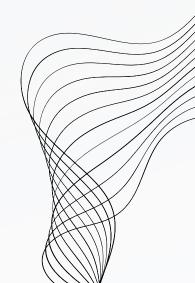


Microsoft Sentinel

(SIEM+SOAR)





Microsoft Sentinel

Cloud-native SIEM and SOAR for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your Office 365 data for Free

Easy integration with your existing tools

Faster threat protection with AI by your side

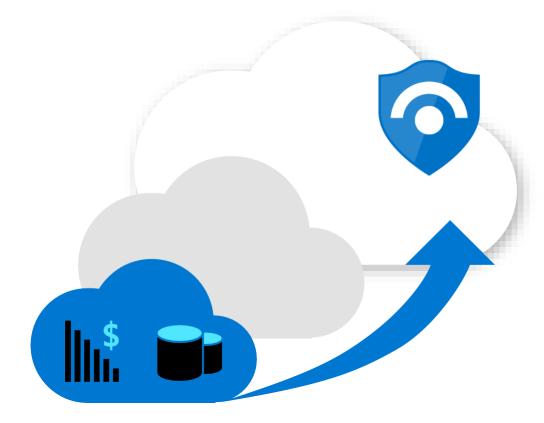


Reduce security and IT costs

No infrastructure costs or upfront commitment

Only pay for what you use

Bring your Office 365 Data for free



Cloud-native, scalable SIEM

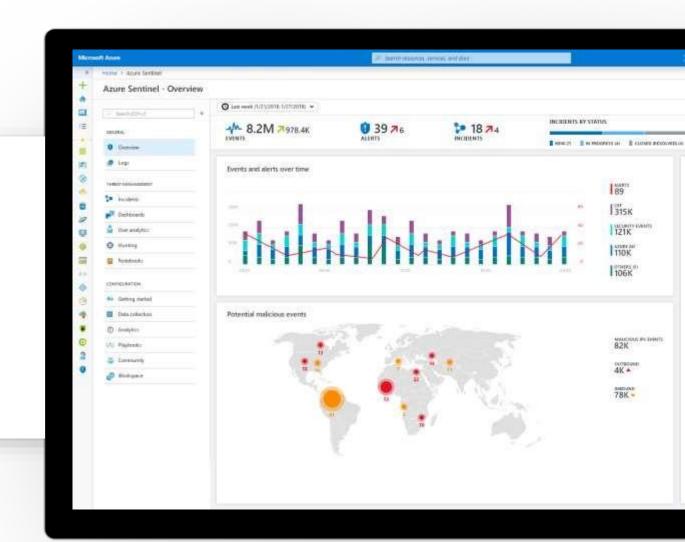
Focus on security, unburden SecOps from IT tasks

No infrastructure setup or maintenance

SIEM Service available in Azure portal

Scale automatically, put no limits

to compute or storage resources



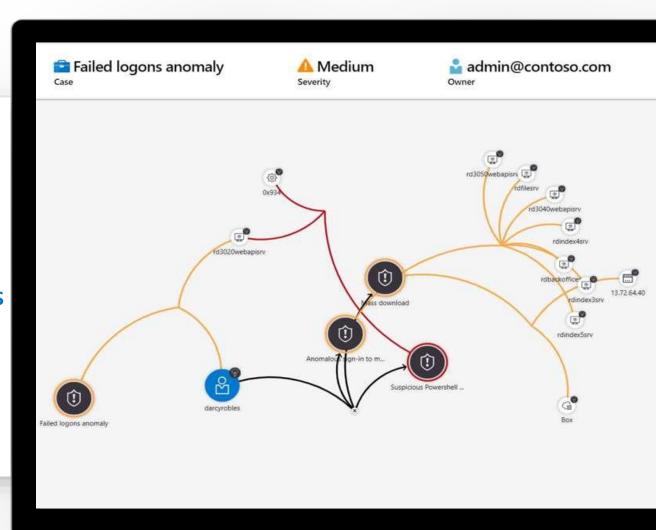
© Microsoft Corporation Azure

Investigate threats with AI and hunt suspicious activities at scale, tapping into years of cybersecurity work at Microsoft

Get prioritized alerts and automated expert guidance

Visualize the entire attack and its impact

Hunt for suspicious activities using pre-built queries and Azure Notebooks



Security Operations Center

Machine Learning (ML) & Al

■■ Behavioral Analytics (UEBA)

Security Incident & Event

Intelligent Security Graph (15G)

Azure

Integrated Threat Intelligence & Deep Human Expertise

A Security Center

A vmware aws

Hybrid Infrastructure and Apps

Management (SIEM)

Microsoft

Security Orchestration, Automation, and Remediation (SOAR)

Sentinel

Security Data Lake

Security & Network

Provide actionable security

(5) 🦠 📈 ...

✓ Symantec

SOPHOS

🛜 Lookout

alerts, raw logs, or both

Carbon Black,

FORTINET

CYBERARK C

Microsoft Reference Architecture

Broad Enterprise View

Classic SIEM

Deep Insights

derived from deep

knowledge of assets,

Actionable alerts

and ML/UEBA

Raw Logs

Security & **Activity Logs**

Case Management <

Alert Integration Graph Security AP

Correlated/Unified

Incident View

