

# SecOps Pathfinder

## Improve Security Operations With Microsoft Sentinel

SecOps teams face numerous challenges, including managing extensive amounts of data, navigating siloed technologies, and swiftly responding to sophisticated threats. To address these issues, our modular SecOps Pathfinder engagement shows how Microsoft Sentinel, AI, and Microsoft Security Analytics will improve your security operations and guide you towards success.

### Why use our SecOps Pathfinder?

- ✓ **Requirement Analysis:** Analyse your requirements and priorities for a SIEM deployment.
- ✓ **Enhance Visibility:** See and stop threats swiftly across identity, email, and data in both on-premises and cloud environments.
- ✓ **Remote Monitoring and Discovery:** Use Microsoft Sentinel incidents and proactive threat hunting to discover attack indicators.
- ✓ **Define Next Steps:** Plan for a production deployment of Modern SecOps.

### Modules

#### Included

- ✓ XDR/ Unified SecOps
- ✓ Identity Threat Detection
- ✓ Communication & Collaboration Threat Detection
- ✓ Azure Threat Detection
- ✓ Threat Intelligence

#### Optional

- ✓ Third-Party Alert/Logs
- ✓ Server Threat Detection
- ✓ SOC Automation

### What's in it for me?



Understand the requirements, features and benefits of a Unified SecOps Platform.



Better understand, prioritise, and mitigate potential threat vectors.



Be ready to rapidly adopt Microsoft Sentinel to compliment existing Microsoft security tools.



Create a tailored deployment roadmap and develop joint next steps.

# SecOps Pathfinder

## Who Is This Suitable For?

A SecOps Pathfinder is suitable for organisations and teams looking to enhance their security operations through advanced tools and methodologies, these include:

- ✓ Security Operations Center (SOC) Teams
- ✓ IT Managers and Directors, CISO (Chief Information Security Officers)
- ✓ Network Security Engineers
- ✓ DevSecOps Teams and Compliance Officers

## What To Expect?

During the SecOps Pathfinder, SCC requires just 4 hours of your time across 5 weeks. In that time, you will gain a clear understanding of how unified SecOps could work for your team.



## Why SCC?

SCC are a member of Microsoft Intelligent Security Association and a Microsoft Security Solutions Partner.

We hold all four advanced specialisations strengthening confidence in our expertise and solidifying our position as a leading provider of managed security services.

SCC Cyber leverage the power of Microsoft Sentinel, Defender for Endpoint, and the Microsoft 365 Defender stack combined with our Security Operations Centre and specialists, to strengthen your security posture and deliver rapid detection & response across your organisation.

Member of  
Microsoft Intelligent Security Association



Microsoft  
Solutions Partner  
Security

Specialist  
Cloud Security  
Threat Protection  
Identity and Access  
Management  
Information Protection and  
Governance