DELPHI
IT STRATEGY | CONSULTING | SUPPORT

Microsoft Partner
Microsoft

Gold Communications
Gold Cloud Platform
Gold Cloud Productivity
Gold Enterprise Mobility Management
Gold Windows and Devices

Azure Sentinel – POC in a Week

Build your Fort-Knox

ABOUT DELPHI CONSULTING:

When it comes to Security, you need an experienced partner. We have been Microsoft security and compliance finalist for 2020. We will work with you to understand your environment and identify opportunities to help you achieve continuous business value from your Teams investment.

As a trusted adviser, Delphi Consulting can help you protect your environments from an ever-evolving threat landscape with Microsoft Security and Compliance solutions.

See what customers are saying:

"One of the many things I love in Azure is Microsoft's capability to unify the user experience behind a single, smooth experience. The same applies to Azure Sentinel – instead of trawling through weird XML-based config files, you can easily provision and onboard Azure Sentinel through Azure Portal.

– Ilyas Mohammad, The First Group

WHAT WE OFFER

Protecting your systems, data and users has never been more challenging. Cyber threats are growing rapidly in volume and sophistication, whilst a cloud-enabled and mobile workforce has restricted visibility and control. For many organizations, incident investigation and response processes are complex, slow and expensive – in today's climate, they are simply unfit for purpose.

Delphi Consulting will help you get started with Azure Sentinel with its Proof of Concept offering and the program running over 4-5 days. We aim to provide you a definite understanding of how Azure Sentinel can contribute to your business from securing the enterprise to saving the infrastructure cost.

Delphi's offering:

- Drive workshop with customer security team to understand all the security reporting and automation requirements.
- Configure and showcase below Azure sentinel functionalities based on the workshop conducted.
    - Analytic rules
    - Workbooks
    - Automation playbooks
    - Integration with third party security devices and native Microsoft components.
- Deliver Azure Sentinel High level design document.
- Deliver TCO based on assessment performed.
- Threat Mitigation Recommendations (Optional)

Why Azure Sentinel and Delphi?

Azure Sentinel Proof of Concept Service

Delphi Consulting provide an Azure Sentinel Proof of Concept Service to help your organization trial and test Microsoft's powerful next generation SIEM+ SOAR solution.

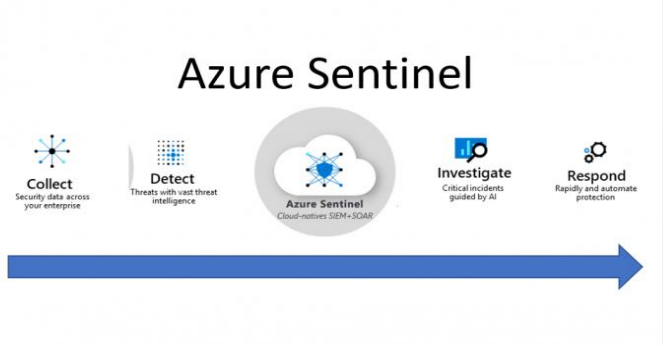
Delphi Consulting will help you to deploy a concept Sentinel instance and provide a demonstration of how the solution works driving intelligent security analytics and threat intelligence across the enterprise.

Scope of Work

- Initial Discovery Assessment – Understanding customer's need around security challenges
- Introduction to Azure Sentinel, its capabilities and how it can help improving security posture
- Technical enablement
  - ➢ Set up Azure Sentinel Workspace
  - ➢ Set-up Syslog Log Collector
  - ➢ Enabling three native M365 Security Components
  - ➢ Demonstrate onboarding of a windows server (Domain Controller)
  - ➢ Demonstrate onboarding of two security log sources
- Configure Built-in Analytics Rules (10-15)
- Customize and create two workbooks
- Demonstrate creation of two automation playbooks
- Provide Technical & Operational Guidance
- Documentation

Customer Key Take-aways

- Get a complete overview of Azure Sentinel
- gain an understanding of your security challenges and infrastructure
- A workshop report and recommendations for next steps
- Get a high-level solution plan, roadmap and next steps
- Get Pricing Details for Azure Sentinel
- Get a high-level Sentinel Architecture Diagram
- Focus on your core strengths - protecting your business
- Cut out the 'noise' and prioritizes incident response
- Enable rapid detection, investigation, and response
- Save on infrastructure and management overheads
- Harness the power of Machine Learning and AI


Azure Sentinel
Collect
Security data across your enterprise
Detect
Threats with vast threat intelligence
Azure Sentinel
Cloud-natives SIEM+SOAR
Investigate
Critical incidents guided by AI
Respond
Rapidly and automate protection

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Features & Capabilities

Single Pane of Glass

Presents bird's eye view of the across the enterprise with Integrated monitoring across both on-prem and cloud infrastructure.

Scalable Model

Scale up to as much capacity as the situation requires. You will pay only for the amount of service they use, without any up-front cost.

Security Analytics & Orchestration powered with AI & ML

Provides intelligent security analytics at cloud scale using the power of Artificial Intelligence & Machine Learning. Built-in automation and orchestration with pre-defined or custom playbooks to respond to threats quickly.

Collect Data

Collect data at cloud scale—across all users, devices, applications and infrastructure, both on-premises and in multiple clouds

Detect Threats

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft

Investigate & Respond

Investigate threats with AI and 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