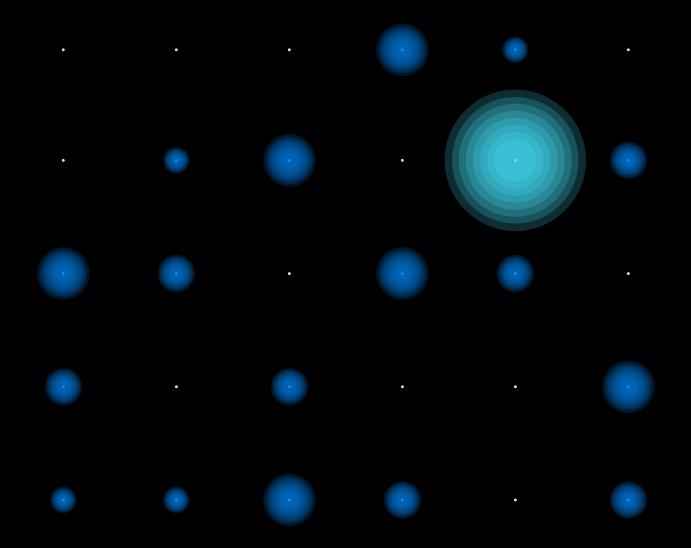
eBook Series



Cloud-Native SIEM: Quick-Start Guide to Azure Sentinel



02

05 /

Why Azure Sentinel?

08/

Getting started with Azure Sentinel

09 Step 1 Access Azure Sentinel 10 Step 2

Connect your data

- 12 Step 3 Use overview dashboard and workbooks to get visibility across enterprise
- 16 Step 4 Detect threats
- **19** Step 5 Investigate incidents
- 23 Step 6 Respond to threats
- 25 Step 7 Hunt for threats



03

Digital and cloud transformation continue to reshape IT. Information security leaders face growing complexity, diverse attack surfaces, alerts growing by orders of magnitude, as well as increasingly sophisticated and difficult-todetect cyber assaults, including insider threats – all in the context of exponential growth in data volume. At the same time, they need to find ways to make systems and processes more efficient, control costs and manage resources.

As IT becomes more strategic, the importance of security grows daily.

A compromised digital business loses trust, customers and revenue. Cyber defence will not suffice. Only a proactive approach to risk answers the call. Organisations need the ability to connect and collect data from all systems, whether in the cloud or on premises, commercial or homegrown.

Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges – let alone tomorrow's unimagined risks. Costly to operate and slow to scale, resource-heavy SIEM infrastructure and tools can easily become obstacles to digital transformation. Evergrowing volumes of data strain the limits of on-premises systems. Managing those same systems creates a huge operational burden that takes time away from strategic activities. Alert fatigue is reaching all-time highs, yet few organisations want to throw more money at the problem. Traditional approaches simply can't handle the pace of change, and IT departments don't have more money to throw at the problem.

That's why Microsoft developed Azure Sentinel, a fully cloud-native SIEM designed to serve all four aspects of security operations.

- Collect data at cloud scale across all users, devices, applications and infrastructure, both on-premises and in multiple clouds.
- **Detect** previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft.
- Investigate threats with AI and proactively 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.

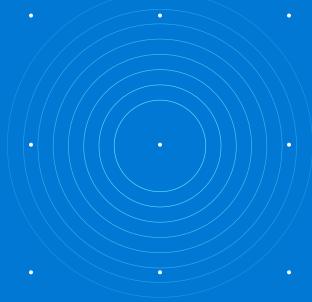
Built on Microsoft Azure, a leading public cloud platform, Azure Sentinel eliminates infrastructure and management complexity. It scales readily to meet dynamic needs. It maximises the skills of your entire team with intelligent, role-based tools. And, it empowers you with insights from Microsoft's global security operations.

Cloud-Native SIEM: Quick-Start Guide to Azure Sentinel

01/

Why Azure Sentinel?

- · · · · ·
- · · · · ·
 - • •
 - - •



Azure Sentinel offers tools for all members of your security team.

Improve threat protection with AI on your side: Intelligent correlation helps reduce false positives and alert fatigue by up to 90% and can detect complex, multi-stage attacks giving you the power to focus on what matters. Built-in intelligence helps automate and orchestrate up to 80% of common tasks, simplifying operations and accelerate threat response.

Secure your entire enterprise: Integrate with existing tools, whether business applications, other security products or home-grown software. Analyse data from users, applications and infrastructure, both on-premises and multi-cloud. Get started fast and grow as needed with a broad range of connectors and industry-standard data formats.

Invest in security, not servers: Powered by the Microsoft cloud platform, Azure Sentinel delivers near-limitless speed and scale without the operational hassle of server-based SIEM. Proven, scalable log analytics get you insights in seconds. That means lower cost, more agility and more time to focus on real security issues.

Cloud-Native SIEM: Quick-Start Guide to September **Azure Sentinel**

2019

Free storage and analysis for Office 365

data: To help you maximise security effectiveness across your enterprise, Azure Sentinel empowers you to bring in data from Microsoft Office 365 for analysis and retain it for free, all in just a few clicks.

Build on Microsoft's investment: In security, knowledge is power. With Azure Sentinel, you gain the power of Microsoft's decades of experience managing security at a massive global scale. Microsoft solutions share insights gained from unparalleled threat intelligence that is informed from analysing trillions of signals every day. Our security experts support proactive threat hunting with prebuilt queries based on years of security experience.

The role of Log Analytics

Azure Sentinel is built on the highly scalable, high performance Azure Monitor Log Analytics platform. Log Analytics is a proven analytics platform designed to store and analyse massive amounts of data in seconds.

Log Analytics uses Kusto query language (KQL), a rich language designed to be easy to read and author. It allows you to join data from multiple tables, aggregate large sets of data and perform complex operations with minimal code. Virtually any question can be answered quickly and analysis performed as long as the supporting data has been collected.

Meeting the needs of security roles

Azure Sentinel offers tools for all members of your security team. For example, security operations professionals can get alerts, investigate incidents and remediate using automated tools. Security analysts and researchers employ its easy-to-learn query language for proactive threat hunting. Decision makers instantly view data across the enterprise using interactive dashboards. Each toolset saves time and helps people contribute maximum value in their roles.

02 /

Getting started with Azure Sentinel





Step 1

Access Azure Sentinel

Azure Sentinel is built on the Azure platform. It provides a fully integrated experience in the Azure portal to augment other Azure services, such as Azure Security Centre and Azure Machine Learning. If you don't already have one, the first step is to create an Azure free account. (Please refer to the pricing page to learn about total costs for Azure Sentinel.)

Once you have an Azure account, simply search for Azure Sentinel in the Azure portal and click **+Add** to add it to your portal.

Note you will also need the following:

- A Log Analytics workspace. Learn how to create a Log Analytics workspace.
- Contributor permissions to the subscription in which the Azure Sentinel workspace resides.
- Contributor or reader permissions on the resource group that the workspace belongs to.
- Additional permissions may be needed to connect specific data sources. Data ingestion pricing may differ among services. For more information, see the Azure Sentinel pricing page.

10

Step 2

Connect your data

Azure Sentinel includes connectors providing real-time integration with many industry solutions. It enables easy connections to a variety of Microsoft services, such as Office 365, Azure Active Directory, Azure Advanced Threat Protection and Microsoft Cloud App Security. You can also collect data from existing security solutions such as firewalls, routers, endpoint security and many more using built-in connectors. Plus, you can use Common Event Format (CEF), Syslog or REST-API to connect any compliant data source to Azure Sentinel.

To connect to a data source:

- 1. Sign in to Azure with account credentials. Navigate to Azure Sentinel.
- 2. Click Data connectors.
- 3. Click the row for the data source you wish to connect.
- 4. Click the **Open connector** page to see the configuration steps for connecting the data source.

After your data sources are connected, your data starts streaming into Azure Sentinel and is ready for you to use. For information about data connectors, see **Connect Data Sources**.

Microsoft Azure	, Search resources, services, and docs (G+/)		5 6 0 % ? ©	Alexw@seccrp.ninja
>> Dashboard > Azure Sentinel work	paces > Azure Sentinel - Data connectors			CONTOJO COM VIJ
+ Azure Sentinel - Da	a connectors			>
C Search (Ctrl+/)	" C Refresh			
General				
·	- III 25 If a A 2 Connectors Connected Coming soon			
E Logs	connected connected			
(A) Threat management			Azure Active Directory	
Incidents	Search by name or provider ROVIDERS : All DATATYPES : All		Azure Active Directory	
🔐 🏓 Dashboards	STATUS 👘 CONNECTOR NAME	•	Connected Microsoft	3 20 minutes age LAST LOG RECEIVED
O Hunting Instebooks	Amazon Web Services	Last log received: 09/04/19 04:42 PM	-	0010010010
Notebooks	Amazon	case fog received, opport to other thin	DESCRIPTION	
Configuration	Azure Active Directory	Last log received: 09/04/19 04:43 PM	Gain insights into Azure Active Directory by connect Azure Sentinel to gather insights around Azure Activ	e Directory scenarios. You can
News & guides Data connectors			learn about app usage, conditional access policies, le our Sign-in logs. You can get information on your St	
Analytics	Azure Active Directory Identity Protection Microsoft	Last log received: 09/03/19 05:57 AM	Directory Management activities like user, group, rol Audit logs table.	e, app management using our
R Playbooks	Azure Activity (Preview)			
Community	Microsoft	Last log received: 09/04/19 04:21 PM	LAST DATA RECEIVED 09/04/19 04:43 PM	
Workspace settings	Azure Advanced Threat Protection	Last log received: 08/28/19 08:30 AM		
			RELATED CONTENT	
	Azure Information Protection (Preview) Microsoft		2 2 Dashboards Queries	
	a Azure Security Center (Preview)			
	Microsoft	Last log received: 09/04/19 08:44 AM	DATA RECEIVED	Go to log analytics SIGNINLOGS
	Barracuda Web Application Firewall	-	500	AUDITLOGS
	Barracuda		400	
	Check Point CheckPoint		Open connector page	

Click the row for the data source you wish to connect.

Micro	soft Azure			D Search resources, services, and dors (6+)/	ninja 🦨
* +	Dashboard > Azure ! Azure Active Di PREVIEW		Sentinel - Data connectors > A		
• •	🚸 Azure Ad	tive Directory		Instructions Next Steps	
:- * - ©	Connected STATUS		6 minutes ago	Prerequisites To integrate with Azure Active Directory make sure you have:	
 <	Azure Sentinel to gather learn about app usage, o our Sign-in logs. You car	Active Directory by connecting A insights around Azure Active Di conditional access policies, legacy or get information on your SSPR of ctivities like user, group, role, ap	irectory scenarios. You can y auth relate details using usage, Azure Active	 Workspace: read and write permission: are required. Disgonotic Settings: required read and write permissions to AAD disgonotic settings. Resource provider registration: your subscription '44-64ffs-1fcb-4a22-a7d6-992ac7286382' needs to be registered to resource provider 'Microsoft.Insights'. Tenant Permissions: required 'Global Admin' or Security Admin' on the workspace's tenant. Leave: required AD P1/P2. 	
	RELATED CONTENT 2 (··) 2 Dashboards Queri			Configuration Connect Azure Active Directory logs to Azure Sentinel Select Azure Active Directory log types:	
	DATA RECEIVED 500 500 500 500 500 500 500 50	11 August 18 August 23 Total data noted	Go to log analytics	Azure Active Directory Audit logs Ho perministens	

After you have clicked **Open connector**, you will see the configuration steps for connecting the data source you selected.

12

Step 3

Use overview dashboard and workbooks to get visibility across enterprise

You can use Workbooks to view data, or create a new dashboard, either from scratch or based on an existing one. These are based on Azure Monitor Workbooks which enable rich, interactive reports for the data you have collected.

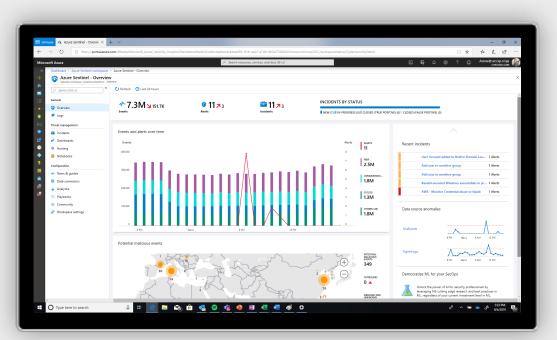
Overview dashboard

Start with the **Overview** dashboard, which provides insight at a glance into the security status of your workspace:

- Events and alerts over time: View the number of events and how many alerts were created from those events.
- **Potential malicious events:** Receive alerts when traffic is detected from sources that are known to be malicious.
- **Recent incidents:** View your most recent incidents, their severity and the number of alerts associated with each incident.
- Data source anomalies: Use models created by Microsoft's data analysts to search your data sources for anomalies.

Cloud-Native SIEM: Quick-Start Guide to September **Azure Sentinel**

13



2019

The **Overview** dashboard provides insight into the security status of your workspace.

Use built-in Workbook templates to get interactive dashboards for specific data sources

For additional visibility on specific data sources, you can use built-in templates. These Workbooks provide contextual insights for the data collected and analysed from specific sources, including information on data collected from Office 365. Azure Active Directory, Palo Alto Networks, Symantec, AWS and many other sources.

In the Azure Sentinel menu under Threat management select Workbooks.

1. You can see the built-in dashboard templates under the Templates tab.

Click the row for the template source you wish to view, make sure you have the relevant data types and click View workbook to see the template.

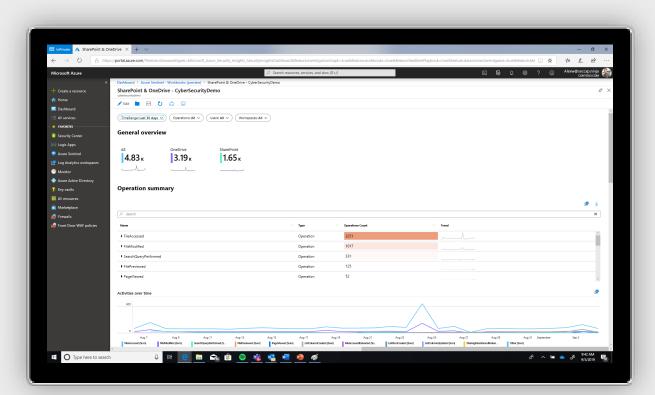
If you're using Azure AD, we recommend that you view the following dashboards:

- Azure AD sign-ins analyses sign-ins • over time to see if there are anomalies.
- Azure AD audit logs analyses admin • activities, such as changes in users, group creation and modifications.
- 2. Under the **My workbooks** tab, you will be able to see the workbooks that you have saved or created.

14

Azure Sentinel - Wor Selected workspace: "CyberSecurityDer	kbooks (preview)			×
,O Search (Ctrl+/)	Refresh + Add workbook Add workbook			
General	Installing. updating and deletin	ng workbooks require Contributor permi	ssions on the workspace's resource group	
 Overview Logs 	** 14 Saved workbooks	+ 19 Templates	Dupdates	
Threat management	My workbooks Templates			Azure AD Sign-in logs
Workbooks (preview)	Search workbooks			MICROSOFT
Dashboards Hunting Notebooks	Azure Activity MICROSOFT			Gain insights into Azure Active Directory by connecting Azure Sentinel
Configuration				and using the sign-in logs to gather insights around Azure AD scenarios. You can learn about sign-in operations, such as user sign-ins and
News & guides Data connectors	Azure AD Audi MICROSOFT	it logs		 locations, email addresses, and IP addresses of your users, as well as failed activities and the errors that triggered the failures.
Analytics				 Required data types: SigninLogs
A Playbooks	Azure AD Sign	i-in logs		Data sources: 0 AsureActiveDirectory
Workspace settings	Azure Firewall			
	DNS MICROSOFT			
	Exchange Onli MICROSOFT	ine		•• •
	FortiGate			

My workbooks houses the workbooks you have saved or created.



Each workbook provides contextual insights for data collected and analysed from specific sources.

Get custom views and insights across different data sources

Customise an existing workbook template:

- 1. Click the row for the template source you wish to edit, then click **Save**.
- 2. Select a location where you want to save this workbook. This saves the workbook template and not the data.
- 3. Click View workbook.
- 4. Click Edit.

Create a new workbook to get a customised dashboard:

- 1. Click **+Add Workbook** to create a new workbook.
- 2. Save the workbook using the save button; make sure to save it under your Azure Sentinel Subscription and Resource Group.
- 3. Edit the workbook using the **Edit** button. Make sure to save again after changing the workbook.

More information and guidelines on how to create visualisations in Azure Sentinel can be found in the 'Create interactive reports with Azure Monitor workbooks' documentation.

Azure Sentinel - V						- 0 ×
	://portal.azure.com/?feature.showassettype	-Microsoft_Azure_Security_Insights_	SecurityinsightsDashboard&deatu <i>P</i> Search resources, so	re.investigationGraph=true&feature.workbooks=true	8:feature.RealtimePlaybook = true8:feature.dataco	nnectorendgame=true&deatureMd 🗌 🚖 🖆 🦾 🛍 … 🖂 🕼 🗘 🚳 ? 💿 Alexw®seccep.ninja 👰
Microsoft Azure	Dashboard > Azure Sentinel - Workbook	fam. (a. A)P Search resources, se	trincei, end doci (u+/)		
+ Create a resource	Azure Sentinel - Workbo	oks (preview)				×
fr Home	Selected voriapace: "SyberSecurityDemo" - Pl	Drtw				
Dashboard	,0 Search (Chri+/)					
IE All services	General	Installing, updating and deleting	g workbooks require Contributor perm	issions on the workspace's resource group		
* FAVORITES	Overview	* 13	1 7	A 0		
Security Center	单 Loga	Saved workbooks	Templates	Updates		
A Logic Apps	Threat management					_
Log Analytics workspaces	 Incidents Workbooks (preview) 	My workbooks Templates				Azure Activity
Monitor	 Dashboards 	,₽ Search workbooks				
Azure Active Directory	Hunting	Azure Activity			â	
💡 Key vaults	Notebooks	MICROSOFT				Gain extensive insight into your organization's Azure Activity by analyzing, and correlating all user operations and events.
III All resources	Configuration					You can learn about all user operations, trends, and anomalous changes over time.nThis dashboard gives you the ability to drill down into caller
a Marketplace	📣 News & guides	Azure AD Audit	t logs			activities and summarize detected failure and warning events.
💼 Firewals	Data connectors	MICROSOFT				Required data types: 0
🙀 Front Door WAF policies	🖕 Analytics					AzureActivity
	(A) Playbooks	CheckPoint				Data sources: 0
	Community	_				AzureActivity
	🥏 Workspace settings	FortiGate				
		MICROSOFT				and the second s
						NI AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
		Identity & Acce	55			
		MICROSOFT				
						And a second sec
		Linux machines				
		Microsoft Clou	d days for such a			View Workbook Delete
	8 🖽 (Microsoft Clou) <i>®</i> j	~	ин өнс өтсере Фа 🥌 🖝 ^ Яд

To customise an existing template, click the row for the template source you wish to edit, then click **Save**.

16

Step 4

Detect threats

After you connect data sources to Azure Sentinel, the next step is to identify suspicious activities and threats. Azure Sentinel provides built-in templates to enable you to do this and get notified of such threats. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors and suspicious activity escalation chains. After you enable these templates, they will automatically search for suspicious activity across your environment. Many of them can be customised to search for, or filter out, activities according to your needs. To enable out-of-the-box detections, go to Rule templates.

	🗄 shines 🔥 Azara Sentinel-Analyli X + V						- 0
← → O A http Microsoft Azure	s://portal.azure.com/?leature.showassettypes=h	dicrosoft_Azure_Security_Insights_SecurityIn	A Search resources, services,		re.RealtimePlaybook - true&feature.da	itaconnectorendgame=true&deature.k	2 🔿 New@seccep.ninja 🖉
	Dashboard > Azure Sentinel - Analytics						CONTOSOLCOM
	Azure Sentinel - Analytics						
		+ Create C Refresh					
Dashboard	,O Search (Chri+/)	T Create O Merresh					
	General	🖕 41 📲	LES BY SEVERITY				LEARN MORE
- 🖈 FAVORITES	📀 Overview		IGH (6) MEDIUM (22)	LOW (9) INFORMATIONAL (4)			About Analytic Rules 12
Security Center	单 Logs						
	Threat management	Active rules Rule templates				Known Phospho	rus group domains
Azure Sentinel	Incidents						
	Workbooks (preview)	,0 Search	X SEVERITY : A	TTYPE : All TACTICS : All		High	Scheduled DETECTION TYPE
Monitor	ne Dashboards						
Azure Active Directory	Hunting	NAME	RULE TYPE	REQUIRED DATA SOURCES	TACTICS	DESCRIPTION	- A
😯 Key vaults	Notebooks	Known Phosphorus group domains	© Scheduled	DNS (Preview) +2 0	Command and Control	Matches domain name IOCs related CommonSecurityLog, DrstVents and	VMConnection dataTypes.
All resources	Configuration	Create incidents based on Azure Active I	Directo 🖪 Microsoft Security			References: https://blogs.microsoft.o protect-customers-from-hacking/.	com/on-the-issues/2019/03/27/new-steps-to-
Frewals	📣 News & guides	Advanced Multistage Attack Detection	Fusion		c) 🚓 👳 🧯		
Front Door WAF policies	Data connectors	Create incidents based on Azure Securit	Cente Microsoft Security			SEARCH QUERY	
	🖕 Analytics	Create incidents based on Microsoft Clo	ud App., I Microsoft Security			(union isfuzzy=true	<pre>smic(["yshoo-verification.org","s</pre>
	(A) Playbooks	Known Strontium group domains	© Scheduled	ONS (Preview) +2.0	Command and Control		<pre>where TimeGenerated >= ago(1d) meGenerated >= ago(1d) extend 5</pre>
	Community	Create incidents based on Azure Advance					TimeGenerated >= ago(1d) parse
	🥏 Workspace settings	-		Azure Active	© 4 ±	Mart Interapty (or	, , , , , , , , , , , , , , , , , , ,
		Suspect Application Consent	© Scheduled		0.00 0	REQUIRED DATA SOURCES	
		Now Ti map IP entity to AzureActivity	Scheduled	Threat Intellig+1 0		DNS (Preview) OnsEvents	
		Ti map URL entity to PaloAlto dat		Palo Alto Net +1 0			
		NEW SharePointFileOperation via devi		Office 365	🕎 Exfiltration	VMConnection	
		Process execution frequency anomaly	Scheduled	Security Events	Execution	Cisco ASA	
		Office Policy Tampering	© Scheduled	Office 365	¢ '8		
		Nov TI map File entity to Syslog Event	Scheduled	Syslog +1 0		You haven't used this template to You can use this template to	
		Anomalous sign-in location by user acco	runt an C Scheduled	Azure Active	🖳 Initial Access		
		Now Ti map Domain entity to PaloAlto	Scheduled	Palo Alto Net., +1 0		Create rule	

Find out-of-the-box detection templates created by Microsoft's team of security experts and analysts in **Rule templates**.

17

You can also create custom analytic rules tailored to your data and environment:

- 1. In the Azure portal under Azure Sentinel, select **Analytics**.
- 2. In the top menu bar, click +Add analytic rule and select **Custom rule**.
- 3. In the **General** tab, provide a descriptive name and a description. Set the Alert severity as necessary. When you create the rule you can enable it, which will cause it to run immediately. Alternatively, you can create it as disabled, in which case the rule will be added to your Active rules tab and you can enable it from there when you need it.
- 4. In the **Settings** tab, you can either write a query directly, or create the query in Log Analytics, and then paste it into the Search query field. As you change and configure your query, Azure Sentinel simulates the query results in the results preview window on the right. This enables you to understand how much data will be generated over a specific interval for the alert you created. This will depend on how you set up the Run query and Lookup data. If you see that your alert will be triggered too frequently, you can set the number of results higher so that it's above your average baseline.

»	Home > Azure Sentinel workspaces > Azure Sentinel - Analytics > Rule creation wizard
+	Rule creation wizard
	General Set rule logic Automate responses Review and create
:≡ ★	Create an analytic rule that will run on your data to detect threats.
0	Analytic rule details
ř	* Name
3	Description
4	
2	Tactics 0 selected V
	Severity Medium
\Leftrightarrow	Status Enabled Disabled
•	
۲	
۰	
٥	
0	
2	
	Next : Set rule logic >

Rule creation wizard allows you to create custom analytic rules.

18

5. Under Query scheduling:

Set the **Run** query every field to set the **Frequency** for how often the query is run – as frequently as every five minutes or as infrequently as once a day.

Set the **Lookup data** from the last field to control the time window for how much data the query runs on. For example, it can run every hour across 60 minutes of data.

You can set Azure Sentinel to **Stop** running the query after an alert is generated if you only want to get an alert once after it occurs. You must set the amount of time to stop running the query, up to 24 hours.

6. Under Entity mapping, you can map the columns in your query to entity fields recognised by Azure Sentinel. For each field, map the relevant column in the query you created in Log Analytics to the appropriate entity field. Each entity includes multiple fields, for example SID, GUID, etc. You can map the entity according to any of the fields, not just the upper-level entity.

- 7. In the Response automation tab, select any playbooks you want to run automatically when an alert is generated by the custom rule. For more information on creating and automating playbooks, see the section 'Respond to threats'.
- 8. Click **Review** to check the settings for your new alert rule, and then click Create to initialise it. After the alert is created, a custom rule is added to the table under Active analytic rules. There, you can also see the number of matches for each rule – the alerts triggered. From this list you can enable, disable or delete each rule. You can also right-select the ellipsis (...) at the end of the row for each alert to edit, disable, clone, show matches or delete a rule. The Analytics page is a gallery of all your active alert rules, including templates you enable and alert rules you create based on templates.
- To view the results of the alert rules you create, go to the Incidents page, where you can triage, investigate incidents and remediate the threats.

19

Step 5

Investigate incidents

An incident is an aggregation of all the relevant evidence for a specific investigation. Incidents are created based on alerts you have defined in the **Analytics** page. The properties related to the alerts, such as severity and status, are set at the incident level. Now you can easily investigate the detected threats and the entire incident. You can quickly view the status of each incidents and manage the full life cycle of this event.

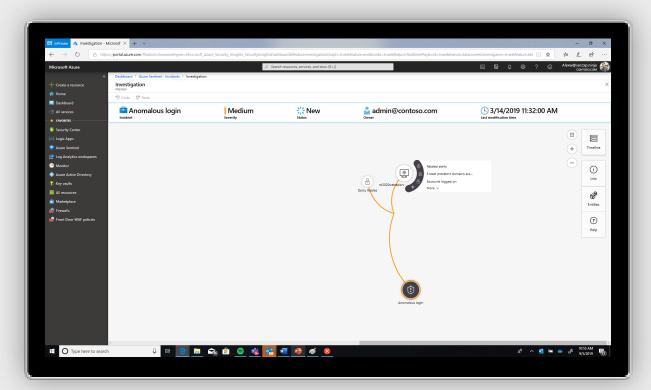
← → C) A https://portal.azure.	m/?feature chrwascettunes-Mirrosoft Ans	a Security Insights SecurityInsight	s Dashboard&faatura inv	ectinationGranh-true&featur	a workhooks-true8r	faatura RaaltimaDladvork-true&faatu	re.dataconnectorendgame=true&feature.Md 🛄 🛧 🚖 💪 🖉
← → Ů A https://portal.azure./	ni reaarchonabergper-meteorieta		Search resources, services			laaren annen 1900 van de er de e	
« Deshboard	Azure Sentinel - Incidents						- 0111030-0000
Selecte	e Sentinel - Incidents workspace: "CyberSecurityDemo" - PREVIEW						
A Home	tri+/) * C Refresh	Last 24 hours					
Dashboard General		missions on the workspace are require	d to modify incidents				
All services All services Service Service Service Service				~ -		Open Incidents By Severity	
Security Center Logs	S OPEN INCI		9				
A Logic Apps Threat manage		DENTS	VINCIDENTS	IN PROGRESS		CRITICAL (0) HIGH (1) MED	DIUM (7) DIUM (0) INFORMATIONAL (1)
Azure Sentinel							🚔 Anomalous login
🔛 Log Analytics workspaces 🗧 Workbo	ks (preview)	v id or title	X SEVERITY :	Informational Low, Medium, I	igh, Critical	TATUS : New, In Progress	Incident Id: 96368
Monitor Dashboi	ds						Medium 💛 🔅 New 🗠 🎍 admin@cor
Azure Active Directory Hunting	INCIDENT	ID 14 TITLE	ALERTS	CREATED TIME	OWNER	STATUS	12 SEVENTY STATUS OWNER
😗 Key vaults 🧧 Notebo	96368	Anomalous login	1	03/14/19 11:32 AM	admin@contoso.co	m New	DESCRIPTION
All resources Configuration Marketplace	584	Add user to sensitive group	a 1	09/05/19 09:46 AM	Unassigned	New	
Grouplic		Base64 encoded Windows	executable 1	09/05/19 06:43 AM	Unassigned	New	TAGS
- Data co	582	AWS - Monitor Credential	abuse or hij 1	09/05/19 06:39 AM	Unassigned	New	+
Analytic	581	Traffic to known bad IPs	1	09/05/19 06:38 AM	Unassigned	New	LAST UPDATE TIME
Commu	580	Kerberos service ticket was	requested 1	09/05/19 06:38 AM	Unassigned	New	03/14/19 11/32 AM
P Worksp	570	Signins from IP's that atten	npted to si 1	09/05/19 06:38 AM	Unassigned	New	
	578	DNS tor proxies	1	09/05/19 06:38 AM	Unassigned	New	CREATION TIME 03/14/19 11:32 AM
	577	User Account Created and	Deleted wit 1	09/05/19 06:38 AM	Unassigned	New	
	576	Yaniv Demo	0	09/05/19 03:04 AM	tiandert@microsoft	Lcom New	CLOSE REASON
	-						
							EVIDENCE
							0 1 R 0 Events Alerts Bookmarks
							Events Alerts Bookmarks

See how many incidents you have, how many are open, how many you've set to In progress, and how many are closed in one view.

Investigating an incident using the Investigation Graph

- To begin an investigation, click on a specific incident. On the right, you can see detailed information for the incident including its severity and a summary of the number of entities involved (based on your mapping). Each incident has a unique ID. The severity of the incident is determined according to the most severe alert included in the incident.
- To view more details about the alerts and entities in the incident, click on View full details on the incident page and review the relevant tabs that summarise the incident information. Full incident view consolidates all evidence in the alert, the associated alerts and entities.
- 3. In the Alerts tab, review the alert itself when it was triggered and by how much it exceeded the thresholds you set. You can see all relevant information about the alert the query that triggered the alert, the number of results returned per query and the ability to run playbooks on the alerts. To drill down even further into the incident, click on the number of events. This opens the query that generated the results and the results that triggered the alert in Log Analytics.
- 4. In the **Entities** tab, you can see all the entities that you mapped as part of the alert rule definition.
- If you're actively investigating an incident, it's a good idea to set the incident status to **In progress** until you close it.
- 6. Incidents can be assigned to a specific user. For each incident you can assign an owner by setting the incident owner field. All incidents start as unassigned. You can go into the incidents and filter by your name to see all the incidents that you own. You can also add comments so that other administrators will be able to understand what you investigated and what your concerns are around the incident.

21



2019

The investigation graph uses raw data to illustrate connections.

7. Click **Investigate** to view the investigation graph tool. The investigation graph helps you understand the scope and identify the root cause of a potential security threat by correlating relevant data with any involved entity. Azure Sentinel analyses your raw data to find additional

insights and connections on the entities extracted from your alerts. It will then surface those connections in the live investigation graph. You can dive deeper and investigate any entity presented in the graph by clicking on it and choosing between different expansion options.

- 8. Select each entity to open the **Entities** pane so you can review each entity.
- 9. Expand your investigation by hovering over each entity to reveal a list of questions that was designed by our security experts and analysts per entity type to deepen your investigation. For example, on a computer you can request related alerts. The related alerts are added to the graph. For each entity, you

can select the option to open the results in Log Analytics to see the raw data for the incidents. The graph provides you with a list of connections that you might not have known about, enabling you to reach full scope of the breach. It also gives you a timeline parallel to the graph. You can hover over the timeline to see which things on the graph occurred at what point in time.

Microsoft Azure		و حر	earch resources, services, and docs (G+/)		E 6 0 @ ? © ^	Vexw@seccxp.ninja соктово.com
«	Dashboard > Azure Sentinel - Incidents > Investiga	ion				
+ Create a resource	Investigation PREVIEW					
A Home	🍤 Undo 🔍 Redo					
Dashboard E All services	🖻 Anomalous login	Medium	🔆 New	🄓 admin@contoso.com	(L) 3/14/2019 11:32:00 AM	
	Incident	Severity	Status	Owner	Last modification time	
Security Center						
(참) Logic Apps					Darcy Robles	
Azure Sentinel		11.12.66.60		+		Timeline
🔛 Log Analytics workspaces		Q			FRIENDLYNAME	
Monitor		No.		-	Darcy Robles	0
Azure Active Directory					CONNECTED ALERTS 4	Info
👔 Key vaults			-		NAME	
All resources Marketplace			0 0		Darcy Robles	68
Firewalls		Shir cover	how we append		DISPLAYNAME Darcy Robles	Entities
Front Door WAF policies			\rightarrow		UPINSUFFIX	?
			7		contoso.com	Help
					SID S-1-5-21-917267712-1342860078-1792151419-500	Thep
					AADUSERID	
					994f97fe-644b-4bda-af55-a3ba8eba1227	
					LOGONID 0xb390b	
			Eury Robes		0803900	
			\sim			
			7			
			\ \			

Dive deeper into the data to investigate the full scope of a breach.

Step 6

Respond to threats

A security playbook is a collection of procedures that orchestrates a threat response. Playbooks can run manually or automatically. Security playbooks in Azure Sentinel are based on Azure Logic Apps, providing built-in templates you can customise. Note that Azure Logic Apps incur charges. View the pricing page for more details.

For example, if you're worried about malicious attackers accessing your network resources, you can set an alert that looks for malicious IP addresses accessing your network and trigger a playbook to stop the attack in real time.

Create a security playbook

- 1. Open the Azure Sentinel dashboard.
- 2. Under Management, select Playbooks.
- 3. In the Azure Sentinel Playbooks (Preview) page, click Add button.
- 4. In the **Create Logic app** page, type the requested information to create your new logic app, then click **Create**.
- 5. In the Logic App Designer, select the template you want to use. If you select a template that necessitates credentials, you will have to provide them. Alternatively, you can create a new blank playbook from scratch. Select Blank Logic App.

 From here you can either build a new playbook or edit the template. Learn more about creating a playbook with Logic Apps.

Automate threat responses

Using real-time automation, response teams can significantly reduce their workload by fully automating routine responses to recurring types of alerts. Note that this requires setting the playbook trigger to **Azure Sentinel**.

- Choose the alert for which you want to automate the response.
- 2. From the Azure Sentinel workspace navigation menu, select **Analytics**.
- 3. Select the alert you want to automate.
- In the Edit alert rule page, under the Automate responses tab, choose the Triggered playbook you want to run when this alert rule is matched.
- 5. Select Next: Review.

	,P. Search resources, services, and docs (0+,/)		🗉 🛱 0 🐵 ? 😄 hitytämionsottoon 🙍
* Home > Aque Section + Arabitics > Rule creation vicand	> another product the rest for the		
Rule creation wizard			,
General Set rule logic Automate responses Review and create			
E Select a playbook to be run automatically when your analytic rule generates an alert.			
NAME (1)	5 59798	1 TRIGODI KIND	
(i) Life is show light	O Enabled	 Azure Sentinel 	
A Approval-tenal	O Enabled	Azure Sectionel	
A BlockUpAppUser,ShawPointList	O Enabled	Acure Sertinel	
(A) Get-Geofronip	O Enabled O Enabled	Azure Sentinel Azure Sentinel	
A Prompt-User		Adure Sertinel Adure Sertinel	
Get-Userhänager Ki istrev	O brabled O brabled	Adult Service Adult Service	
[A] Served [A] Variabilitation	O Evaluation	Appre Section	
A det deo FromiP	0 Enabled	Acute Section	
A Verify Update-existing-incident	O Crabled	Q Aput Section	
Approximity BiokUnAppUnit	O Brubled	 Azure Sentinel 	
A Prompt-Over	O Enabled	9 Apure Sectione	
A BlockApp	O trabled	Q Azure Sertinel	
A BlockP_User_Securit	O Enabled	Azure Sertinel	
A Bookuser	O Enabled	Azure Sentinel	
A ChangeUserPassword	O trubled	Azure Sertinel	
A tecontriguous, Sendimat	O tradied	Azure Serticel	
A destruío	O Enabled	Azure Sectionel	
[A] GetURDeputation	O Enabled	Azure Sectionel	
∆ isolateMachine	O trabled	Azure Sertinel	
A Merilybook	O Enabled	Q Azura Sertinal	
A Openmident, ServiceNow	O Enabled	Azure Sectionel	
(A) OpenTicektika	O brabled	Azure Sertinel	
A PostMessaprTeams	O Enabled	Carlos Sertinel	
A seatinal	O Enabled	Azure Sectional	
A ShutdowMachine	© brabled	Azure Sentinel	
A BlockP-PNW-AAD,SNOW	O Enabled	Azure Sectionel	
111 Marchan Marchana Association	A Paralited	A to conficient	

Reduce team workloads by automating routine responses to recurring types of alerts.

Step 7

Hunt for threats

Analysts need to proactively look for threats that may not have been discovered by security apps. Azure Sentinel includes built-in hunting queries that guide you to ask the right questions to find previously undiscovered threats.

With Azure Sentinel hunting, you can take advantage of the following capabilities:

- Built-in queries: A starting page provides preloaded query examples designed to get you started quickly and familiarise you with the tables and the query language. These built-in hunting queries are developed and fine-tuned by Microsoft security researchers and the GitHub community on a continuous basis to provide you with an entry point and help you start hunting for the beginnings of new attacks.
- Powerful query language with IntelliSense: Built on top of a query language, this gives you the flexibility you need to take hunting to the next level.
- Create your own bookmarks: Bookmarks let you save items for later so you can use them to create an incident for investigation. You can bookmark a row, promote it to an incident and then investigate with an investigation graph.

- Use notebooks to automate investigation: Notebooks encapsulate all the hunting steps in a reusable playbook that can be shared with others in your organisation.
- Query the stored data: The data is accessible in tables for you to query. For example, you can query process creation, DNS events and many other event types.
- Links to community: Leverage the power of the greater community to find additional queries and data sources.



Azure Sentinel's built-in hunting queries guide you into asking the right questions to find issues in the data you already have on your network. 27

September Cloud-Native SIEM: Quick-Start Guide to **Azure Sentinel**

Try Azure **Sentinel today**

No infrastructure investment. Powerful AI built in. Tools for every role. Virtually unlimited scalability. All backed by Microsoft security research. If you're looking to improve the security posture of your enterprise while simplifying security operations, consider Azure Sentinel.

See how fast, easy and inexpensive it is to get started.



2019

Talk to an Azure Specialist about Azure Sentinel now

 $\ensuremath{\mathbb{C}}$ 2019 Microsoft Corporation. All rights reserved. This document is provided 'as is'. Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

28