Softcat

SENTINEL MATURITY ACCELERATOR SERVICE

Enhances Microsoft Sentinel deployment by accelerating detection coverage and improving SIEM maturity through key activities, such as detection content improvements, detection content tuning recommendations, and cost optimisation.

CYBER SECURITY

HOW DOES THE SERVICE WORK?

This service is tailored to your Microsoft Sentinel environment. It is split into three (3) potential focus areas that can be worked through and are all designed to work together and bring maximum value by improving your overall SIEM maturity.

Detection Content Improvements: We analyse your data sources, recommend additional detection rules (using both open-source and in-house libraries), and provide recommendations on additional data sources to onboard to enhance detection coverage. All detection rules align with the MITRE ATT&CK framework.

Detection Content Tuning Recommendations: We offer recommendations for entity tuning for existing incidents within Microsoft Sentinel. Our guidance optimises configurations for entities involved in ongoing incidents, leveraging the platform's robust capabilities to accurately identify and assess entities tied to security alerts. This enhances alert detection precision, improves security posture, and streamlines investigations, ultimately accelerating incident resolution.

Cost Optimisation: Ingestion costs can easily get out of control. We review your existing data sources and provide recommendations for data filtering, including moving data to new tables and adjusting Log Analytics pricing tiers. Our expertise covers both native and custom data sources, and we've achieved an average savings of 40%* on annual Microsoft Sentinel costs.

**Actual savings may vary depending on specific circumstances, usage and deployment.*

BENEFITS TO YOU

People

Receive expert analysis and recommendations on improving detection content and tuning.

This can give you a deeper understanding of your security posture and enhance your ability to anticipate and respond to threats.

Technology

Specialised guidance and implementation support on optimising entity configurations and fine-tuning detection rules allows you to streamline your security operations.

This leads to more precise alert detection and faster incident resolution, reducing the workload and stress on your security teams.

Commercials

Access tailored recommendations for cost optimisation opportunities.

We can help you manage and reduce your data ingestion costs effectively.

SUITABLE FOR YOU IF...

- ✓ You are looking to expedite the journey towards SIEM maturity.
- ✓ You want to identify potential gaps in existing detection coverage.
- ✓ You want to reduce noise and alert fatigue with existing content.
- ✓ You are looking to expedite custom use case development.
- ✓ You are looking to manage Sentinel costs that result from data ingestion.

WORKS WELL WITH

Managed Sentinel Service

Combines the threat protection, security intelligence and automation of the Sentinel security platform with expert monitoring and management by Softcat's Security Operation Centre.

Threat Exposure Management

Provides a holistic and proactive approach to managing cyber security risks, helping you validate existing controls and stay ahead of emerging threats and vulnerabilities.

Managed Azure Service

Utilise the power of Azure cloud and enhance your IT team's public cloud expertise.

WHAT'S INCLUDED

Specialised recommendations - Guidance on optimising configurations for entities involved in ongoing incidents within Microsoft Sentinel.

Cost optimisation - Through data filtering, data splitting, or moving specific data to new tables and changing Log Analytics pricing tiers, achieving cost savings in relation to Sentinel Ingestion.

Reducing alert fatigue - Through tuning recommendations, we assist in reducing noise and alert fatigue with existing content.

Detection coverage - Identify and provide recommendations on any gaps in existing detection coverage.

SERVICES THAT BRING YOUR TECHNOLOGY TO LIFE

Contact your Softcat Account Manager today.

JULY 2024