

Microsoft Sentinel

- Hannes Lagler-Gruener
- Cloud Architect @ ACP IT Solutions GmbH
- Twitter @HannesLagler
- MVP



Official sponsors



RECAST SOFTWARE

NORDIC

— VIRTUAL SUMMIT —

Session Agenda

- What?
- Why?
- How?

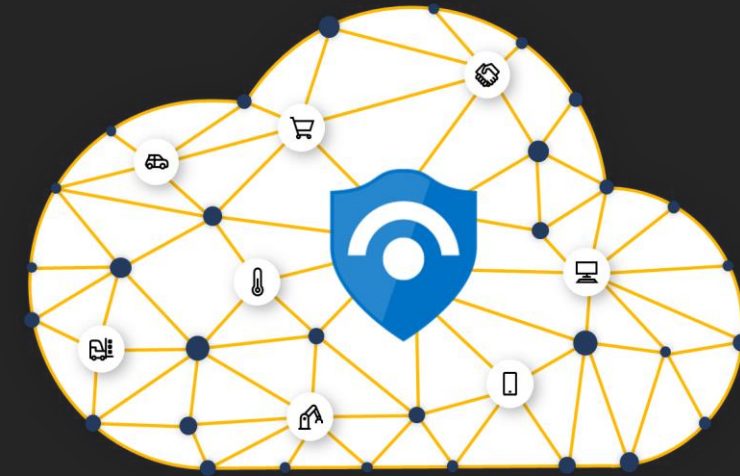
What?

What is Microsoft Sentinel

- Cloud native SIEM system
- Based on the PaaS model
- Hybrid solution
- Limitless Cloud speed and scale
- AI on your side for faster threat detection
- Cost efficient and secure



+



Cloud + Artificial Intelligence

Why?

Why Microsoft Sentinel







Here are some starting discussion points for a new SIEM system:

- System size (rightsizing)
- Disconnected services (lot,..)
- Cloud integration (Azure and more)
- Monthly costs
- Required upfront invest
- Automation options



Why Microsoft Sentinel

Here are the answers when you're using Microsoft Sentinel:

- System size (rightsizing)  Don't care, you're using PaaS
- Disconnected services (lot,..)  Public service
- Cloud integration (Azure and more)  Data connectors available
- Monthly costs  Pay-as-you-Go and RI
- Required upfront invest  Nothing
- Automation options  No automation limit

How?



How to start

The basic steps to onboard Microsoft Sentinel

- Define UseCases
 - Collect data
 - Implement visibility
 - Implement/use analytics rules
 - Implement/use hunting rules
 - Handle incidents
 - Implement automation



Collect Data

Collect data

Azure Activity Logs, Office 365 Activity Logs, Alerts from Microsoft Threat Protection are available at no cost. M365 E5 and Security E5 beneficiary

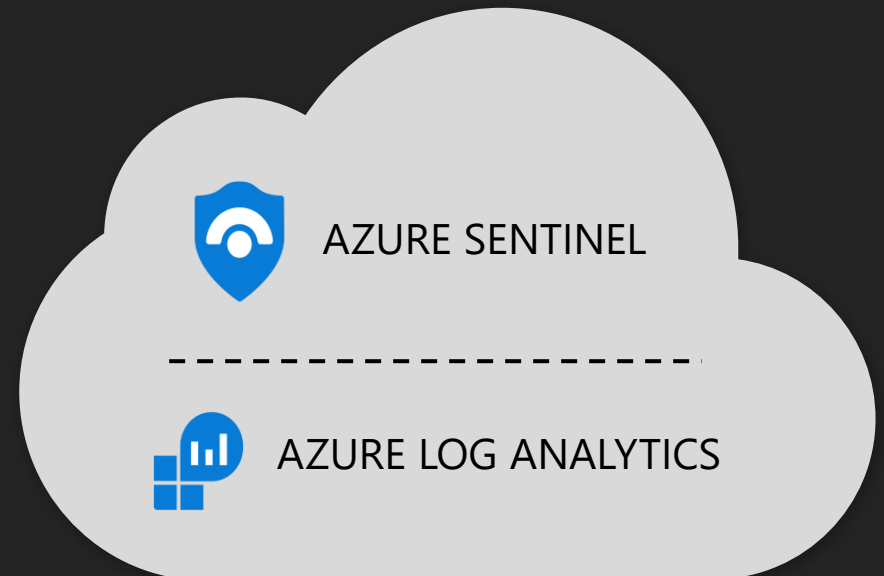


**AZURE + MICROSOFT 365
Security Alerts, Activity Data**

COLLECTORS
CEF, Syslog, Windows, Linux

TAXII + MS Graph
Threat Indicators

APIs
Custom Logs



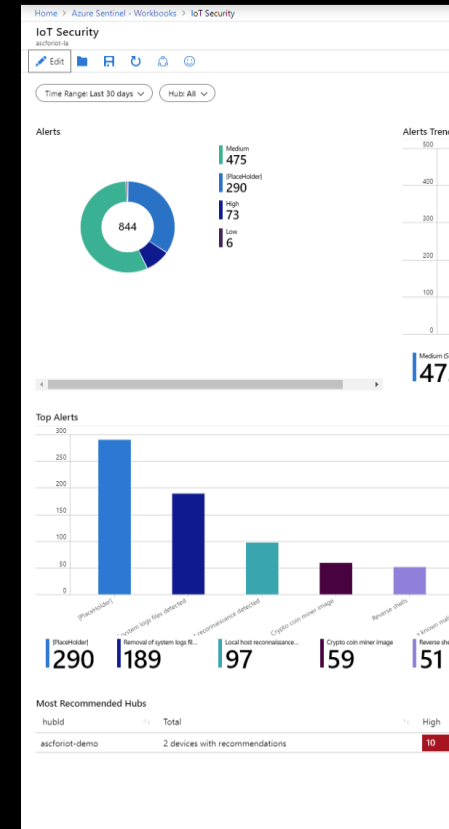


Implement visibility

Implement visibility

Azure Workbooks are the modern way, to visualize your data and allow you to quickly gain insights across your data as soon as you connected a data source

- Workbooks are used for many services
- Build-in workbooks available
 - Customizable
- Build your own workbooks
 - Huge design options
 - Different datasources

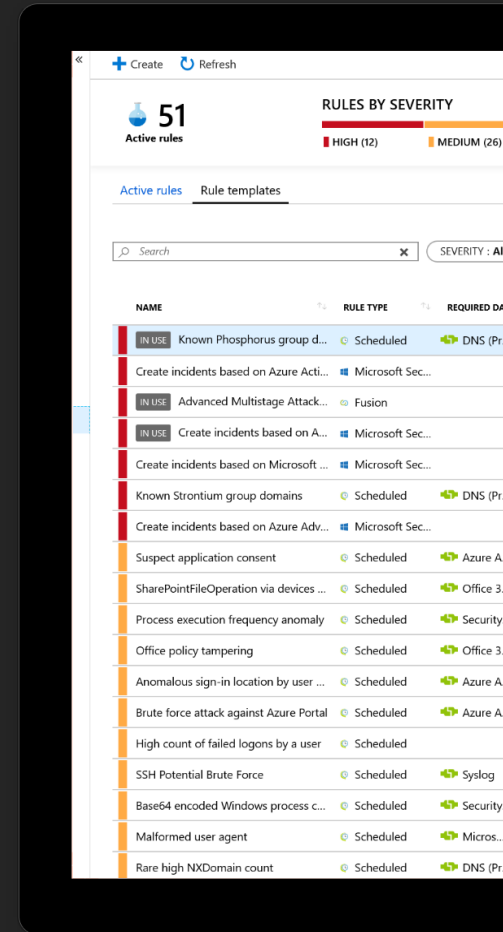


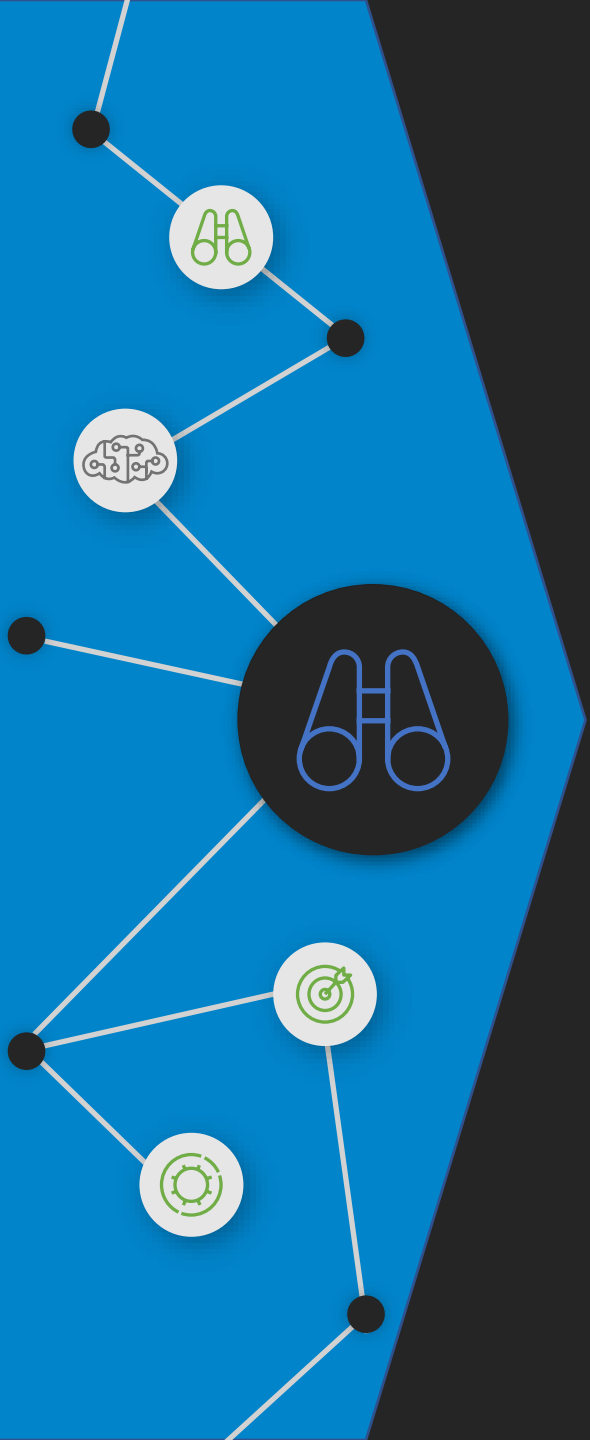


Analyse

Implement/use analytics rules

- More than 100 built-in Rule from Microsoft and community available
- Create your own rules based on KQL
- IaC is the key (Export and Import)
- Different rule types:
 - Microsoft Security (Defender, AzureAD,...)
 - Fusion (Correlation engine with scalable ML)
 - Machine learning (ML behavioral analytics template)
 - Anomaly (Preview) (Anomaly rule templates based on ML)
 - Scheduled (KQL based)
 - NRT (Preview) (KQL based)

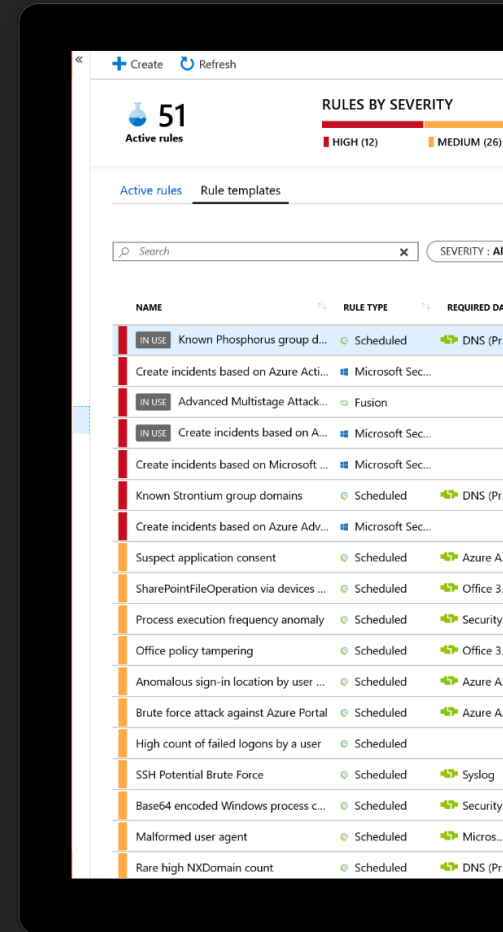




Hunting

Implement/use hunting rules

- More than 100 built-in Rule from Microsoft and community available
- Create your own rules based on KQL
- When should you use Hunting?
 - Before an incident occurs
 - During a compromise (livestream)
 - After a compromise
- Advanced hunting with Notebooks



Demo

Azure sentinel overview

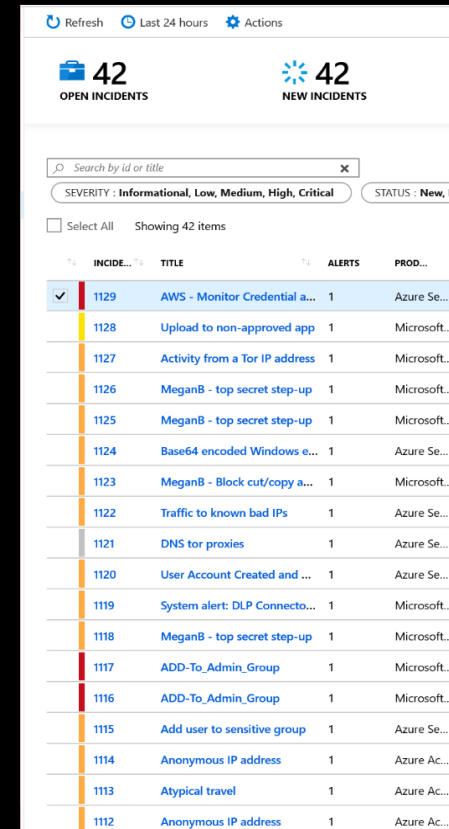
- Connectors
- Workbooks
- Analytics and hunting rules



Incidents

Incidents

- Use incident to collect related alerts, events, and bookmarks
- Assign incidents to users (AzureAD)
- Manage assignments and track status
- Add tags and comments
- Trigger automated playbooks

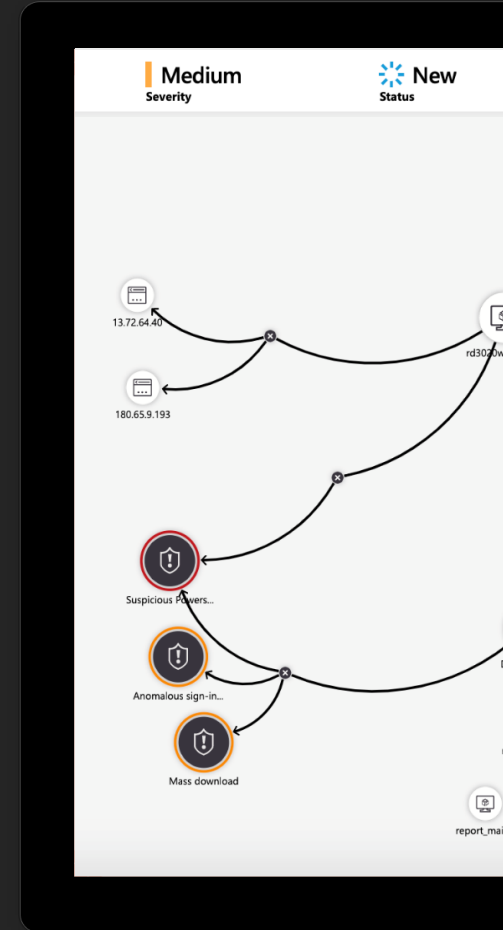


The screenshot shows the Microsoft Sentinel 'Incidents' page. At the top, there are buttons for 'Refresh', 'Last 24 hours', and 'Actions'. Below this, a summary bar shows '42 OPEN INCIDENTS' and '42 NEW INCIDENTS'. A search bar is present with the placeholder 'Search by id or title'. Below the search bar, filters for 'SEVERITY' (Informational, Low, Medium, High, Critical) and 'STATUS' (New) are visible. A table of incidents is displayed with columns for 'INCIDENT ID', 'TITLE', 'ALERTS', and 'PROBABLE CAUSE'. The first incident is selected, indicated by a checkmark in the first column.

INCIDENT ID	TITLE	ALERTS	PROBABLE CAUSE
✓ 1129	AWS - Monitor Credential a...	1	Azure Se...
1128	Upload to non-approved app	1	Microsoft...
1127	Activity from a Tor IP address	1	Microsoft...
1126	MeganB - top secret step-up	1	Microsoft...
1125	MeganB - top secret step-up	1	Microsoft...
1124	Base64 encoded Windows e...	1	Azure Se...
1123	MeganB - Block cut/copy a...	1	Microsoft...
1122	Traffic to known bad IPs	1	Azure Se...
1121	DNS tor proxies	1	Azure Se...
1120	User Account Created and ...	1	Azure Se...
1119	System alert: DLP Connecto...	1	Microsoft...
1118	MeganB - top secret step-up	1	Microsoft...
1117	ADD-To_Admin_Group	1	Microsoft...
1116	ADD-To_Admin_Group	1	Microsoft...
1115	Add user to sensitive group	1	Azure Se...
1114	Anonymous IP address	1	Azure Ac...
1113	Atypical travel	1	Azure Ac...
1112	Anonymous IP address	1	Azure Ac...

Visualize attacks

- Use visualization to
 - Get connection between Alerts, Bookmarks and entities
 - Advanced queries to get more details
 - Analyze timeseries

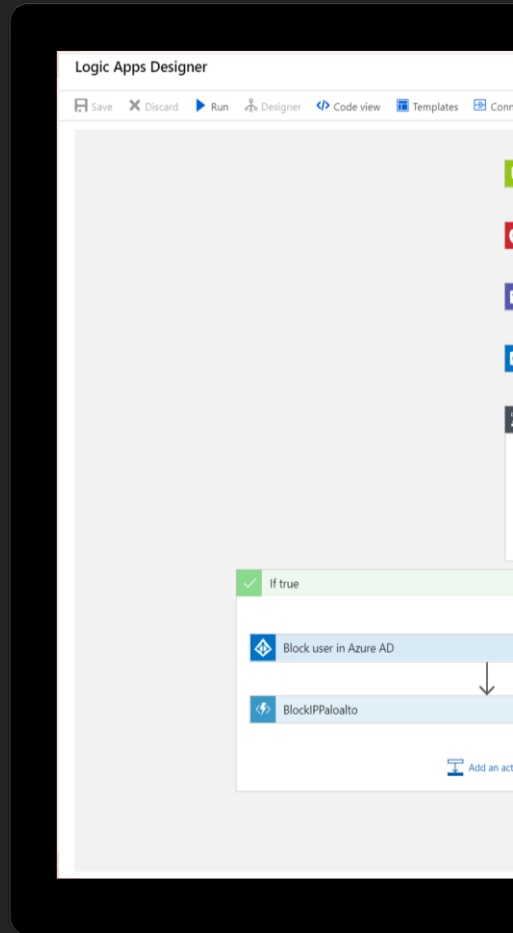




Automation

Implement automation

- Build automated and scalable playbooks
- Choose from a library of samples
- Create your own playbooks
- Trigger a playbook from an alert or incident investigation



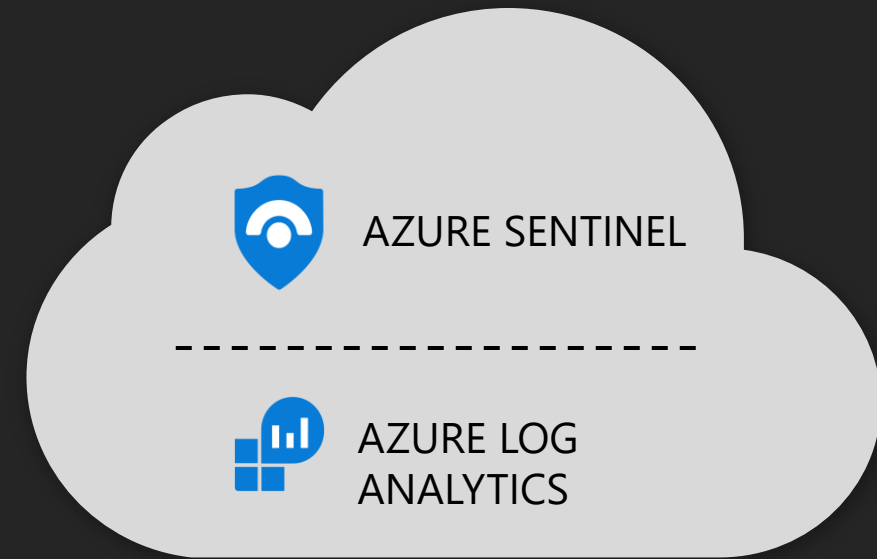
Demo

Azure sentinel SOAR

- Handle incident
- Automation
- Playbooks

Recap

- Build-in PaaS Service in Azure
- Based on Pay-as-you-Go
- High availability and scalability
- Better investigate and analyze security issues
- Massive automation options



Thank you
Q & A