

# Modernise your security operations centre (SOC) with Microsoft Sentinel







The frequency and intensity of cyberattacks continue to increase—and the rise of AI technologies contributes to the growing problem. **Can your traditional security information and event management (SIEM) keep up?** We're a Microsoft partner focused on security, and we want to help you modernise your SIEM.

## Secure your multi-cloud, multi-platform environment with an AI powered SIEM

Microsoft Sentinel delivers a scalable, cloud-native solution for comprehensive threat detection and response. Designed to work across your entire digital estate, you'll get a single solution for attack detection, threat visibility, proactive hunting, user and entity behavior analytics (UEBA), and threat response.

### Collect and analyse data

-  Eliminate infrastructure set up and maintenance with a cloud-native SIEM
-  Flexible data ingestion and storage options
-  350+ out-of-the-box connectors
-  Single-click use case discovery and deployment






### Detect evolving threats

-  Alerts automatically correlated into prioritised incidents
-  Full visibility of an attack path, even across multiple sources
-  Built-in UEBA to automatically detect anomalies
-  Automatic enrichment with Threat Intelligence backed by Microsoft Threat research







### Respond across all your tools

-  Built-in security orchestration, automation, and response (SOAR)
-  Customisable automations for rapid response via logic apps
-  200+ Microsoft created solutions and 280+ community contributions







### Use advanced threat hunting

-  Comprehensive hunting across all your data, including archives
-  Track coverage with MITRE dashboard
-  Easily query for threats using KQL
-  Search across verbose data using summary rules



### Investigate incidents with full context

-  Security Copilot embedded into the experience
-  Built-in machine learning for incident correlation, SOC optimisations, automatic attack disruption, and more
-  Visual investigations of the full scope of incidents
-  Unified data model across Defender XDR and Defender for Cloud for comprehensive incident creation, and 50% faster responses

## Let's modernise your SOC together

Professional Advantage is uniquely qualified to accelerate your security operations modernisation project with our service offerings.

Contact us today to learn more.

1800 126 499  
enquiries@pa.com.au  
pa.com.au/sentinel

Contact us today