REPLY

IDENTITY AND ACCESS MANAGEMENT (IDAM)

Service Definition
G-Cloud 15

REPLY
38 Grosvenor Gardens - London SW1W 0EB - United Kingdom - tel +44 (0) 207 730 6000 - fax +44 (0) 207 259 8600
infouk@reply.com

www.reply.com

TABLE of CONTENTS

SERVICE DESCRIPTION

Reply provide comprehensive Vulnerability Management Services that includes internal & external vulnerability scanning, plus agent-based scanning for remote and cloud devices. Our service is to discover, assess and classify, and address vulnerabilities in the environment through remediation & mitigation. We use industry-leading vulnerability tools and our team will perform regular vulnerability scans, prioritize risks based on severity, provide detailed reports, and recommend remediation steps to enhance your organization's overall security posture.

Standard

Our Standard Package is tailored for vulnerability management solution that utilises a mix of custom tools and open-source tools such as OpenVAS, Burp, nuclei and ZAP. Key features of our Standard Package include:

- Perform scheduled vulnerability scans across systems, networks, and applications.
- Classify and assess security risks as per CVSS Threat Score.
- Prepare a rollout plan to remediate and mitigate critical and high risk vulnerabilities in the first 72 hours.
- Prepare a regular remediation plan to address and mitigate medium and other risk vulnerabilities.
- Provide detailed reports with actionable recommendations for remediation.

Enterprise:

We offer Enterprise Package with enterprise Vulnerability tools and provide access to the customer to the Dashboard and integrate with the Customer's ticketing system. Key features of our Enterprise Package include:

- Internal agent and external network scanning to assess vulnerabilities within the organization's network infrastructure.
- Automated Attack Surface Management (ASM) scans for continuous monitoring and comprehensive coverage.
- Customer Access to the Dashboard and access to the vulnerability scans data in real-time.
- Priority Emerging Threat Scans to prioritize mitigation efforts for critical vulnerabilities.
- Vulnerability remediation SLA timeframes to ensure timely resolution of identified vulnerabilities.

Features

- Internal and external network vulnerability scanning.
- Asset prioritization based on usage or role.
- Risk-based vulnerability prioritization.
- Continuous assessment of IT assets to find vulnerabilities.
- Monitors the vulnerability status of all endpoints, whether on-premises, off-premises, or in the cloud, in real-time.
- Comprehensive reporting and dashboard functionalities.
- Detect vulnerabilities and critical misconfigurations per CIS asset benchmarks.

Benefits

- Identification and classification of security vulnerabilities and weaknesses.
- Establishment of a best practice vulnerability management program for visibility of digital assets and network devices.
- Measurement of patch management process, reducing the risk of successful cyber attacks.
- Scheduled custom reporting and proactive identification of vulnerabilities, with prioritized remediation.

- Compliance with industry and regulatory benchmarks including PCI, NIST, SANS, ensuring adherence to best practices.

ONBOARDING

With our Vulnerability Management Service, we start with an initial consultation to understand our customer's needs and assess the IT infrastructure. Following this, we draft a service agreement that includes the service offering that covers the number of assets, vulnerability management plan and deliverables and the tools. After agreement, we conduct an initial vulnerability scan to establish a discovery of the assets and applications. Throughout the engagement, we provide ongoing support and assistance, including regular monitoring and reporting.

Offboarding

We have a comprehensive transition plan that outlines timelines and responsibilities to transition the service to the customer. We facilitate the transfer of all relevant data, assets and documents to the customer or their new service provider. Formal closure is through proper documentation, including termination of contract.

Access to Data

All client data will be securely stored within the client's infrastructure, ensuring continuous access. At least one member of the client organization will always maintain administrator-level access to any system, facilitating smooth transitions. Additionally, any data residing on our systems will be securely deleted after transfer has been verified, ensuring complete confidentiality and data integrity. Revoking Spike Reply's access will not disrupt client accessibility to the data in any way

SECURITY

Personnel Security

As a Specialist Cloud Service, the capability being offered is not limited to specific Impact levels (as it is not infrastructure, software or a platform) and can be used, subject to personal Security Clearance levels.

Reply consultants are mostly Security Cleared (SC), some have higher-level Developed Vetting (DV) clearances. We also have a pool of NPPV3 Consultants for Policing work. The majority of our work for both public and private sector clients is at IL2 but we work in the Official, Secret and Top-Secret domains.

Our hard and soft information security processes have been designed and approved by independent CESG CLAS accredited consultants.

Information Security

We are ISO27001, Cyber Essentials certified and our Quality Assurance processes are based upon and compliant with our ISO 9001 accreditation. Our Information Security processes are directly guided by our ISO27001 accreditation. We shall adhere to local information and other security policies and will apply local Security Operating Procedures (SyOPs) as may exist. If such do not exist we shall apply our own SyOPs.

Physical Security

The Main Reply Office (London, UK) is a Police Accredited Secure Facility (PASF) with access controls for each point of entry. All Laptops/Phones must be stored securely overnight. When working on a client-site our consultants adhere to client security policies.

TRAINING & KNOWLEDGE TRANSFER

Reply's training program is designed to equip clients with the knowledge and skills necessary to effectively utilize our solution/service. It includes comprehensive instruction tailored to the client's specific needs, covering various aspects of vulnerability management. This encompasses hands-on training sessions conducted by experienced trainers, as well as access to training materials, documentation, and resources for ongoing learning and support.

It is included in both the basic and enterprise packages, providing clients with instruction and support for vulnerability management. While the basic package offers standard training, additional sessions or customization can be negotiated as optional additions. The enterprise package includes an enhanced level of training, with more extensive sessions and advanced topics. Further customization or additional training is available based on the client's needs.

ORDERING AND INVOICING PROCESS

To begin the process, please contact glue.frameworks@reply.com with details of your organisation, role and high-level requirements.

Our Framework Manager will connect you to our experts and from here we will organise an introductory discussion to go into more detail and shape a proposed engagement that suits your needs.

We invoice for both fixed price and time and materials engagements one month in arrears. For fixed price engagements, this takes place upon completion of the deliverable(s), or in stages, if the size of the engagement is greater than £40,000 excluding VAT.

Payment terms are 30 days net of receipt of invoice.

CUSTOMER RESPONSIBILITIES

To ensure successful delivery, Reply requires active collaboration and engagement from the customer. This includes providing access to relevant systems, networks, and applications for vulnerability scanning and assessment. Additionally, we need timely provision of necessary information such as network diagrams, asset inventories, and configuration details to accurately scope the engagement and prioritize vulnerabilities. Clear communication of business objectives, risk tolerance, and compliance requirements is essential to align our services with the customer's goals effectively. Finally, ongoing feedback and support from the customer help us tailor our approach and deliver optimal results aligned with their expectations.

ABOUT REPLY

Reply is a company that specialises in Consulting, Systems Integration and Digital Services with a focus on the conception, design and implementation of solutions based on the new communication channels and digital media.

Reply partners with key industrial groups in defining and developing business models made possible by the new technological and communication paradigms such as Artificial Intelligence, Big Data, Cloud Computing, Digital Communication, the Internet of Things and Mobile and Social Networking. In so doing, it aims to optimise and integrate processes, applications and devices.

Reply's offer is aimed at fostering the success of its customers through the introduction of innovation along the whole economic digital chain. Given its knowledge of specific solutions and due to a consolidated experience, Reply addresses the main core issues of the various industrial sectors.

Through our network of specialist companies, Reply supports some of Europe's leading industrial groups in Telco & Media, Industry & Services, Banks & Insurance, and Public Administration to define and develop business models, suited to the new paradigms of Artificial Intelligence, Big Data, Cloud Computing, Digital Media and the Internet of Things.

We make innovation happen.

We started with a small team and a purpose: to help the digital revolution happen. Today, we are a team of more than 14,600 people in 16 different countries but we still have the same DNA, made up of agile, vertical task forces and an inner passion for innovation.

We are a decentralised network of specialised companies.

Among Replyers, you will find passionate geeks, visionary strategists, and creative minds, each with sharp skills in a specific business, who cooperate together and never stop learning from each other.

Make forward, act sustainably.

We know a sustainable future is possible and technology can be a strong asset to reach it. As leaders in digital transformation, we push for change and operate in full accordance with the highest ethical standards and with respect for the rights of future generations