e2e assure

**Breach Disruption Assessment**

Service Definition Document

Breach Disruption Assessment

## Service Definition Document – G-Cloud 15

## CONTENTS

## SERVICE INTRODUCTION

Businesses invest heavily in security tooling, automation, and monitoring, yet many lack certainty that these controls will perform effectively in a live attack scenario. Security teams often assume that detections will trigger as expected, that automated response workflows will contain threats efficiently, and that analysts will respond with the right actions under pressure. However, without controlled validation, these assumptions remain untested, leaving potential gaps in detection coverage, unknown weaknesses in automation, and uncertainty about whether response processes align with operational expectations.

## SERVICE OVERVIEW

The e2e-assure SOC Breach Disruption Assessment systematically validates your organisation's detection, containment, and security automation capabilities against real-world attack scenarios. Using controlled simulations mapped to the MITRE ATT&CK® framework, we assess how well your security controls detect and respond to adversary tactics, techniques, and procedures.
We test endpoint detection and response (EDR), SIEM correlation rules, and orchestration workflows to ensure they trigger appropriate alerts and actions. Through targeted attack scenarios, we identify gaps in security tooling, rule misconfigurations, and response inefficiencies, providing actionable recommendations to enhance the cyber resilience of your organisation.

## SCOPE OF ACTIVITIES

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

| Stage | Tasks |
|---|---|
| **Customer Infrastructure & SOC Assessment** | • Conduct an initial scoping session to understand the environment, security tools, and detection capabilities.<br>• Review SOC processes, detection rules, and response automation workflows in place.<br>• Review expected detection and response coverage.<br>• Identify key security monitoring tools and how alerts are managed. |
| **Attack Simulation Tooling Deployment, Setup, and Integration** | • Deploy and configure attack simulation agents within the customer environment.<br>• Integrate with supported SIEM (as specified in contractual agreement) to track detection events in real-time. |

| | |
|---|---|
| | • Configure attack scenarios based on customer risk profile, industry threats, and known attacker techniques.<br>• Test attack execution paths to confirm successful simulation without disrupting business operations. |
| **Attack Simulation & Detection Monitoring** | • Execute controlled attack scenarios across different tactics and techniques from MITRE ATT&CK®.<br>• Monitor detection and response activity in real-time to assess SOC visibility and effectiveness.<br>• Validate security tooling performance, including endpoint detection and automated response actions.<br>• Assess SIEM alert detection time and accuracy in identifying, classifying, and responding to threats.<br>• Conduct ad-hoc adjustments to test detections against variations of attack techniques. |
| **Reporting & MITRE ATT&CK® Coverage Analysis** | • Document attack techniques tested, including successful and missed detections.<br>• Map detection coverage to the MITRE ATT&CK® framework to highlight security strengths and weaknesses.<br>• Identify gaps in detection logic, alert fidelity, or response playbook execution.<br>• Provide logs from the attack simulations for further SOC review and tuning. |

## SCOPE OF DELIVERABLES

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

| Output | Description |
|---|---|
| **Recommendations for Improvement** | • Prioritised recommendations for improving detection rules, response playbooks, and security tool configurations.<br>• Provide guidance on detection engineering, including SIEM rule enhancements and EDR tuning.<br>• Suggest automation improvements where playbooks or integrations can reduce response time and analyst workload. |
| **Findings Presentation** | • Structured session to brief key stakeholders on findings summary and handle any clarification requirements |

## SERVICE OUTCOMES

- Benchmark security performance against the MITRE ATT&CK® framework and industry best practices

- Calibrate cybersecurity priorities and business objectives alignment with precision, ensuring risk mitigation strategies are proactive and effective
- Provide evidence-backed assurance to executives, auditors, and stakeholders on the effectiveness of current security investments
- Provides SOC analysts with hands-on experience responding to simulated attacks, reinforcing skills and decision-making under pressure
- Gain a measurable view of current detection, automation, and response capabilities.
- Data to inform future security investments