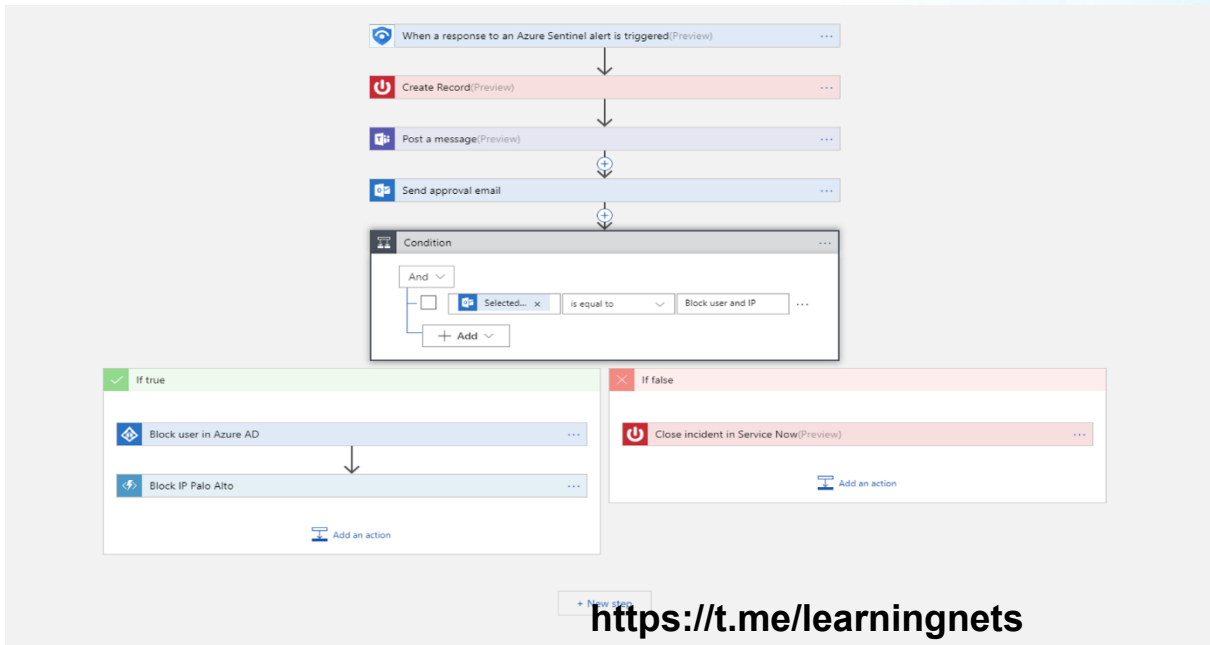
INCIDENT ID	TITLE	ALERTS	PRODUCT	CREATED TIME	OWNER	STATUS
17758	Suspicious Volume Shadow Copy ...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
17757	Suspicious command execution	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
17756	Suspicious process executed	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
17755	Suspicious double extension file e...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
17743	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 10:40 PM	Unassigned	New
17741	Suspicious authentication activity	1	Azure Secur...	09/14/19, 10:33 PM	Unassigned	New
17729	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 09:40 PM	Unassigned	New
17716	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 08:40 PM	Unassigned	New
17714	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:34 PM	Unassigned	New
17713	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
17712	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
17711	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
17710	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
17709	Susioicious authentication activitv	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New

<https://itmelearning.net>



Security Automation & Orchestration

Automate your common tasks and simplify security orchestration with playbooks that integrate with Azure services as well as your existing tools. Built on the foundation of Azure Logic Apps, Azure Sentinel's automation and orchestration solution provides a highly-extensible architecture that enables scalable automation as new technologies and threats emerge.



<https://t.me/learningnets>



Investigation

Azure Sentinel deep investigation tools help you to understand the scope and find the root cause, of a potential security threat. You can choose an entity on the interactive graph to ask interesting questions for a specific entity, and drill down into that entity and its connections to get to the root cause of the threat.



Incident Anomalous login **Medium Severity** **New Status** **admin@contoso.com Owner** **3/14/2019, 11:32:00 AM Last incident update time**

Timeline

- Anomalous login**
3/13/2019, 10:21:00 AM
Finds cases in which we had more than 400 failed logins L...
- Suspicious Powershell Activity Detec...**
3/13/2019, 11:25:00 AM
Analysis of host data detected a powershell script running...
- Anomalous sign-in to multiple comp...**
3/13/2019, 1:51:00 PM
Account sign-in activity indicates numerous sign-ins to m...
- Mass download**
3/13/2019, 2:48:00 PM
The user 'Darcy Robles (darcyrobles@contoso.com)' dow...

<https://t.me/learningnets>



Hunting

Use Azure Sentinel's powerful hunting search-and-query tools, based on the MITRE framework, which enable you to proactively hunt for security threats across your organization's data sources, before an alert is triggered.



The screenshot displays the Azure Sentinel Hunting console. On the left is a navigation pane with sections like 'General', 'Threat management', 'Configuration', and 'Hunting'. The main area shows a list of queries with columns for 'QUERY', 'DESCRIPTION', 'PROVIDER', 'DATA SOURCE', 'RESULTS', and 'TACTICS'. The top of the main area shows '19 Total Queries' and '106 Total Results'. A detailed view for the query 'New processes observed in last 24 hours' is shown on the right, including a description, query information with a KQL query, entities, and tactics.

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

Entities

Tactics

Execution

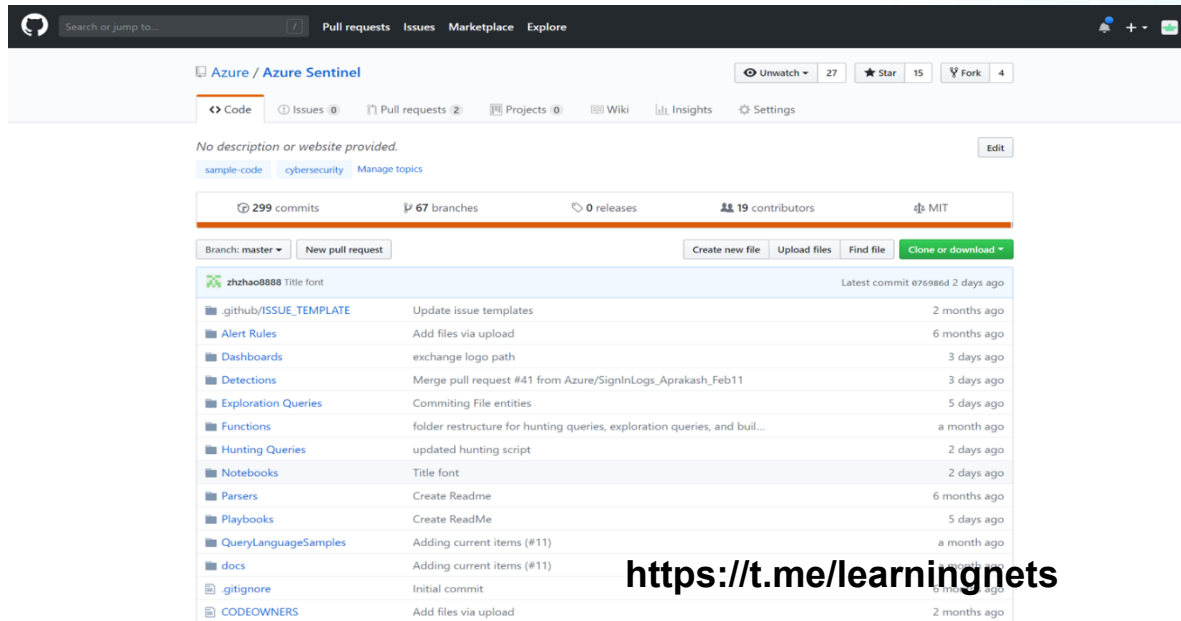
The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.

<https://t.me/learningnets>



Community

The Azure Sentinel community is a powerful resource for threat detection and automation. Our Microsoft security analysts constantly create and add new workbooks, playbooks, hunting queries, and more, posting them to the community for you to use in your environment.



The screenshot shows the GitHub repository for Azure Sentinel. The repository has 299 commits, 67 branches, 0 releases, and 19 contributors. The files and folders listed are:

File/Folder	Description	Latest Commit
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

<https://t.me/learningnets>

