e2e assure

Dark Web Exposure & Credential Leak Risk Assessment

Service Definition Document

Dark Web Exposure & Credential Leak Risk Assessment

Service Definition Document – G-Cloud 15

CONTENTS

SCOPE OF ACTIVITIES

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

Stage	Tasks
Information Gathering	Collect and review relevant information including: • Business profile • Domain names • Public IP Ranges • Email addresses • Current threat detection capabilities and coverage
Dark Web trawling & data exposure scanning	Run the Dark Web intelligence tools & processes to search for the following: • Leaked user credentials against business email domain and source identification of stealer malware • Dark web market transactions indicative of Ransomware campaign planning against the customer • Source IP address and ports generating dark web / TOR traffic in/out of customer infrastructure indicative of threat actor presence • Registration of domains indicative of Phishing campaign preparation or brand abuse • Social chats sharing nefarious intelligence on customer organisation and infrastructure • Network vulnerabilities including open ports, CVEs identified against attributes such as IP addresses, CIDRs and ASNs • Sensitive files found in publicly accessible cloud storage or repositories • High value keywords specific to the business that are found in public code repositories such as GitHub • Identification of file, domain and network attributes that have been identified on VirusTotal.
Findings Analysis	• Assess & categorise exposures based on potential impact specific to the client profile • Extended review on the most critical threats

SCOPE OF DELIVERABLES

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

Output	Description
Risk Report	• Outline of all identified threats and exposures • Extended commentary on the most critical threats • Actionable recommendations and remediation strategies
Findings Presentation	• Structured session to brief key stakeholders on findings summary and handle any clarification requirements

SERVICE OUTCOMES

- Early warning of Dark Web, Perimeter Vulnerability, and Leaked Data threat exposure to enable proactive mitigation before threats escalate
- Establishes confidence with supply chain partners through demonstration of proactive mitigation
- Support compliance efforts in adopting assertive approach to threat monitoring and response capabilities
- Ensure external cyber risk is minimised to support Business Continuity & Disaster Recover and Cyber Insurance activities