Cloud Direct®

Sentinel:
2-Day Proof of Concept

Independently audited and certified expertise

Gold
Microsoft
Partner

Microsoft

Azure
Expert
MSP

Microsoft
Modernisation of Web Applications
Advanced Specialisation

Microsoft
Windows SQL Server
Advanced Specialisation

Microsoft
Azure Virtual Desktop
Advanced Specialisation

Microsoft
Teams Calling
Advanced Specialisation

Microsoft
Adoption and Change Management
Advanced Specialisation

Microsoft
Identity and Access Management
Advanced Specialisation

Microsoft
Information Protection and Governance
Advanced Specialisation

Microsoft
Threat Protection
Advanced Specialisation

vmware PARTNER
ENTERPRISE SOLUTION PROVIDER

CITRIX Partner Service Provider

ISO 27001 ISOQAR REGISTERED www.alcumusgroup.com

ISO 20000 ISOQAR REGISTERED www.alcumusgroup.com

Cloud Direct®

Plan

How

Sentinel Proof-of-Concept

What

Assess
- Analyse your requirements and priorities
- Define scope & deploy Sentinel for selected workloads
- Use temporary credits to initiate remote monitoring and proactive threat hunting to discover attack indicators

Explore the 'art of the possible'
- Discover threats and demonstrate how to automate responses.
- Engage in the POC in one of two scenarios:
  - Remote monitoring
  - Joint threat exploration

Build the plan
- Recommend next steps on how to proceed with a full implementation of Microsoft Sentinel

Value

- Access Microsoft funding
- 'Test drive' Sentinel to understand features, benefits and cost modelling
- Visibility of genuine threats
- Next-step deployment and management roadmap

Assess → **Plan** → Implement → Operate

Cloud Direct®

Sentinel Proof of Concept

Positioning

Azure Sentinel Discovery

An analysis of security requirements mapped to Azure Sentinel. A Sentinel proof of concept configured and deployed for the business to assess its value.

Benefits

Experience the results

The Sentinel POC will help you discover threats, understand how to mitigate threats and provide the information for a full on-boarding to Sentinel.

Deliverables

PoC to demonstrate the benefits of Sentinel to your organisation.

Analysis report and mitigation recommendations.

Walk through with key business stakeholders.

Summary of works

Analyse

- Business and IT requirements
- Existing SIEM/SOC tools
- Data sources to be connected
- Security Operations automation requirements

Define Scope & Deploy

- Define the scope of the Azure Sentinel deployment
- Deploy and configure Azure Sentinel
- Connect Azure Sentinel to ingest data from:
  - Azure AD Identity Protection
  - Microsoft Cloud App Security
  - Agreed 3rd party Syslog integration
  - Limited nr. of on-premises servers

Remote Monitoring

- Remote incident monitoring during the data collection phase
- Threat hunting to discover Indicators of Attack in the ingested data

Discover

- Use Azure Sentinel to analyze and discover threats to your organization

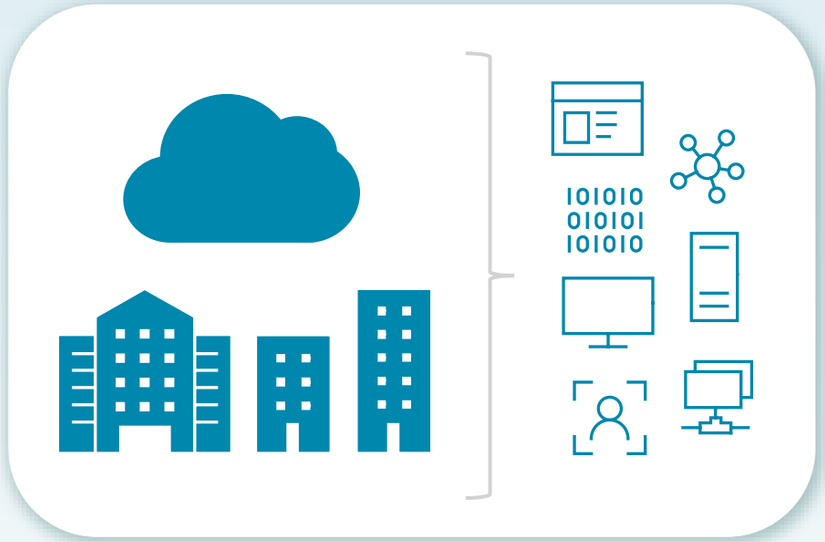
Recommend

- Detail found threats and recommendations
- Provide an Azure Sentinel deployment roadmap

Assess → **Plan** → Implement → Operate

Cloud Direct®

Collect security signals at scale



AZURE & MICROSOFT 365
Security Alerts, Activity Data

COLLECTORS
CEF, Syslog, Windows, Linux

TAXII + MS Graph
Threat Indicators

APIs
Custom Logs

Microsoft Sentinel

Azure Monitor Log Analytics

Cloud Direct®