Vulnerability Scanning and Management

Service Description for G-Cloud 15

zenzero

Document Purpose

This is document serves as a high-level description of our vulnerability scanning and management service.

The aim is to describe, in simple terms, the service, the deliverables of the service and the associated benefits. This is described in a non-technical and vendor agnostic way.

More detail can be provided when engaging with our team so that we can understand your specific requirements.

For more information:

- Please visit: IT Support, Security, Data and AI Solutions | Zenzero
- Phone: 0333 3209 900
- Email: Hello@Zenzero.co.uk

Scope of Service

Introduction

Each month there's an endless parade of vulnerabilities, with the next exploit being classified as more critical than the previous one. Continuously identifying the seemingly endless stream of vulnerabilities, reacting to them and managing emerging vulnerabilities are challenges that most businesses are trying to figure out how to solve.

Apart from simply applying patches, businesses need to also be aware of the zero-day vulnerabilities that are continuously being identified. With a lag time in-between discovery and remediation, organisations need to have robust controls that allow them to rapidly identify affected systems and implement mitigating controls in the interim, until a patch is released.

Vulnerability scanning and exposure assessment shouldn't be a one-off, annual activity. Similarly, remediation shouldn't be limited to ad-hoc patching of systems. Continuous vulnerability management plays a key role in a well-functioning cyber security strategy by covering a variety of compliance requirements and protecting the business from the legal and reputational risks associated with a security incident.

Service Features

Our comprehensive assurance service includes vulnerability scanning (internal, external, network, application and agent based), simulated email phishing assessments, patch management, security awareness training and dark web monitoring. It offers ongoing assurance, identifies potential security weaknesses and threats across assets and provides actionable remediation advice

Our vulnerability scanning solution offers easy deployment for both external and internal network, web application, and agent-based scanning. Designed to identify potential security weaknesses and threats across a wide array of assets, it provides actionable remediation advice. With seamless integration into existing infrastructure, it ensures comprehensive coverage and effective risk mitigation strategies. Includes options for 3rd party patch management to allow for quick and efficient remediation of identified issues.

Where necessary we're also able to deploy under a hybrid model, with on-premise network scanners and endpoint agents to provide greater visibility and flexibility of scans. Through our mature onboarding process, the vulnerability scanning platform can be easily deployed with little impact to our clients' operations teams, giving additional insights into the array of hardware, software and cloud-based applications in use at any given moment.

By performing regular scans, our team can quickly identify vulnerabilities and provide a clear picture of what's in your environment and what needs to be addressed. This allows businesses to root out rogue assets before

they become a threat. Zenzero SOC analysts are uniquely equipped to interrogate your vulnerability data to provide more meaningful insights.

Service Level Agreements

Our standard agreed service levels are included in the table below:

Incident Priority	Business Impact	Target Response	Business Hours
Critical – P1	Very high impact in all business areas, extreme impact on users and disruption is excessive. Possibility of a security breach. Major incident. Possible financial implications, loss of company or user data at risk. Possible ICO implications or Pii / Pfi data loss possible	1 Hour	24/7
Standard – P2	Medium impact, security alarm has been triggered and is not a false positive. There is a medium risk to the business.	4 Hours	Working Day 9-5
Low – P3	The risk to the business from the security alarm is low or minimal.	Next Business Day	Working Day 9-5

Next steps

Speak with a member of our team to build an Vulnerability Management service that works for you using the phone number and email address above. Or you can use our website to book a consultation.

Pricing

Service Tier	0 -250 IP's	250 - 1000 IP's
Managed Vulnerability Scanning*	£7,220.00	£9,450.00

*Pricing is shown as annual billing. Bespoke pricing and deviation from standard service delivery will require price adjustments to be scoped, size and quoted.