secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Build Configuration Security Review

Build Configuration Security Reviews can provide system administrators with a comprehensive overview of the security of their assets, whereby the local policies and settings of a device are examined to assess their security implications.

Who Is It For?

Build configuration reviews can assess server builds, end user device builds, or standardised images used for deploying systems (commonly known as "gold images") for security issues and to review their level of security hardening.

Therefore, most organisations would benefit from a Build Configuration Security Review to ensure their servers and end user devices are as secure as they should be.

How Can We Help?

This form of assessment is not intended to be representative of a real-world threat, but instead a transparent approach to allow you to gain an understanding of the security-related configurations, and how this may hinder defence-in-depth.

We review the security configuration of devices and give guidance on how systems can be reconfigured to make them more resilient to attacks, including remote attacks, local network attacks, and insider threats.

What We Test

We assess all aspects of the device configuration; some commonly assessed areas include:

- **Local Configuration** - The local configuration considers hardening options available on the operating system and device. Such as registry keys, file-system permissions, and BIOS settings.
- **Domain Configuration** - The domain configuration includes any policies or configurations applied as a result of being a domain-joined asset, such as group policy and account lockout options.
- **Network Configuration** - The network configuration includes any policies or configurations which impact the security of the asset from the local-area network such as host firewall configuration and protocols such as NetBIOS.
- **Software Configuration** - The software configuration includes any software installed on the host which may impact the security of the asset such as outdated browsers, office packages, and protections such as Anti-virus.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

Our Build Configuration Security Review takes into account best practice guidance from operating system vendors, and information from the Centre for Internet Security, as well as experience from our penetration testing team. A list of the major testing categories we will perform is outlined below:

LOCAL CONFIGURATION

This takes into account the settings on the host operating system and the device itself, such as:

Local Users - Just like domain users, local users should be configured with an appropriate account lockout configuration to reduce the risk of bruteforce attacks.

Security options such as Local Administrator Password Solution (LAPS) should be deployed to mitigate the risk of administrator password reuse.

File-System Permissions - Should be configured so that users can't write to sensitive areas of the disk, such as where services executables are stored, and that users cannot access other users' files.

Services - These should be hardened to common privilege escalation attacks, by having restrictive permissions on who can reconfigure services.

The BIOS and hardware configuration should prevent users from booting unauthorised operating systems or disabling security features.

Disks Encryption - Deployed to prevent loss of data in the event that a device is lost or stolen.

DOMAIN CONFIGURATION

The domain configuration is assessed to ensure that hardening options around user accounts, such as secure passwords and account lockout are applied.

Group Policy - Configurations are assessed to ensure that devices are locked down to prevent users from accessing system areas and functionality that they do not require as part of their role.

NETWORK CONFIGURATION

The network configuration includes any policies or configurations which impact the security of the asset from the local-area network.

Host Firewalling - Assessed to ensure the device is protected from common network attacks and to ensure that unnecessary network services are restricted.

Proxy and Filtering Controls - Assessed to ensure that users cannot access potentially malicious websites, that the devices are protected from common and sophisticated phishing attacks, and that simple bypasses are not possible.

SOFTWARE CONFIGURATION

The software configuration is assessed including system updates and updates for third third-party software as well as to ensure that end-point protection is installed.

Software Updates - Many organisations have rigorous processes in place to ensure that operating system patches are installed, but these often do not take into account common software such as web browsers, office packages, and software such as remote collaboration tools.

End-Point Protection - This software is also assessed to ensure the device is protected from common threats such as malicious software and that the end-point protection cannot be trivially disabled or bypassed.