Build and Configuration Reviews

Build and configuration reviews help ensure that corporate system builds for servers, workstations, laptops, and other network infrastructure are configured securely and in line with security best practices and standards.

It is important to have robust and secure standardized builds that are consistently deployed, as this provides assurance that business-critical systems are protected from both a network and a local perspective.

Insecurely configured environments can allow malicious users to obtain unauthorized access, and if a standard build containing weaknesses is deployed across hundreds or thousands of servers, the impact can be significant.

After a review, we will provide you with a detailed report stating the associated risks to your business as well as recommendations for remedial actions. This helps to ensure that your IT assets are aligned to the latest industry and vendor guidance and thus hardened against attack.

Desktop and server builds

We can carry out desktop and server build reviews to rectify flaws in an organization's processes that could be contributing to security problems. Context has a range of experience in reviewing the configuration of desktop and server builds against industry good practices and vendor guidelines.

We will review the system configuration settings to identify security weaknesses and deviations from good practice. These are based around assessments of system security; registry security and permissions; and running services and user account configuration.*

The following areas are typically covered:

—Patching and update
—User management, password and login policy
—Filesystem permissions and configuration
—Networking configuration and hardening
—System architecture and purpose
—Privilege escalation
—Installed software
—Physical access
—Resource management
—Logging and auditing

Application servers

We are able to review the configuration of a wide range of application servers, including common web servers, database servers, application servers and virtualization technologies, as well as their underlying operating systems.*

Examples of application servers we can review:

—SQL Server
—MySQL
—Oracle
—Apache httpd
—Nginx
—Apache Tomcat
—WebSphere
—ESXi
—OpenVZ
—Citrix
—Active Directory
—Exchange
—SCCM
—Sharepoint
—IIS

**The checks are aligned to the configuration benchmarks produced by the Center for Internet Security (CIS), and supplemented by Context's proprietary data collection tools and methodologies.*

Build and Configuration Reviews

Firewalls and network devices

Many organizations have come to rely on firewalls and network devices as a keystone of their defenses, so it is important to ensure that they are fit for purpose and delivering optimum performance.

Context has developed a tried-and-tested methodology for reviewing the configuration and rules of firewalls and network devices such as switches, load balancers and security appliances.

Our testing is designed to identify security vulnerabilities, such as failure to achieve best practice, or instances of incorrect firewall configuration. This typically involves configuration and password auditing, access control list analysis and device patching.

Typical vulnerability types discovered during reviews include insecure access points, services and encryption methods, inadequate or no logging or overly permissive rules that enable too great a degree of access between hosts via various protocols.

Context review devices from mainstream vendors such as:

—Cisco
—Check Point
—F5
—Juniper
—Blue Cat
—Palo Alto

Mobile devices

Mobile devices are increasingly used by employees within organizations to access sensitive enterprise data. As a result it is vital that these devices are secure. This can be achieved by having a robust Mobile Device Management (MDM) solution to manage all devices that have access to enterprise resources.

Context can perform security reviews to assess your deployed MDM solution configuration, the supporting network architecture, as well as the mobile device security policies and management processes.

The assessment is performed via hands-on reviews of the MDM configuration, paper-based review of the design documentation and policy documents as required, as well as conversations with key technical operators. The reviews are aligned to both security best practices and documented policies.

We can also test the relevant mobile devices to verify that the deployed policy and configuration options provide expected security. This provides assurance that corporate MDM systems and BYOD set-ups are secure and that risks relating to lost or stolen devices and data are mitigated.

At Context we can:

—Provide pre-testing consultancy to develop a secure MDM deployment strategy
—Review the internal policies of an MDM solution
—Review deployed MDM policies and policy implementation
—Assess external and internal infractructures of cloud and on premise MDM deployments
—Assess builds of servers and networking components involved in an MDM deployment
—Assess the security of applications deployed by MDM solutions

context