

GUIDE


Your Guide to Patching and Vulnerability Management for Cyber Essentials Success




INTRODUCTION

By obtaining Cyber Essentials certification, organisations demonstrate their commitment to implementing fundamental cyber security controls and safeguarding sensitive information. This comes with a range of benefits including the opportunity to bid for government contracts, reduce insurance premiums, a better understanding of your cyber security and increased credibility with stakeholders. The problem is organisations often feel that there are obstacles in their way, stopping them from achieving Cyber Essentials and Cyber Essentials Plus.

In our experience, patching is the primary issue for organisations trying to achieve Cyber Essentials.



Only 31% of organisations have a policy in place to apply software security updates within 14 days

 DATACONNECT Gov UK: Cyber Security Breaches Survey 2024

The statistic above emphasises just how much organisations struggle with this one aspect of the certification process.

Within the Cyber Essentials question set, patch management is included in the section 'security update management' which states:

"You must install all high and critical security updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question."

To have effective patch management, you need to have a vulnerability management regime also in place. Like the debate of what came first, the chicken or the egg, there's been many discussions about which one an organisation should implement first and what is more important. To fully understand this debate, you need to know the difference:

Patch Management:

Patch management is the process of identifying, acquiring, testing, and installing patches or updates to systems and applications to address known vulnerabilities. It focuses on ensuring that all software is up to date with the latest security patches to protect against potential threats.

Vulnerability Management:

On the other hand, vulnerability management (VM) involves the continuous process of identifying, prioritising, and addressing vulnerabilities in systems and applications. It goes beyond just patching and includes activities such as vulnerability scanning, risk assessment and remediation to enhance your overall cyber security posture.

The **key difference between patch management and vulnerability management lies in their scope and approach. Patch management is more focused on applying patches to known vulnerabilities, whilst vulnerability management takes a broader view of identifying and addressing all security gaps affecting the organisation. Also, VM can be used to further verify that you are finding all patches within your patch management regime and vice versa. Organisations must effectively integrate both practices to enhance their overall cyber security.**

The Cornerstone of Vulnerability Management

A successful vulnerability management regime involves several moving parts and the constant barrage of new risks is often overwhelming to IT teams. Due to this, there is a need for ongoing resource, time and effort. However, with a comprehensive vulnerability management regime, you'll not only be more secure but confidently meeting the Cyber Essentials requirements.

To get started, here are **three areas that need to be considered when creating your vulnerability management plan.**

Visibility

You can't fix what you can't see. Comprehensive coverage is essential for effective vulnerability management. The ability to see all assets on and off the network, as well as the types of vulnerabilities is imperative. When selecting a vulnerability management service or tool, this factor should be a driving force for your decision.

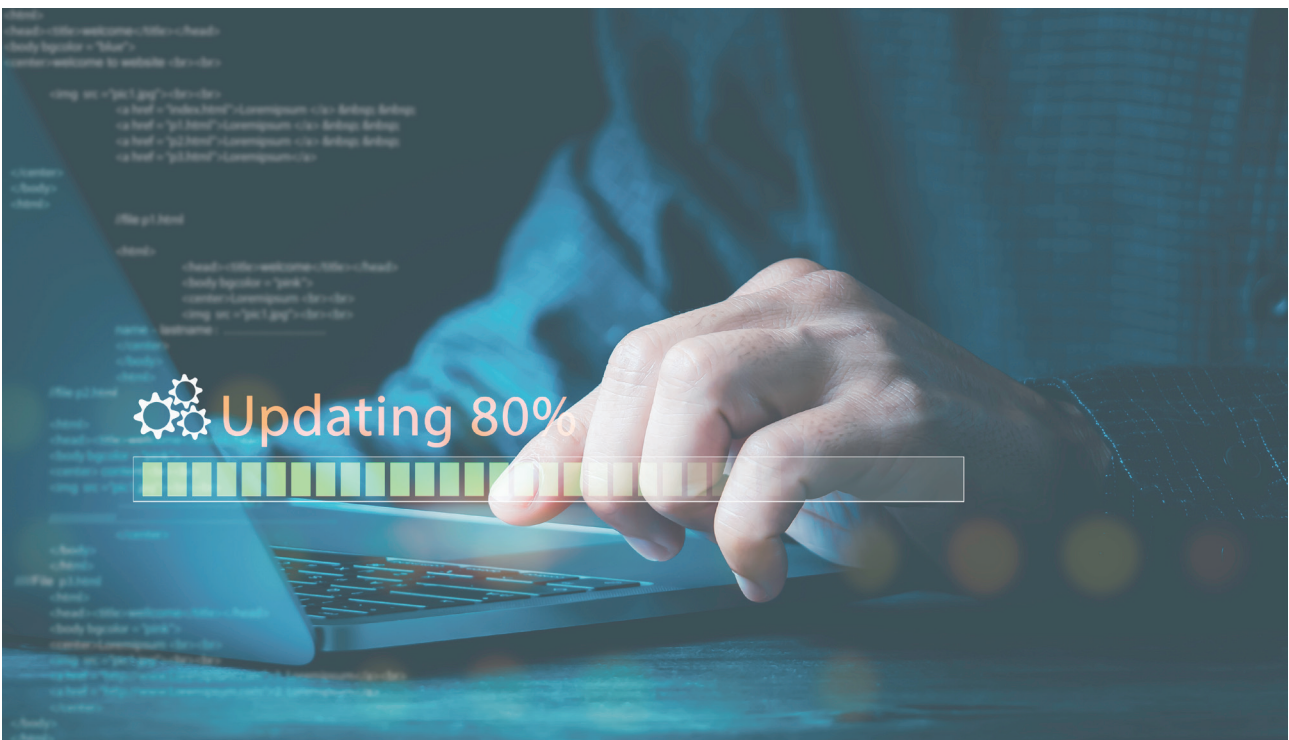


Management

Vulnerability management is a daunting task for many IT teams as there are a lot of factors that must be taken into account, including:

- Software / hardware vulnerabilities
- Misconfigurations
- End of life assets
- How to prioritise remediations
- Who's responsible for what
- The acceptance of risk and how to handle false positives

Knowing where to start and not feeling overwhelmed with the amount of elements that need to be considered is hard. However, with careful planning and time, this should become simpler. It's important to consider how vulnerability management can be matured and where ongoing developments are possible. To watch a video on the Vulnerability Management Maturity Model, [please click here.](#)



Prioritisation

Prioritisation often is bespoke to your organisation's specific circumstances and attack surface. Without the right tools and procedures, this can be drastically time consuming.

A risk-based approach allows you to focus on addressing the most critical risks first, ensuring that your resources are allocated where they are most needed. Linking back to the Cyber Essentials scheme, it states that a vulnerability marked as high or critical severity must be remediated within 14 days to meet the scheme's requirements.

The **Common Vulnerability Scoring System (CVSS)** is internationally recognised and the most common method used for evaluating vulnerability severity. Each vulnerability is checked against a set criteria to be given a score. We recently created a video explaining the scoring system, [click here to watch](#).

There are other methods too that can be considered when remediating vulnerabilities for example, a laptop used daily by your finance team is a higher priority than a laptop that is used occasionally by lesser privileged users.

In reference to the first factor mentioned, the key is to have a system that is providing current and consistent visibility. This helps ensure a structured and methodical approach where your prioritisation is still up to date.

Achieving Cyber Essentials

By achieving Cyber Essentials certification, businesses demonstrate their commitment to protecting sensitive information and guarding against cyber threats. This certification not only enhances your business opportunities but also gives current clients, stakeholders and your supply chain peace of mind knowing that you take cyber security seriously.

As we wrap up our discussion on patching and vulnerability management, it's clear to see how IT teams can find this to be a daunting task. However, by considering the cornerstones described above, this should give you and your team a solid foundation to start your vulnerability management plan.

Remember, patching and vulnerability management play a vital role in maintaining a strong cyber security posture. By regularly updating software and systems, businesses can close security gaps and reduce the risk of falling victim to cyber attacks. This proactive approach can save companies from costly data breaches and reputational damage in the long run.

With that said, the CEO of the National Cyber Security Centre announced that obtaining Cyber Essentials can decrease the likelihood of a cyber insurance claim by 80%

START YOUR CERTIFICATION JOURNEY TODAY

(vSOC CERT)

Cyber Essentials Review Toolkit

Streamline your certification process each year with the Cyber Essentials Review Toolkit (CERT). Plus, easily view which vulnerabilities are making you non-compliant including severity scores and step-by-step remedial actions.

- + Cyber Essentials subscription service
- + Access the right technology, consultancy and support
- + Full visibility with the vSOC Connect Console
- + Easily stay compliant and secure throughout the year.
- + Simplify Cyber Essentials recertification

[FIND OUT MORE](#)



DATACONNECT

CYBER SECURITY - CONSULTANCY | SERVICES | TECHNOLOGY

 01423 425 498  dataconnect.co.uk  moreinfo@dataconnect.co.uk