Insight

Microsoft Sentinel Foundations

Gain control and visibility of your entire IT security environment

Business challenge

The proliferation of platforms, data, users and mobility is creating new challenges for security teams. Visibility and manageability are hard to attain, let alone staying on top of endless alerts and tool updates. Microsoft Sentinel, the Microsoft cloud-based Security Information and Event Management System (SIEM), was created to provide a whole new level of control and visibility across the entire IT security environment.
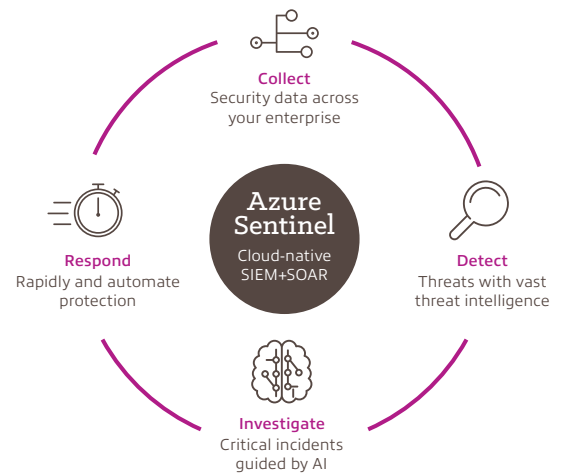
Microsoft Sentinel lets you combine and analyse security data from all your users, endpoints and infrastructure to make threat protection smarter and faster. The platform offers built-in and third party capabilities such as Threat Intelligence, Machine Learning, and Security Orchestration and Automated Response.

How we help

Insight's Microsoft Sentinel Foundations offers expert-led workshops that combine training and assessment of your security environment. Centered around best practices for cloud and security, this engagement familiarises your team with new technology and provide you with a working environment you can begin using right away.

Our goal is to help you meet your transformation goals — and move forward with confidence. We'll work collaboratively with your team to deliver:

- An assessment of your existing security infrastructure and evaluation of your policies and requirements
- Technical design of your Sentinel solution and Security Operations Centre (SOC) integrations
- Deploy and configure Microsoft Sentinel and Connectors
- Three-week data ingestion period for baselining data
- Develop and present a threat exploration report and roadmap for next steps

Collect
Security data across your enterprise

Azure Sentinel
Cloud-native SIEM+SOAR

Respond
Rapidly and automate protection

Detect
Threats with vast threat intelligence

Investigate
Critical incidents guided by AI

Duration

- 1.5 months

Benefits

- Collect security data across your enterprise
- Detect threat with vast threat intelligence
- Respond rapidly and automate protection

Related offers

- Security Envisioning Workshop
- Security Assessment
- Azure Security, Governance & Cost Control Assessment

Get started.

To learn about pricing and how to begin, contact **ANZ_DI_Sales@insight.com**

Microsoft Solutions Partner
Microsoft Cloud

Microsoft Solutions Partner
Security

1800 189 888
au.insight.com

0800 933 111
nz.insight.com
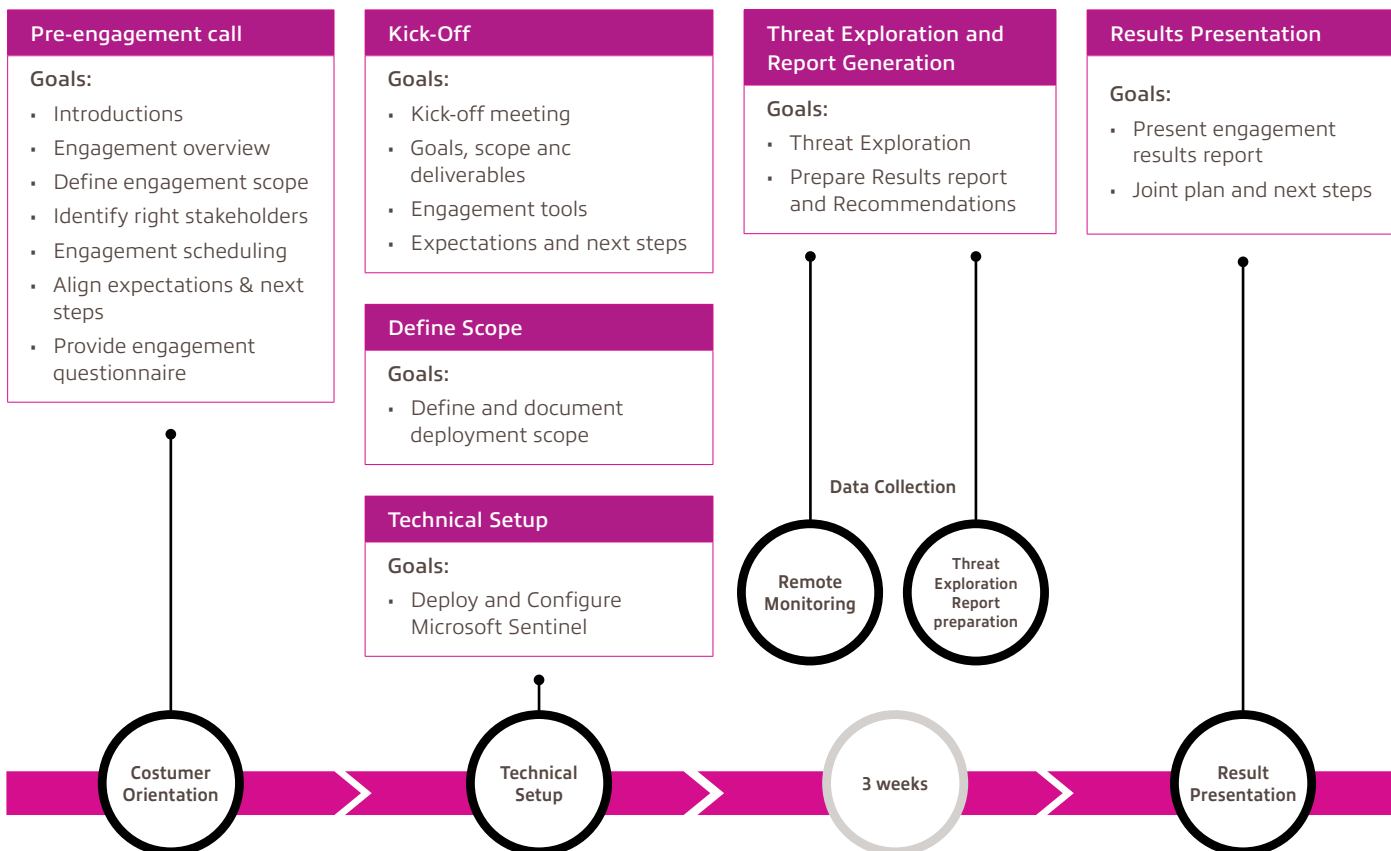
65 6438 2995
sg.insight.com

Preparing for transformation

To ensure you receive the greatest value from this engagement, our experts will need the following:

- Discovery workshop with your Business and Technical stakeholders to align on a definition of business and technical goals and assess current environment.

- An Azure subscription approved to receive data from your business systems.
- A preliminary view of what data sources you are looking to connect to Microsoft Sentinel.

What to expect

Discovery & Assessment	Implementation & Threat Analysis	Next Steps & Roadmap
We'll begin by exploring your organisation's current security strategy, goals and requirements. We will educate your key stakeholders on Microsoft security services and Microsoft Sentinel. Through the whiteboarding sessions, we will review the Microsoft Sentinel build and the strategies and best practices to be leveraged for the design.	We will deploy Microsoft Sentinel and create a log analytics workspace to analyse your data. We will connect up to three existing Microsoft data sources, such as Advanced Threat Protection, Office 365 and Cloud App Security, into your Microsoft Sentinel SIEM. Three weeks of data ingestion will be monitored and a threat exploration report will be generated.	The assessment report and technical design document will be provided. The threat analysis review will be presented to your key stakeholders, providing recommendations on next steps. A transformation roadmap will also be delivered, providing guidance on how to best maximise your Microsoft Sentinel investment and further mature your organisation's security posture.

Pre-engagement call

Goals:

- Introductions
- Engagement overview
- Define engagement scope
- Identify right stakeholders
- Engagement scheduling
- Align expectations & next steps
- Provide engagement questionnaire

Kick-Off

Goals:

- Kick-off meeting
- Goals, scope anc deliverables
- Engagement tools
- Expectations and next steps

Define Scope

Goals:

- Define and document deployment scope

Technical Setup

Goals:

- Deploy and Configure Microsoft Sentinel

Threat Exploration and Report Generation

Goals:

- Threat Exploration
- Prepare Results report and Recommendations

Results Presentation

Goals:

- Present engagement results report
- Joint plan and next steps

Data Collection

Remote Monitoring

Threat Exploration Report preparation

Costumer Orientation → Technical Setup → 3 weeks → Result Presentation

About Insight

Insight Enterprises, Inc. is a Fortune 500 solutions integrator with more than 11,500 teammates worldwide helping organisations accelerate their digital journey to modernise their business and maximise the value of technology. We enable secure, end-to-end transformation and meet the needs of our clients through a comprehensive portfolio of solutions, far-reaching partnerships and 33+ years of broad IT expertise. Rated as a Forbes World's Best Employer and certified as a Great Place to Work, we amplify our solutions and services with global scale, local expertise and a world-class e-commerce experience, realising the digital ambitions of our clients at every opportunity.

Insight.

Microsoft