Vulnerability Management Services

G-Cloud (Cloud Support Services)

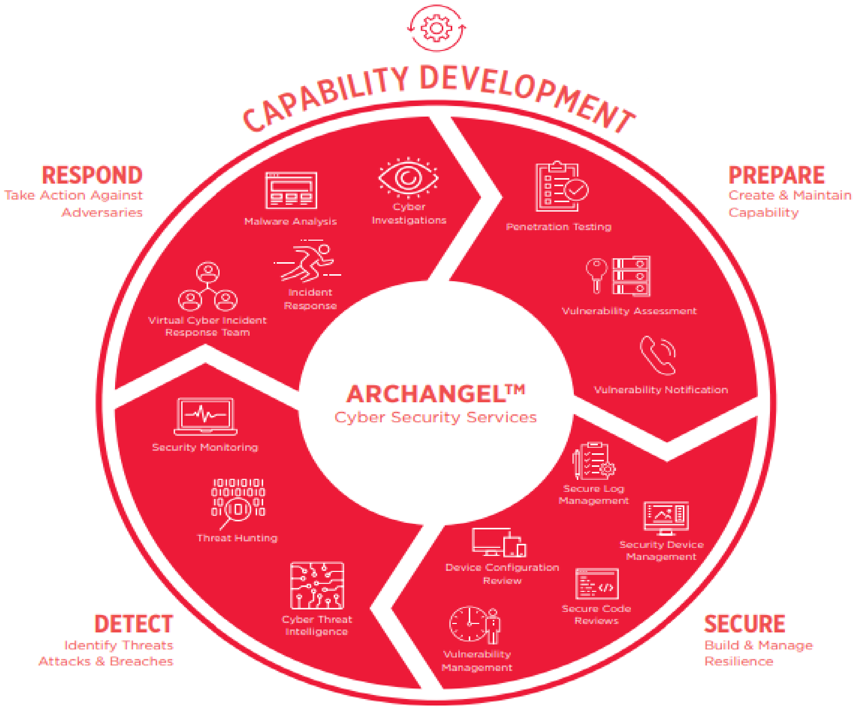
Service Definition Document

Leonardo UK Ltd
Registered Office: 1 Eagle Pl, St. James's, London SW1Y 6AF
Tel: +44 (0)117 988 0033   Fax: +44(0)117 988 0034

Table of Contents

1. Introduction

Leonardo MW (Leonardo) has a specialist Vulnerability Management Team that provides a complete portfolio of services surrounding Log collection to device vulnerability assessments. The services assume that every organisation is open to Digital reconnaissance and attack.



2. Service Overview

Enterprise networks are increasingly at risk of digital threats. To remain competitive in the digital age, organizations frequently introduce new hardware devices and software installations to their IT environments. However, these assets may suffer from vulnerabilities that, if left open, may be abused by attacker’s abuse to change a device’s configuration or make unauthorized modifications to some of an organization’s important files.

Either of these scenarios could help the bad actors establish an initial foothold on the network, access that they could then be leveraged to move laterally to other systems, remove important data, and overall cause additional harm.

Companies can leverage security configuration management (SCM) and file integrity monitoring (FIM) to address some of these risks and reduce their attack surface. However, organizations cannot hope to secure their infrastructure unless they have an accurate idea of what is happening and what happened in their environment.

To achieve that level of visibility, they must turn to Vulnerability Management; this is a security control, which addresses all system and network logs.

3. Secure Log Management

Each event in a network generates data, and that information then makes its way into the logs, records that are produced by operating systems, applications and other devices. Logs are crucial to security visibility. If organizations fail to collect, store, and analyse those records, they could open themselves to digital attacks.

Leonardo collect logs over encrypted channels. Our log management solution comes equipped with multiple means to collect logs. We should use agent-based collection whenever possible, as this method is more secure and reliable than its agentless counterparts. Once Leonardo have collected the Logs, we preserve, compress, encrypt, store, and archive a client’s logs, this can help clients meet their compliance requirements and ensure scalability.

Secure log management is designed to collect and store security logs from your infrastructure, usually in order to meet regulatory, compliance and audit activities. For example, complying with RIPA, GDPR & DPA.

3.1 What does it deliver?

- Fully managed secure on/off premises log storage
- Storage which is built and operated to industry good practice
- Delivered through ITIL V4 aligned processes
- Predefined solution for rapid on-boarding

3.2 How can it benefit you?

- Support of compliance requirements
- Support of legal and forensic investigations
- Assistance in reducing cost risks associated with poor security e.g. fines associated with breaches of compliance, legal fees or the price to your business of an incident occurring

3.3 How do we provide it?

The technology aspects of the service can be delivered via a range of options for example on-premise, off-premise, in the cloud or a hybrid of solutions. Software based log collection appliances are deployed on your sites. Logs are collected and then stored centrally on your chosen solution to maintain the level of integrity needed to achieve compliance audit requirements.

The service supports many common industry standards including PCI DSS, SOX, HIPAA / HITECH, NERC-CIP, FISMA and GLBA.

On client request, retained log sets can be restored and returned electronically to client site; small volumes using secure file transfers and larger volumes using encrypted storage devices via couriers.

Monthly reports are provided showing log volumes stored and deleted in a period along with a summary of any log access requests.

3.4 Sizing Drivers

- Events per Second:(EPS) – the rate data is ingested to the service
- Type and Number of data sources
- Retention time and type (online/offline)
- Type of Compliance

4. Vulnerability Assessment

Our Vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in organisations computer systems, applications and network infrastructures and providing the organisation the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Leonardo's vulnerability assessment provides an organization with information on the security weaknesses in its environment and provides direction on how to assess the risks associated with those weaknesses and evolving threats. This process offers the organisation a better understanding of its assets, security flaws and overall risk, reducing the likelihood that a cybercriminal will breach its systems and catch the business off guard.

Vulnerability assessments help you detect and manage external and internal vulnerabilities across your estate, giving you an opportunity you to manage your security risks and compliance objectives. The service offers one-off or managed vulnerability scans, which deliver reports detailing how to mitigate or manage identified or potential vulnerabilities.

4.1 What does it deliver?

- External vulnerability assessment of your public facing systems & networks
- Internal vulnerability assessment of your internal network and infrastructure.
- Vulnerability assessment testing and reporting
- Application and infrastructure vulnerability assessments
- On-premise and remote vulnerability scanning / assessment
- Cloud vulnerability assessment

4.2 How can it benefit you?

- Improved security posture – both external & internal
- Provision of an alternative independent approach to security assessment
- Identification of areas of risk where the cyber security posture can be improved

4.3 How do we provide it?

The service has flexible deployment options, for example we can deliver a single assessment of your public facing address space or multiple assessments which cover public facing and internal environments.

If delivered internally, a scanning agent will be deployed onto your network to provide vulnerability management of internal hosts which may not be directly accessible outside of your network.

4.4 Sizing Drivers

- Number of IP addresses
- Public or private IPs

5. Vulnerability Management Service

Our Vulnerability Management Service (VMS) is built on the need for organisations to develop capability across people; process and technology in order to build an effective vulnerability management program that forma a core component of an organisations security program.

Vulnerabilities emerge every day within new networks, web applications and databases. They may occur due to software defects or misconfigurations of information systems. Because cyber attackers can exploit them, it is essential to eliminate these exposures to protect your critical IT assets and safeguard sensitive information.

Vulnerability management supervises the process of remedial patch actions, in order to continuously assess vulnerabilities and protect your assets. A maintained inventory of assets is periodically checked against known vulnerabilities and a report of findings, including a prioritised list of vulnerabilities to address, is provided to you. This information can be used to guide effective patch management.

Our approach has four main components:

- Discovery - provides the ability to schedule and run either external or internal asset scans across your environment/s
- Assessment and prioritisation – assets are assigned an owner and criticality score based on business impact
- Remediation – helps to identify vulnerabilities and assigns them to your designated asset technical managers for review and remediation
- Assurance – scans can be scheduled to show the current state of assets, which delivers assurance that patching is being implemented effectively and risks are being managed

5.1 What does it deliver?

- External and Internal scanning
- Accurate and detailed vulnerability results
- Risk based approach toward vulnerability management
- Ability to track individual assets, and assign criticality and owners

5.2 How can it benefit you?

- Improvement of your resilience to cyber-threats
- Reduction of a large administrative overhead for your staff freeing them up for cyber security projects and continuous improvements
- Prioritisation of where to focus your patching effort

5.3 How do we provide it?

The service may be delivered either externally or internally to your environment. If delivered externally, this will be undertaken from an ARCHANGEL™ location. If delivered internally, a scanning agent will be deployed into your network to provide vulnerability management of internal hosts which may not be directly accessible outside of your network.

5.4 Sizing Drivers

- Number of IP addresses
- Public or private IPs
- Number of services
- Number of devices

6. Vulnerability Notification Service

Adversaries can exploit vulnerabilities in corporate systems to cause damage or disruption. Our vulnerability notification service gives you timely notifications of new vulnerabilities either generic or targeted, which relate to your deployed systems. The service collates and assesses information from varied intelligence feeds (open, commercial and our own proprietary research) in order to identify and alert you to new vulnerabilities in applications, services, operating systems and network equipment. With early warning, you can eliminate or manage the vulnerability to prevent it being exploited by an adversary.

6.1 What does it deliver?

- Vulnerability management to track and prioritise vendor updates/ patches according to your deployed technologies
- Service support for a comprehensive set of security technologies

6.2 How can it benefit you?

- Improvement in your resilience to cyber-threats
- Cost-effective solution which allows your staff to focus on securing your estate more effectively and efficiently

6.3 How do we provide it?

Notifications are delivered through security bulletins emailed to nominated contacts within your organisation

6.4 Sizing Drivers

- Generic or targeted bulletin
- Type and number of systems (applications, services, operating systems, network equipment)
- Type of vulnerability (standard CVE only or emerging threats detection)

END OF DOCUMENT