e2e assure

Targeted Threat Hunt

Service Definition Document

Targeted Threat Hunt

Service Definition Document – G-Cloud 15

CONTENTS

Service Introduction 2
Service Overview 3
Scope of activities 4
Scope of Deliverables 5
Service outcomes 6

Service Introduction

Businesses face persistent and evolving adversaries who employ sophisticated tactics to evade detection, when a sector-aligned threat actor is particularly active with novel approaches to breaching targets, this can drive uncertainty about potential undetected compromises.
Security leaders must have confidence in their team's ability to detect and respond to emerging attack techniques. Without this assurance, blind spots and misconfigurations can go unnoticed, increasing the likelihood of a successful breach.

Service Overview

The e2e-assure Targeted Threat Hunt is designed to uncover hidden threats within your environment using a hypothesis-driven approach, we conduct a deep-dive analysis across relevant logs, telemetry, and security tooling to identify indicators of compromise (IoCs) and adversary behaviour.
Targeted Threat Hunt delivers deep investigative analysis to expose hidden threats and strengthen cyber resilience.

SCOPE OF ACTIVITIES

The assignment will include the following actions and areas of assessment:

Stage	Tasks
Pre-Hunt Preparation	• Define scope, objectives, and areas of focus based on business risk profile. • Identify relevant threat actors, tactics, techniques, and procedures (TTPs) aligned to the sector. • Conduct initial threat intelligence review to inform hunting hypotheses
Hypothesis Creation & Planning	• Develop threat hypotheses based on recent adversary behaviours and attack trends. • Map hypotheses to MITRE ATT&CK framework where feasible and industry-specific threat models. • Identify relevant log sources, telemetry, and security controls for analysis
Data Collection & Enrichment	• Aggregate relevant logs and telemetry • Correlate threat intelligence feeds with internal security data. • Normalise and structure collected data for efficient analysis
Log Querying & Threat Detection	• Execute custom and predefined queries to detect indicators of compromise (IoCs) and behavioural anomalies. • Analyse endpoint, network, identity, and cloud activity for stealthy attacker presence. • Identify anomalous process execution, credential abuse, suspicious persistence mechanisms, and lateral movement attempts. • Investigate failed and successful authentication events, privilege escalations, and data exfiltration patterns
Findings Analysis & Risk Prioritisation	• Assess severity, impact, and likelihood of detected threats or weaknesses. • Identify detection gaps, misconfigurations, and blind spots in security tools. • Correlate findings with business-critical assets and operational risks

SCOPE OF DELIVERABLES

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

Output	Description
Reporting & Recommendations	• Deliver an executive summary outlining key findings, risk areas, and high-level recommendations. • Provide a detailed technical report with identified threats, security gaps, and step-by-step remediation guidance. • Offer detection rule improvements and guidance on refining SIEM alerts and security tooling configurations
Post-Hunt Consultation & Next Steps	• Conduct a debrief session with key stakeholders to walk through findings. • Provide prioritised action plan for remediation and security enhancements. • Recommend ongoing monitoring strategies and improvements to proactive threat detection

Service outcomes

- Identifies gaps before they result in costly data breaches, regulatory fines, or business disruptions
- Delivers targeted insights on adversaries most relevant to the business sector and operations
- Detects hidden threats and potential breaches before they escalate into major security incidents
- Provides data-driven insights to inform security investments and reduce organisational risk exposure