CyStack

DATA SHEET

Internal Network Audit

Securing your network from the inside out

Overview

An internal network security audit is an assessment of an organization's network infrastructure and security controls to identify vulnerabilities and ensure compliance with security policies and industry regulations. The audit typically includes evaluations of network architecture, access controls, data security, and incident response processes.

The main goal of an internal network security audit is to identify and mitigate potential security risks to an organization's network infrastructure. This includes identifying vulnerabilities in the network's architecture and configuration, assessing the effectiveness of security controls, and evaluating the organization's compliance with security policies and industry regulations.

The audit can also help organizations to:

- Detect any malicious activity or breaches of security that may have already occurred.
- Evaluate the readiness of incident response processes.
- Verify the network's compliance with data protection laws and regulations.
- Ensure the security of sensitive data stored on the network.
- Improve overall security posture.
- Provide a baseline for ongoing monitoring and improvement.

It is important to note that the goal of an internal security audit is not to "hack" or "penetrate" the network, but to identify potential vulnerabilities and recommend solutions to improve security.

Customer Benefits

- Strengthen the security of the internal network
- Ensure compliance with industry standards and regulations
- Understand and manage security risks more effectively
- Develop a better governance model and make a more robust risk management strategy
- Has an independent third-party validation of the internal network security posture

How CyStack Helps

The CyStack Audit Team is a group of highly skilled security testers who use a goal-oriented approach to testing, refined through years of experience and extensive testing. Our team members have a unique blend of infrastructure building and security testing expertise, enabling them to conduct comprehensive security evaluations that uncover potential risks for organizations. Members of this team are also regular speakers at world-known cyber security conferences and also talented bug hunters who discovered many critical vulnerabilities in the products and are acknowledged in the Hall of Fame of global tech giants such as IBM, HP, Microsoft, Sea Group, Alibaba, etc.

The team can perform a review of the business's internal network, including servers, networks, and storage, as well as the architecture of the systems and how they are configured to identify any vulnerabilities or misconfigurations that could be exploited by attackers. They will also review the security settings and configurations of the internal networks and applications to ensure they are properly configured, including checking for proper encryption, access controls, and network security.

Methodology

CyStack Internal Security Audit typically involves:

1. **Network architecture review**: This service will involve assessing the organization's network architecture and identifying any vulnerabilities that could be exploited by attackers. This can include evaluating the use of firewalls, intrusion detection and prevention systems, and other security devices.
2. **Access controls review**: This service will assess the effectiveness of the organization's access controls, such as authentication and authorization mechanisms, and identify any potential weaknesses.
3. **Data security review**: This service will review the organization's data security measures and assess the confidentiality, integrity, and availability of sensitive data stored on the network.
4. **Incident response review**: This service will evaluate the organization's incident response processes and assess their effectiveness in detecting and responding to security incidents.
5. **Compliance review**: This service will review the organization's compliance with relevant security policies, standards, and regulations.
6. **Provide a comprehensive report** that summarizes the findings of the audit and provides recommendations for improvement.

CyStack also provides additional support such as remediation guidance, security training, and ongoing monitoring and management.

During an internal network security audit, the specific targets or objects that will be tested will depend on the scope of the audit. The scope refers to the specific areas of the network infrastructure and security controls that will be assessed. The targets that will be tested may include:

1. **Network devices**: such as routers, switches, and firewalls, as well as wireless access points and other networking equipment.
2. **Servers**: including web servers, database servers, and other types of servers.
3. **Endpoints**: such as laptops, workstations, and mobile devices, including operating systems, software, and applications.
4. **Cloud infrastructure**: such as IaaS, PaaS, and SaaS, if any.
5. **Remote access**: such as virtual private network (VPN) connections, Remote Desktop Protocol (RDP), and other remote access solutions.
6. **Network services and protocols**: such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and other services and protocols that are used to support network operations.
7. **Access control mechanisms**: such as authentication and authorization protocols, multi-factor authentication, and user access rights.
8. **Data security measures**: such as data encryption, data backups, and data loss prevention.
9. **Incident response processes**: such as incident detection and response, incident handling procedures, and communication protocols.
10. **Compliance**: with relevant security policies, standards, and regulations such as HIPAA, PCI-DSS, and SOC2.

Key Features

- Gain assurance that your infrastructure is secure
- Review comprehensively infrastructure including configurations, architecture, policies, and procedures
- Manage, track, prioritize and remediate the findings in CyStack Vulnerability Management Platform
- Receive actionable recommendations to enhance security
- Reduce your risks and improve operational efficiency

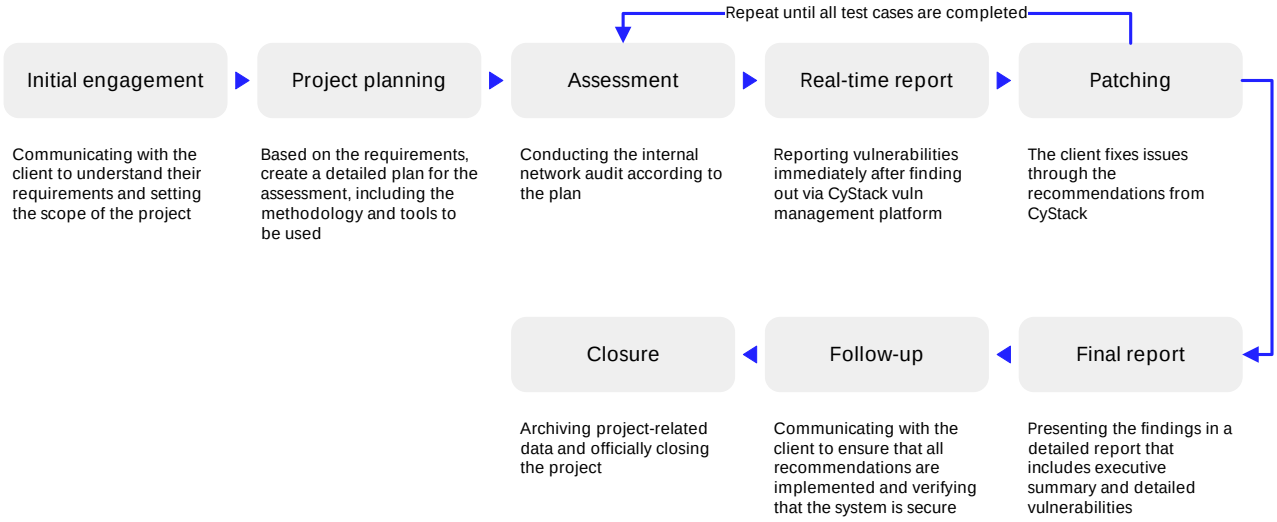
Standards

When conducting an internal network security audit, CyStack uses various industry standards and best practices to guide the assessment. The specific standards used by CyStack may depend on the specific needs and requirements of their clients, as well as the industry or regulatory environment in which they operate. Some common standards that may be used include:

- **NIST SP 800-53**: This standard provides guidelines for security controls for federal information systems, and is often used as a framework for internal network security audits.
- **ISO/IEC 27001**: This international standard provides a framework for the management of information security and is widely adopted by organizations worldwide.
- **PCI DSS**: The Payment Card Industry Data Security Standard provides a framework for securing credit card transactions and is a requirement for any organization that processes, stores or transmits credit card information.
- **SOC 2**: The Service Organization Control 2 report provides a framework for assessing the security, availability, processing integrity, confidentiality, and privacy of a service organization's system.
- **OWASP**: The Open Web Application Security Project provides a set of guidelines and best practices for securing web applications.

CyStack also uses additional standards and best practices such as OWASP Top 10, CIS Critical Security Control, and our own audit framework. It's also important to note that besides using industry standards, we will take into consideration the organizational policies and regulations that the company must comply with. And it would be ideal to align the audit with the specific goals and objectives of the organization.

Flow To Work With Clients



About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net