The importance of a vulnerability scan.

Any organization conducting business over -- or even just connected to -- the internet is in jeopardy of a network-based attack stemming from a vulnerability within a connected system. Every day new vulnerabilities are announced by hardware and software vendors. Vulnerabilities are errors in the code that make up the operating system or application you are using that criminals exploit to get access into your systems. Once in they can steal your data or encrypt your informations systems for ransom. Regular vulnerability scanning and patching of systems is essential to protect your organization from being breached.

Patch management is a requirement of the **Cyber Essentials Plus infrastructure requirements and IASME GDPR Patch Management requirements.**

- All software kept up to date with an up to date support and license agreement.
- All unsupported or unlicensed software removed from devices.
- All software patched within 14 days of an update being released with a severity level of critical or high risk.

IASME/GDPR Patch Management

Questions in this section apply to: Servers, Computers, Laptops, Tablets, Mobile Phones, Routers and Firewalls.

Q 122. Are all operating systems and firmware on your devices supported by a supplier that Produces regular fixes for any security problems? Please list any operating systems that are not supported.

Q 123. Are all applications on your devices supported by a supplier that produces regular fixes for Any security problems? Please list any applications that are note supported.

Q 124. Is all software licensed in accordance with the publisher's recommendations?

Q 125. Are all high-risk or critical security updates for operating systems and firmware installed Within 14 days of release? Describe how do you achieve this.

Q 126. Are all high-risk or critical security updates for applications (including any associated files And any plugins such as Adobe Flash installed within 14 days of release? Describe how you achieve this.

Q 127. Have you remove any applications on your devices that are no longer supported and no Longer received regular fixes for security problems?

Vulnerability scanning should happen on a frequent basis. The frequency at which vulnerability scans are performed is determined by the organization's risk appetite and any applicable regulatory requirements. It is recommend at least quarterly scans as part of a robust program. The reason being that a single vulnerability scan each year puts companies at risk of not uncovering new vulnerabilities for an extended time period. This period of limbo is all an attacker needs to compromise a network.

There are a lot of vulnerability scanning tools but CySure uses Qualys. Qualys covers all operating systems and applications using the US Governments Security Content Automation Protocol (SCAP) linked to the National Vulnerabilty Database (NVD). The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

CySure provides the lowest cost vulnerability scanning on the market. See the following link for pricing

https://www.scmagazine.com/penetration-testing-vulnerability-assessment-risk-assessment/products/6530/6/