# CYBER SECURITY 101:
# VULNERABILITY MANAGEMENT

In today's fast-changing technology landscape, cyber security is more important that ever. Hackers and cyber criminals are constantly finding new ways to exploit vulnerabilities in our networks, devices and systems. To stay protected, it is crucial to have a solid understanding of how you can protect your security posture.

Whether you are a novice or an experienced security professional, our vulnerability management guide enables you to stay one step ahead of threat actors, by identifying where risk is present across your ecosystem, as well as highlighting the actions required to prioritise and remediate vulnerabilities.

# CONTENTS

# AN OVERVIEW OF VULNERABILITY MANAGEMENT

Vulnerability management refers to the process of identifying, prioritising, and mitigating vulnerabilities in an organisation's IT infrastructure, including networks, systems, applications, and databases. It also helps you discover hidden IT assets and identify vulnerabilities before cyber criminals do. It is a critical component of any organisation's cyber security strategy to protect against potential security breaches and minimise the risk of cyber attacks.

Every single organisation is riddled with vulnerabilities and a lack of identification and remediation can leave you vulnerable to costly cyber breaches. Regular patching is important but not enough and misconfigurations are common, including enabling insecure and outdated protocols – all of which can be identified by vulnerability scanning solutions.

An effective vulnerability management programme leverages threat intelligence and expertise in IT and business operations to determine the most critical risks and promptly address vulnerabilities. By prioritising the most severe vulnerabilities, and taking swift action to mitigate them, you can strengthen your security posture and reduce your risk of cyber attacks.

# VULNERABILITIES, RISKS AND THREATS – WHAT'S THE DIFFERENCE?

Vulnerabilities, risks and threats are related concepts; however, they refer to different aspects of the security landscape.

A vulnerability is a weakness or flaw within a system. A risk is the possibility of something bad happening, and a threat is the actor (thing or person) likely to cause damage or danger, such as exploiting a vulnerability to cause harm. Understanding the differences between these concepts is crucial for effective cyber security management, as it allows you to identify and prioritise vulnerabilities based on the potential risks and the threats that you face.

### Vulnerability

A vulnerability is a weakness or flaw in a system or application that could be exploited by an attacker to compromise the system's confidentiality, integrity, or availability. Vulnerabilities can exist in hardware, software, configurations, or human factors, and can be introduced at any stage of the system's lifecycle.

### Risk

Risk is the likelihood that a threat actor will take advantage of a vulnerability to cause damage to a system or organisation. Risk is typically expressed in terms of likelihood and impact.

### Threat

A threat is the actor, whether human or automated, that seeks to exploit a vulnerability to cause damage to an organisation or its assets. Threats can come from a variety of sources, including hackers, malicious insiders, or natural disasters.

# HOW ARE VULNERABILITIES RANKED AND CATEGORISED?

Vulnerabilities are ranked and categorised based on their severity, impact, and exploitability.

The Common Vulnerability Scoring System (CVSS) is commonly used to rank vulnerabilities on a scale from 0 to 10. The score is based on various factors such as the potential impact of the vulnerability, how easy it is to exploit, and whether a patch or workaround is available.

Vulnerabilities are also categorised based on their type, such as software, hardware, or configuration vulnerabilities. They can also be classified based on the attack vector, such as network-based, application-based, or physical-based attacks.

In addition to these rankings and categorisations, vulnerabilities may also be prioritised based on the likelihood of exploitation, the potential impact on the organisation, and the available resources to address the vulnerability.

**You can access a handy CVSS calculator** here.

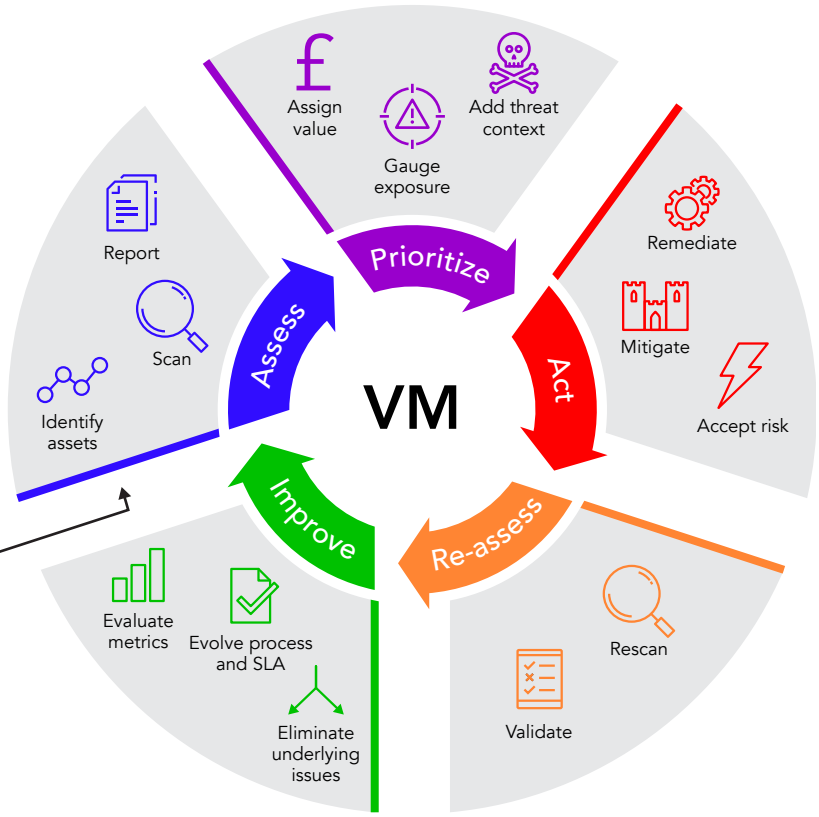
# THE VULNERABILITY MANAGEMENT LIFECYCLE

Gartner's Vulnerability Management Lifecycle is a framework that provides structured approach to identify, prioritise, and remediate vulnerabilities in your systems and networks.

### The Vulnerability Management Cycle

**Prework**

- Determine scope of program
- Define roles and responsibilities
- Select vulnerability assessment tools
- Create and refine policy and SLAs
- Identify asset context sources




Source: Gartner
ID: 410271

## Assess

The first step is to assess the current state of your organisation's attack surface by identifying and capturing a holistic inventory of all access points, including unidentified and unauthorised assets. This initial step is crucial in identifying which assets require protection and guarding against possible risks.

## Prioritise

The next step is to prioritise vulnerabilities that pose the most immediate risk based on factors such as location, blast radius, exploitability, and business impact. This prioritisation allows organisations to concentrate remediation efforts on the most critical vulnerabilities that require immediate attention.

## Act

This phase involves implementing patches or other mitigation measures to reduce the risk of an attack.

## Reassess

This phase involves validating the success of remediation efforts and leveraging technology to scale and improve the programme.

## Improve

The final step is to continuously improve the vulnerability management programme by measuring its effectiveness and identifying areas that could benefit from automation, or other process improvements.

By following this framework, you can implement a comprehensive vulnerability management program that helps to mitigate the risk of cyber attacks and ensure the security of your networks and systems.

# THE BENEFITS OF VULNERABILITY MANAGEMENT

The world we live in today is fraught with cyber threats, and the risk of cyber attacks is higher than ever. With the rise of remote work and the increasing sophistication of cyber criminals, it's no longer a matter of if, but when, an organisation will face a cyber attack.

1.

### Enhanced Security

By proactively identifying and addressing vulnerabilities, organisations can improve the security posture of their IT assets and reduce the risk of security breaches or data breaches.

2.

### Risk Reduction

Vulnerability management helps organisations prioritise vulnerabilities based on their severity and potential impact, allowing them to allocate resources efficiently to address the most critical risks.

3.

### Compliance and Regulatory Requirements

Many industries are subject to regulatory requirements that mandate regular vulnerability assessments and remediation. Implementing effective vulnerability management practices can help organisations meet these compliance requirements, avoid penalties, and maintain a good standing with regulatory agencies.

4.

### Cost Savings

Addressing vulnerabilities proactively can help organisations avoid the costs associated with security incidents, such as data breaches, system downtime, and reputational damage.

# THE COSTS ASSOCIATED WITH VULNERABILITY MANAGEMENT

**Like all investments, there are business costs to vulnerability management. However, the reward far outweighs the initial costs.**

1. **Initial Investment:** Acquiring and implementing vulnerability scanning tools, penetration testing services and other software or hardware. These costs will vary depending on the size and complexity of your organisation's IT environment.
2. **Ongoing Operational Costs:** Maintaining an effective vulnerability management program requires ongoing operational costs, such as staffing, training and software licensing. However, these costs are generally outweighed by the potential cost savings resulting from proactive vulnerability management.
3. **Remediating Vulnerabilities:** Fixing a vulnerability may be as simple as applying a patch or updating software, which can be done relatively quickly and at low cost. However, in other cases, fixing a vulnerability may require significant time and resources, such as rewriting code or replacing hardware, which can be much more expensive.

# WHAT TO LOOK FOR IN A VULNERABILITY MANAGEMENT TOOL

When considering a vulnerability management solution, there are several factors to consider. Here are some of the key things to look for:

**Comprehensive Coverage:** Look for a solution that can scan and identify vulnerabilities across all parts of your IT infrastructure, including on-premises, cloud, and mobile environments.

**Accuracy and Efficiency:** The solution should provide accurate information on vulnerabilities and prioritise them based on risk, allowing you to focus your remediation efforts where they are most needed.

**Integration:** The solution should integrate with your existing security tools, such as patch management and security information and event management (SIEM) systems, to streamline the vulnerability management process.

**Flexibility:** The solution should be flexible enough to accommodate your organisation's unique needs and workflows, allowing you to customise the scanning and remediation process to fit your specific environment.

**Reporting and Analytics:** The solution should provide detailed reporting and analytics, allowing you to track your progress over time and communicate your vulnerability management efforts to stakeholders.

**Automation:** The solution should offer automation features to help reduce the workload and improve efficiency, such as automated patch management and ticketing integration.

**Support and Services:** Look for a vendor that provides good customer support and services, including training, consulting, and technical support.

# MANAGEMENT OF A VULNERABILITY MANAGEMENT PLATFORM

Managing vulnerability management in-house can be a significant effort for businesses, especially for those with limited resources or expertise in cyber security. It involves continuously monitoring and assessing the security of your network, systems, and applications, identifying vulnerabilities, and prioritising and addressing them in a timely manner. This process can be time-consuming and requires specialised knowledge and tools.

By outsourcing this function to a Managed Service Provider (MSP) such as Daisy, you can offload this responsibility to a third-party expert with the necessary resources and expertise. The provider can help you stay up-to-date with the latest threats and vulnerabilities, provide real-time monitoring, and help prioritise and remediate vulnerabilities quickly and efficiently.

This can save you time and resources and provide a higher level of protection against cyber threats. Additionally, managed vulnerability management providers can offer further services such as compliance management and reporting, which can help you to meet your regulatory requirements and demonstrate your commitment to cyber security.

# HOW CAN DAISY HELP?

Overall, the right vulnerability management solution can help you reduce risk, improve your security posture, and ensure compliance with industry regulations. By considering these factors when evaluating solutions, you can find the best-fit solution for your organisation's needs.

Developing a true vulnerability management program requires time and resources to prioritise what's most critical in the context of your business. Daisy's Vulnerability Management service can ease the burden through leveraging the extensive knowledge and experience of the highly skilled experts within the Daisy Security Operations Centre to proactively highlight vulnerabilities, evaluating what should be prioritised and identifying the corrective actions required to maintain an enhanced security posture and ensure compliance.

For more information our specialists are on hand:

Call: **0344 863 3000**

Email: **enquiry@daisyuk.tech**