e2e assure

Microsoft Sentinel Operations Consultancy

Service Definition Document

Microsoft Sentinel Operations Consultancy

Service Definition Document – G-Cloud 15

CONTENTS

SERVICE INTRODUCTION

Microsoft Sentinel has increased commercial and technical accessibility for real-time threat detection, analysis, and response. As cyber threats increase in sophistication and complexity, businesses need to ensure their Sentinel deployment is optimised for comprehensive detection coverage and containing threats in minimal time, while simultaneously maintaining the appropriate balance between cyber risk and investment.

SERVICE OVERVIEW

The e2e-assure Microsoft Sentinel Operations Assessment provides a detailed analysis of your existing Sentinel configuration, processes, and effectiveness, along with practical recommendations to uplift overall SOC maturity. e2e-assure consultants will use their extensive experience in designing, implementing, and optimising Microsoft Sentinel to assess the level of coverage, identify gaps & optimisation opportunities, pinpoint any blind spots, inefficiencies, or areas where best practices aren't being fully leveraged to full potential.

SCOPE OF ACTIVITIES

The end-to-end review assignment will include the following actions and areas of assessment:

Stage	Tasks
Data Connectors:	• Assessment of Log Ingestion & Telemetry • Verify that each connector is up to date • Review the data connectors to confirm that the correct sources are integrated, and that ingestion is active, accurate, and efficiently managed.
Analytics Rules:	• Review & Tuning - Examine existing analytics rules for accuracy, false-positive rates, and alignment with the latest threat intelligence. • New Analytics Development – recommendations to develop or refine analytics rules to address newly discovered threats, tactics, techniques, and procedures (TTPs).
Workbooks	• Assess the design and utility of existing Workbooks for real-time monitoring and incident investigation. • Identify opportunities to implement best practices for building custom Workbooks that amalgamate data from multiple sources into cohesive views.
Hunting Queries:	• Evaluate and identify opportunities to enhance existing hunting queries to search for subtle or emerging threats. • Validate that the level of threat intelligence integration is appropriate to guide the development of new, high-priority hunt queries.
Watchlists:	• Review current watchlists to ensure timely updates and coverage of critical assets and indicators. • Validate watchlist-driven queries for performance and provide guidance to align watchlists with business context.
Playbooks & Azure Logic Apps:	• Evaluate existing playbooks for coverage and effectiveness in automating incident triage, containment, and remediation steps. • Provide recommendations to expand playbook coverage, enhance logic flows, reduce MTTR (Mean Time to Respond), and increase precision.

SCOPE OF DELIVERABLES

The following tangible outputs will be provided as part of the engagement sign-off:

Output	Description
Current-State Assessment Report	• Detailed analysis of your Microsoft Sentinel setup, highlighting strengths, weaknesses, and gaps.
Prioritised Recommendations & Action Plan	• A clear roadmap with time-bound, actionable steps to enhance your Sentinel-based SOC.
Enhanced Analytics & Automation Samples	• Examples or prototypes of tuned analytics rules, hunt queries, watchlists, and playbooks for future reference and adoption.
Best Practices Guide	• Tailored documentation summarising key configurations, governance steps, and operational procedures for ongoing SOC maturity.
Knowledge Transfer Session	• Presentation and handover session for stakeholders, SOC analysts, and engineers on recommended improvements and usage of advanced features.

SERVICE OUTCOMES

- Improved efficiency and effectiveness of Microsoft Sentinel SOC operations.
- Increase in security posture and reduction in probability of breach scenario
- Uplift in team skills, capabilities, and confidence levels to evolve SOC performance.
- Clarity on areas for potential future investment to achieve step changes in detection & containment capabilities.