

#POWERCON2023

Microsoft Sentinel: Parola D'ordine
Automazione!

Guido Imperatore

*Microsoft Solution Specialist @ WeAreProject
guido.imperatore@project.it*



/guido.imperatore



@GuidoImpe



/guidoimperatore

Agenda

- Cosa è Microsoft Sentinel
- Cosa ci permette di fare Microsoft Sentinel
- Licensing
- Kusto Query (KQL)
- Automatizzare Incident con i Playbook

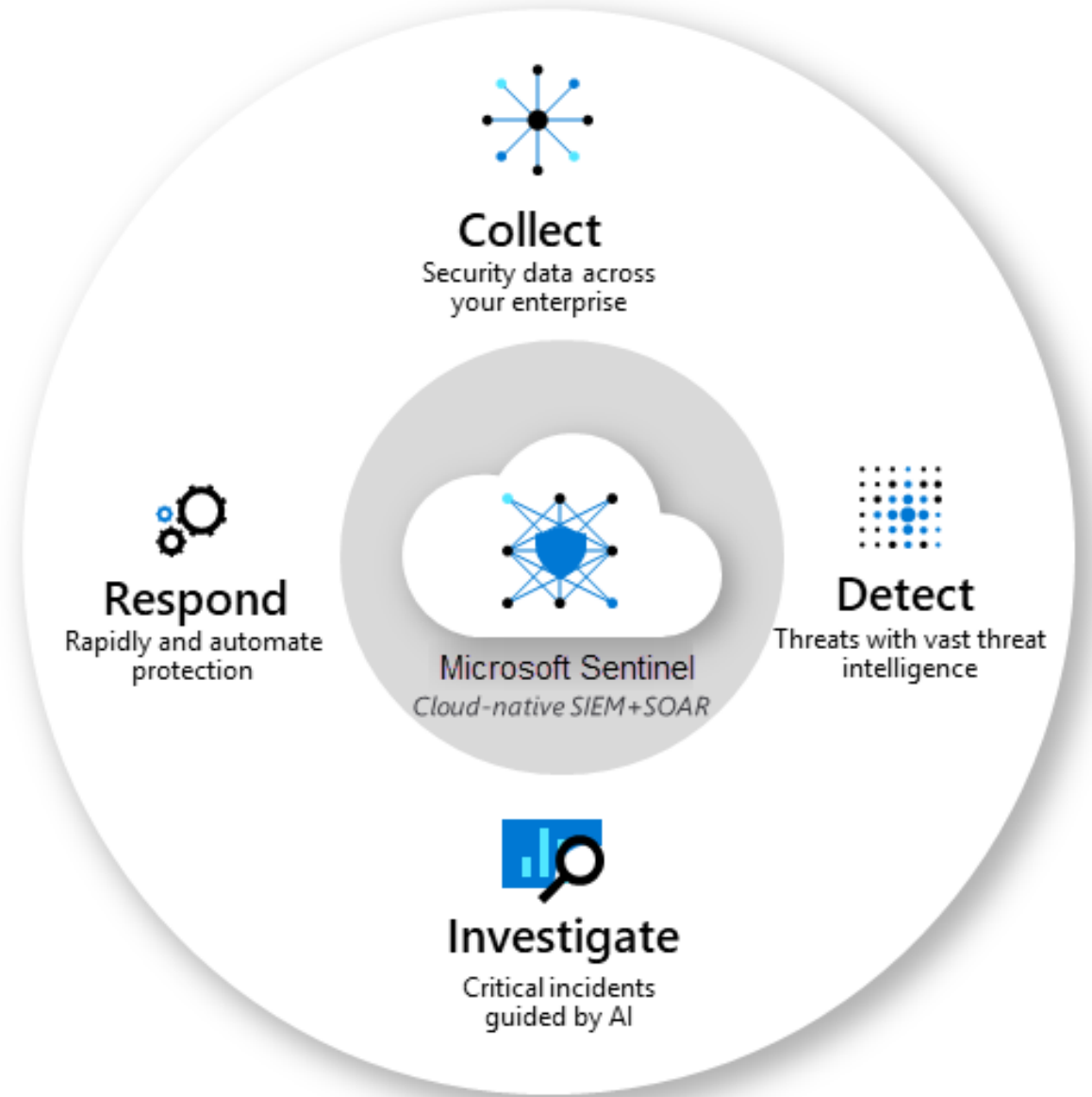
Cosa è Microsoft Sentinel ?



Microsoft Sentinel

- Soluzione Scalabile Cloud Based
- Gestisce Eventi di Sicurezza (SIEM)
- Automatizza Risposte ad Eventi (SOAR)
- Estende Data Retention dei Log

Schema Microsoft Sentinel



Log Collection

- Origini Microsoft
- Origini Azure
- Connettori Terze Parti
- Syslog

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Data connectors

Selected workspace: 'contoso-sentinel-workspace'

Search

Refresh Guides & Feedback

137 Connectors 12 Connected

More content at Content hub

Search by name or provider Providers: All Data Types: All Status: All

Status	Connector name ↑
Connected	Azure Active Directory Microsoft
Connected	Azure Active Directory Identity Protection Microsoft
Connected	Azure Activity Microsoft
Connected	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](#)

Data Connector

Azure Active Directory ...


 Azure Active Directory

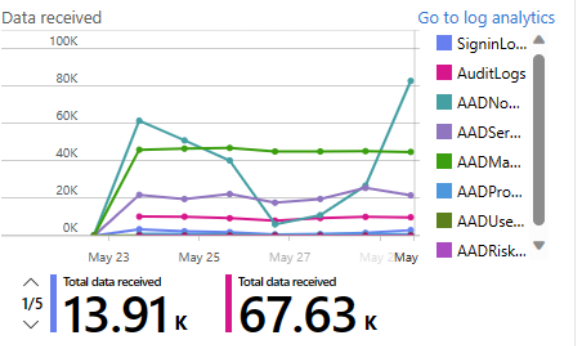
Connected Status  Microsoft Provider  5 minutes ago Last Log Received













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 management using our Audit logs table.

Last data received ⓘ
05/30/23, 04:09 PM

Related content

-  9 Workbooks
-  2 Queries
-  110 Analytics rules templates



- Data types**
-  SigninLogs 05/30/23, 04:09 PM
 -  AuditLogs 05/30/23, 04:08 PM
 -  AADNonInteractiveUserSignInLogs 05/30/23, 04:09 PM
 -  AADServicePrincipalSignInLogs 05/30/23, 04:09 PM
 -  AADManagedIdentitySignInLogs 05/30/23, 04:09 PM
 -  AADProvisioningLogs 05/30/23, 04:08 PM
 -  ADFSsignInLogs --
 -  AADUserRiskEvents 05/30/23, 04:07 PM
 -  AADRiskyUsers 05/30/23, 02:39 PM
 -  NetworkAccessTraffic --
 -  AADRiskyServicePrincipals --
 -  AADServicePrincipalRiskEvents --

Instructions

Prerequisites


To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Diagnostic Settings:** read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel
Select Azure Active Directory log types:

Sign-In Logs

 In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a fr](#)

- Audit Logs
- Non-Interactive User Sign-In Log (Preview)
- Service Principal Sign-In Logs (Preview)
- Managed Identity Sign-In Logs (Preview)
- Provisioning Logs (Preview)
- ADFS Sign-In Logs (Preview)
- User Risk Events (Preview)
- Risky Users (Preview)
- Network Access Traffic Logs (Preview)
- Risky Service Principals (Preview)
- Service Principal Risk Events (Preview)

Apply Changes

Workbooks

- Visualizzazione Grafica Eventi
- Permette Analisi Approfondita Eventi
- Dati Eventi in Tabella o Grafico
- Possibilità di Eseguire KQL per la ricerca dei log

The screenshot shows the Microsoft Sentinel Workbooks interface. The top navigation bar includes a search box, a refresh button, an 'Add Workbook' button, and a 'Guides & Feedback' link. Below the navigation bar, there are three status indicators: 'My workbooks' (0), 'Templates' (22), and 'Updates' (0). A 'More content at Content hub' link is also present. The main content area is divided into two tabs: 'My workbooks' and 'Templates'. The 'My workbooks' tab is active, displaying a section titled 'Microsoft Sentinel Workbooks' with a 'What is it?' subsection. This section explains that workbooks provide instant visualization and analysis of data across connected sources, and offers links to learn more. Below this is a 'Getting started' section with a 'Featured workbooks' subsection, which includes a 'Get these workbooks' button. On the right side of the page, there is a 'More workbooks' section with a 'Go to content hub' button. The left sidebar contains a navigation menu with categories like 'General', 'Threat management', 'Content management', and 'Configuration', with 'Workbooks' currently selected.

Data Analytics Rule

- Identificazione Vulnerabilità
- Identificazione Attività Anomale
- Definire modalità di Generazione Eventi
- Definire modalità di Generazione Incident

The screenshot displays the Microsoft Sentinel Analytics interface. The top navigation bar includes a search box, a 'Create' button, and various action buttons like 'Refresh', 'Analytics workbooks', 'Enable', 'Disable', 'Delete', 'Import', 'Export', and 'Guides & Feedback'. The main content area shows 'Active rules' with a count of 1. Below this, there are tabs for 'Active rules', 'Rule templates', and 'Anomalies'. A search box for rules is present, followed by a table of active rules. The table has columns for Severity, Name, Rule type, Data sources, Tactics, Techniques, and Source name. The rules listed include various security alerts such as 'GitHub Signin B...', 'Cross-tenant Ac...', 'Malicious Inbox...', 'Authentication ...', 'SUNBURST and...', 'Threat Essential...', 'Failed logon att...', 'Attempts to sig...', 'Suspicious appl...', 'Threat Essential...', 'SUNBURST net...', 'Cross-tenant Ac...', 'AV detections r...', and 'Azure Active Dir...'. The severity levels range from Low to High. The bottom of the interface shows pagination controls: '< Previous', 'Page 1 of 3', 'Next >', and 'Showing 1 to 50 of 128 results'.

Severity	Name	Rule type	Data sources	Tactics	Techniques	Source name
Medium	GitHub Signin B...	Scheduled	Microsoft Entra...	Credentia	T1110	Azure Active Dir...
Medium	Cross-tenant Ac...	Scheduled	Microsoft Entra...	Initial Acce:	T1078 +2 ⊕	Azure Active Dir...
Medium	Malicious Inbox...	Scheduled	Microsoft 365 (...)	Persistence	T1098 +1 ⊕	Microsoft 365
High	Authentication ...	Scheduled	Microsoft Entra...	Persisten	T1098	Azure Active Dir...
High	SUNBURST and...	Scheduled	Microsoft 365 ...	Execution †	T1195 +2 ⊕	Microsoft 365 ...
Medium	Threat Essential...	Scheduled	Cisco ASA +2 ⊕	Exfiltratio	T1030	SecurityThreatE...
Medium	Failed logon att...	Scheduled	Syslog	Credentia	T1110	Syslog
Medium	Attempts to sig...	Scheduled	Microsoft Entra...	Initial Acc	T1078	Azure Active Dir...
Low	Suspicious appl...	Scheduled	Microsoft Entra...	Credentia	T1528	Azure Active Dir...
Medium	Threat Essential...	Scheduled	Microsoft 365 (...)	Collection	T1114 +1 ⊕	SecurityThreatE...
Medium	SUNBURST net...	Scheduled	Microsoft 365 ...	Execution †	T1195 +2 ⊕	Microsoft 365 ...
Medium	Cross-tenant Ac...	Scheduled	Microsoft Entra...	Initial Acce:	T1078 +2 ⊕	Azure Active Dir...
High	AV detections r...	Scheduled	Microsoft 365 ...	Persisten	T1053	Microsoft 365 ...
Low	Azure Active Dir...	Scheduled	Microsoft Entra...	Initial Acc	T1078	Azure Active Dir...

Playbook

- Assegnare Incident al personale SOC corretto
- Chiudere Incident (Falsi Positivi)
- Rispondere in Modo Automatizzato ad Incident Critici
- Basati su Logic App di Azure (generano costi aggiuntivi)

KQL (Kusto Query)

- Linguaggio per ricerca dei dati
- Ricerca in sola lettura
- Simile a SQLs (database, tabelle, colonne)
- Linguaggio case-sensitive

Struttura KQL

- Tabella di Riferimento (signinlogs)
- Parametri di ricerca (where)
- Raggruppamento dei «risultati» (Project)

```
1 SigninLogs
2 | where TimeGenerated > ago(3d)
3 | where UserPrincipalName == "guido@xxxxxxxxxxxxxx.com"
4 | where ResultType == 0
5 | project TimeGenerated, Location, IPAddress, UserAgent
```

Results Chart Add bookmark

<input type="checkbox"/>	TimeGenerated [Local Time] ↑↓	Location	IPAddress	UserAgent
<input type="checkbox"/>	07/11/2023, 08:32:17.808	IT	192.168.1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)...
	TimeGenerated [UTC]	2023-11-07T07:32:17.8089426Z		
	Location	IT		
	IPAddress	192.168.1.1		
	UserAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0		
<input type="checkbox"/>	> 07/11/2023, 08:31:19.784	IT	192.168.1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch...
<input type="checkbox"/>	> 07/11/2023, 08:30:53.411	IT	192.168.1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch...
<input type="checkbox"/>	> 07/11/2023, 07:45:48.554	IT	192.168.1.1	Windows-AzureAD-Authentication-Provider/1.0
<input type="checkbox"/>	> 06/11/2023, 18:54:26.085	IT	192.168.1.1	Mozilla/5.0 (iPhone; CPU iPhone OS 17_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML,...
<input type="checkbox"/>	> 06/11/2023, 18:37:12.871	IT	192.168.1.1	Mozilla/5.0 (iPhone; CPU iPhone OS 17_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML,...
<input type="checkbox"/>	> 06/11/2023, 16:30:49.556	IT	192.168.1.1	Windows-AzureAD-Authentication-Provider/1.0
<input type="checkbox"/>	> 06/11/2023, 12:07:21.615	IT	192.168.1.1	Windows-AzureAD-Authentication-Provider/1.0
<input type="checkbox"/>	> 06/11/2023, 09:09:06.310	IT	192.168.1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch...
<input type="checkbox"/>	> 06/11/2023, 09:08:15.108	IT	192.168.1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch...
<input type="checkbox"/>	> 06/11/2023, 09:07:04.170	IT	192.168.1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch...

```
SigninLogs
| where TimeGenerated > ago(3d)
| where UserPrincipalName == "guido@xxxxxxxxxxxxxx.com"
| where ResultType == 0
| project TimeGenerated, Location, IPAddress, UserAgent
```

User and Entity Behavior Analytics

- Analisi Comportamentale
- Correlazione dei Comportamenti Utente/Server
- Uso delle informazioni per rilevare anomalie/potenziati attacchi

The screenshot displays the Microsoft Sentinel 'Entity behavior' interface. The page title is 'Microsoft Sentinel | Entity behavior' with a sub-header 'Selected workspace: 'sentinelworkspace''. The navigation menu on the left includes sections for 'Threat management' (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview)), 'Content management' (Content hub, Repositories (Preview), Community), and 'Configuration'. The main content area features a search bar with the placeholder text 'Search for accounts, hosts, IP addresses, IoT devices or Azure resources'. Below the search bar, there are two charts: 'Accounts by # of alerts' and 'Hosts by # of alerts'. The 'Accounts by # of alerts' chart shows a table with the following data:

Account	# of alerts
Guido	38
Guido	15
Sentinel Service	1

The 'Hosts by # of alerts' chart displays a message: 'No data to display'.

Hunting

- Ricerca di tecniche MITRE
- Ricerche personalizzate per analizzare comportamenti dannosi
- Permette di creare regole analitiche in base ai risultati ottenuti
- Ricerca di vulnerabilità note

Microsoft Sentinel | MITRE ATT&CK (Preview) ...
Selected workspace: 'contoso-sentinel-workspace'

Search by technique ID, name

General	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Overview (Preview)	2 Active Scanning	0 Acquire Infrastructure	4 Drive-by Compromise	13 Command and Scripting...	28 Account Manipulation	1 Access Token Manipulation	0 Access Token Manipulation
Logs	0 Gather Victim Host...	0 Compromise Accounts	9 Exploit Public-Facing...	0 Container Administrati...	0 BITS Jobs	0 Boot or Logon Autostart...	0 BITS Jobs
News & guides	0 Gather Victim Identity...	0 Compromise Infrastructure	3 External Remote...	0 Deploy Container	0 Boot or Logon Autostart...	0 Boot or Logon Initialization...	0 Build Image on Host
Search	0 Gather Victim Network...	0 Develop Capabilities	0 Hardware Additions	5 Exploitation for Client...	3 Boot or Logon Initialization...	0 Create or Modify System...	0 Debugger Evasion
Threat management	0 Gather Victim Org...	0 Establish Accounts	1 Phishing	0 Inter-Process Communicati...	2 Browser Extensions	1 Domain Policy Modification	0 Deobfuscate/Decode Files...
Incidents	0 Phishing for Information	0 Obtain Capabilities	0 Replication Through...	0 Native API	0 Compromise Client...		
Workbooks							
Hunting							
Notebooks							
Entity behavior							
Threat intelligence							

Log4j Vulnerability Detection

Microsoft Provider | Microsoft Support | 2.0.4 Version

Workbooks: 2, Analytic Rules: 4, Hunting Queries: 10, Watchlists: 1, Playbooks: 2

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type

- 4 Analytics rule
- 10 Hunting query
- 2 Playbook
- 1 Watchlist
- 2 Workbook

Category

- Application, Security - Vulnerability

Pricing

Free

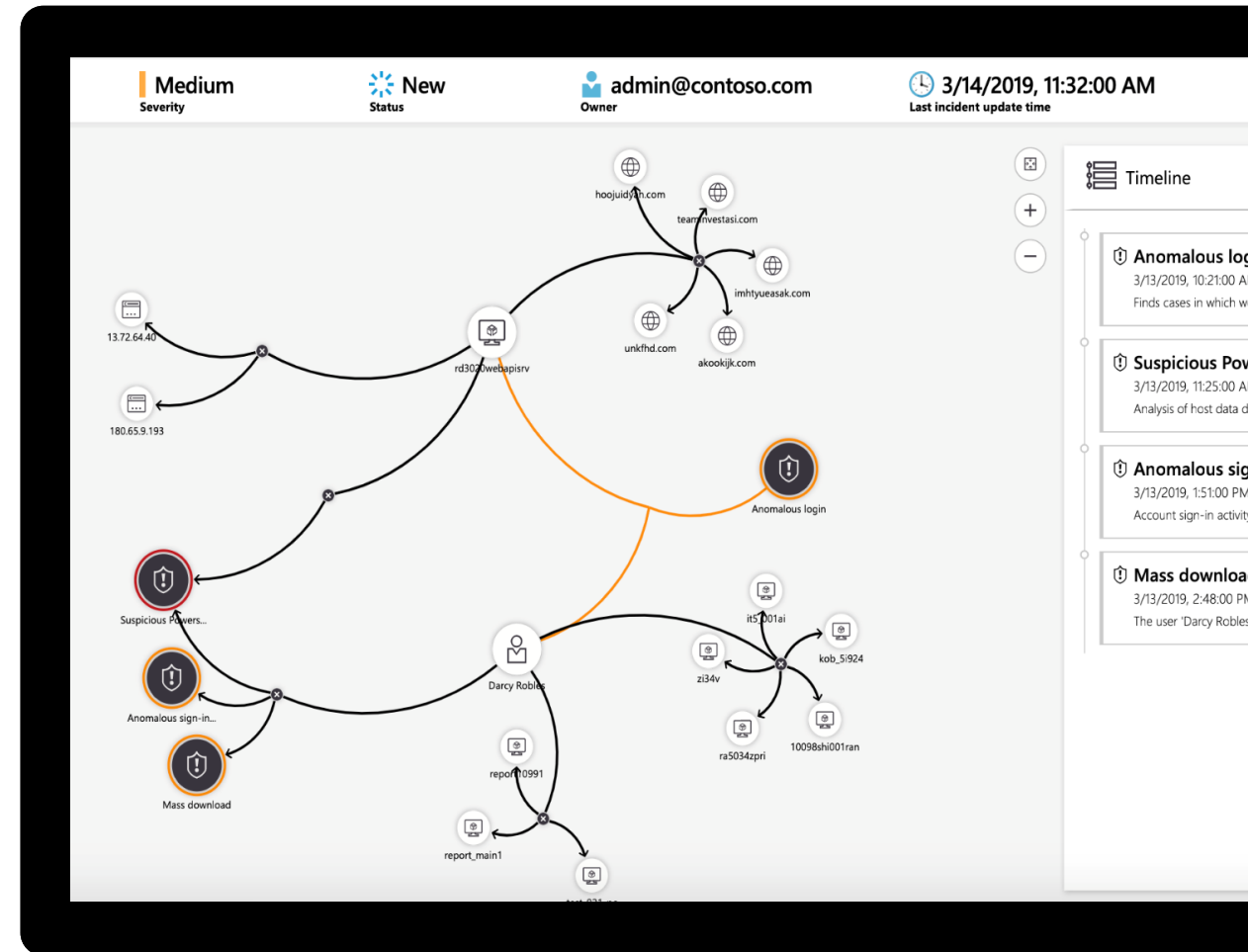
Manage | Actions | View details

- Create hunt (Preview)
- Add to existing hunt (Preview)
- Reinstall
- Delete

Visualizzazione Attacco per determinarne ambito e impatto

- Esplorare la correlazione tra gli "avvisi"
- Ricerca approfondita utilizzando query specifiche
- Ottenere informazioni approfondite sugli attori coinvolti

80% reduction in investigation effort compared to legacy SIEMs

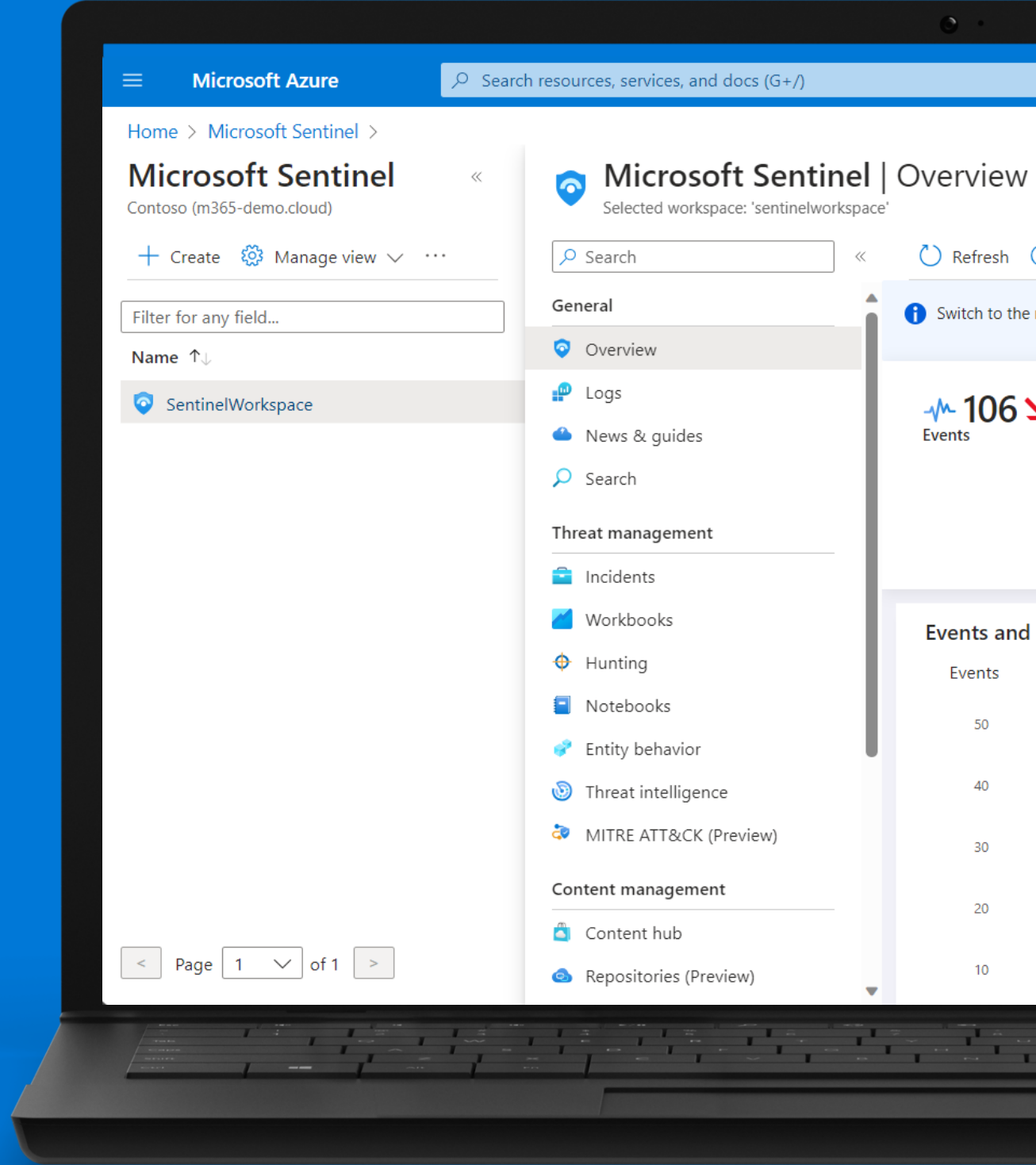


Licensing

Livello	Prezzo Microsoft Sentinel	Prezzo effettivo per GB ¹	Risparmi rispetto al pagamento in base al consumo
Pagamento in base al consumo	5,29 € per GB importati	5,29 € per GB importati	N/A
100 GB al giorno	€361.89 al giorno	3,62 € per GB	32%
200 GB al giorno	€669.94 al giorno	3,35 € per GB	37%
300 GB al giorno	€977.98 al giorno	3,26 € per GB	38%
400 GB al giorno	€1,268.07 al giorno	3,18 € per GB	40%
500 GB al giorno	€1,546.32 al giorno	3,10 € per GB	41%
1.000 GB al giorno	€3,031.48 al giorno	3,04 € per GB	43%
2.000 GB al giorno	€5,867.10 al giorno	2,94 € per GB	44%

DEMO

Microsoft Sentinel



Microsoft Sentinel | Incidents

Selected workspace: 'sentinelworkspace'

Search + Create incident (Preview) Refresh Last 24 hours Actions Delete Security efficiency workbook Columns Guides & Feedback

- General
 - Overview
 - Logs
 - News & guides
 - Search
- Threat management
 - Incidents
 - Workbooks
 - Hunting
 - Notebooks
 - Entity behavior
 - Threat intelligence
 - MITRE ATT&CK (Preview)
- Content management
 - Content hub
 - Repositories (Preview)
 - Community
- Configuration
 - Workspace manager (Preview)
 - Data connectors
 - Analytics
 - Watchlist
 - Automation
 - Settings

Open incidents: 0 New incidents: 0 Active incidents: 0

Open incidents by severity: High (0) Medium (0) Low (0) Informational (0)

Search by ID, title, tags, owner or product | Severity: All Status: 2 selected Product name: All Owner: All

Auto-refresh incidents

No incidents were found





What is it?

Microsoft Sentinel incidents are containers of threats in your organization – alerts, entities and any additional related evidence. An incident is created based on alerts that you have defined in the security analytics page. The properties related to the alerts, such as severity and status are set at the incident level.

How does it work?

Incidents are automatically created as a result of alerts triggered based on detections defined in 'Security analytics'. The incidents page provide a full view of all the context required for triage, investigation and response. For each incident, you can see the time it was generated and its status.

These are the types of activities you can perform with incidents

-  **View related alerts**
View all related alerts that are aggregated into an incident based on the alert trigger definition of the alert fusion strategy enabled. Review all details related to the alert in a unified location.
 -  **Triage and investigate**
Review all related entities in the incident and additional contextual information meaningful to the triage process. Investigate the alerts and related entities to understand the scope of breach.
-  Incident management  Respond to alerts in the incidents

Guide su Microsoft Sentinel – ICT Power

- [Configurare Microsoft Sentinel per ricevere Log da dispositivi On-Premises - ICT Power](#)
- [Creare Data Collection Rule con Azure ARC e Microsoft Sentinel per il monitoraggio dei sistemi operativi Windows on-premises - ICT Power](#)
- [Automatizzare le Remediations degli incidents in Microsoft Sentinel con i playbook - ICT Power](#)

Grazie

Guido Imperatore

Microsoft Solution Specialist @ WeAreProject

Guido.imperatore@project.it



/guido.imperatore



@GuidoImpe



/guidoimperatore