# Security Health Check Services

## Do You Know Where You Are Susceptible to Attack or Exploitation?

### What Is a Security Health Check?

Today we are faced with a high-threat world, where cybercriminals and state-sponsored entities are constantly targeting U.S. organizations. In order to identify whether your enterprise is at risk of attack from the outside, as well as identify if your internal infrastructure is at risk from attack or insider threat, you must perform a series of comprehensive technical security analyses as well as a policy and configuration review to measure, document, and validate your risk management strategy. The testing and analysis includes:

- External penetration testing (ethical hacking)
- Wireless security penetration testing
- Social engineering and phishing assessments
- Firewall auditing
- Routing/switching configuration reviews and security evaluation
- Server and domain evaluation
- Internal network security testing
- Organizational and policy audits

This testing must be conducted periodically to ensure your security IT and security management practices meet performance requirements over time. Our experts are ready to help. Connection is your trusted partner in identifying, documenting, and planning a prioritized remediation strategy to address your security risk.

### We Offer Two Types of Ethical Hacking

In order to determine your organization's resiliency to external Internet-based attacks, you must periodically perform the same types of attacks that the cybercriminal performs daily. This testing will determine if you are susceptible to exploitation by these criminals.

- **Black Hat Testing:** You provide only minimal information to Connection. Typically only the target IP addresses are given, with no supporting information. You are not required to make any adjustments to your security infrastructure to accommodate the testing (true hacker approach).
- **Gray Hat Testing:** You provide Connection with detailed information about targets. For example, you may provide a target, function, operating system, and other useful information. Your organization also allows scanning through your perimeter security infrastructure.

### Wireless Penetration Testing

With the growth of mobile computing, wireless networks, and always–on connectivity in our hyper-connected world, it is critical to know if your wireless infrastructure is at risk of compromise. A Wireless Security Assessment determines if your wireless infrastructure is configured appropriately to meet your critical needs, while enforcing your security policies and controls. As part of our Wireless Penetration Testing, Connection's security experts will attempt unauthorized access to your wireless network. This will provide a complete risk profile for your wireless access points and infrastructure, including appropriate coverage, secure access and authentication controls, proper segmentation between guest and corporate networks, and proper controls for secure application and data access.

### Phishing and Social Engineering Testing

Phishing, vishing (voice phishing), and social engineering analysis is a collection of techniques used to test your employees' security education and susceptibility to social engineering tactics that might influence them to perform certain actions or divulge confidential information. Users have a responsibility to help protect sensitive and proprietary information, and we can provide a report card on how well your team is doing to protect against this constant real-world threat.

Our services will:

- Find out what percentage of your staff clicks on HTML links in email messages
- Test employees to determine if they enter information on a fake website
- Perform safe malware phishing experiments to determine the effectiveness of your filters
- Test employees to determine their effectiveness and awareness of social engineering attacks over the phone

Our assessment emulates the approach used by hackers because we manually perform a controlled, real-world attack on your users and measure their response and actions.

*Continued* 〉

### Firewall Audit

Firewalls are traditionally the first area of defense for your network. Are your firewalls providing you the best level of protection possible? Are your rules clear, concise, and consistent across all of your firewalls? Are you utilizing best performance practices, such as high availability? Our experts can perform a Firewall Audit to help ensure you do not have any configuration flaws that will invite hackers to penetrate your network.

### Routing/Switching Configuration and Security Evaluation

As with firewalls, your routing and switching fabric can allow an attacker to penetrate your network. Connection's Security Practice can identify and evaluate the current design, utilization, and configuration of your network core switches and routers. Our experts provide detailed documentation of all findings—including remediation for alleviating configuration, operational, and security issues. Our assessment emulates the approach used by real-world hackers, performing controlled attacks on your routing and switching configuration to determine flaws and exploitable attack vectors.

### Server and Domain Evaluation

Once an attacker is inside your network, they will look for weaknesses that they can exploit in your domain configuration, servers, systems, and applications. Our team can identify and evaluate the current configuration and health of each server in your environment and provide detailed documentation of all findings, to include your Windows, Mac, and *NIX-based servers. We conduct a physical inventory, review patch levels, identify services, and recommend best practices for system lockdown.

### Security Organization and Policy Review

Effective information security programs and risk management depend on three key core components: people, process, and technology. It is critical to understand how your organization is structured to handle the challenges of today's advanced threats, and if your policies are effective in ensuring compliance with mandated government, commercial, or internal standards. We can review your organizational roles and responsibilities and document process and policy to help you ensure there are no gaps in your security risk management strategy.

## What Value Does a Security Health Check Provide?

During our Security Health Check, Connection utilizes a comprehensive, methodical approach to threat testing. Our Security Practice experts will uncover vulnerabilities in your environment, expose security weaknesses, and provide recommendations to remedy and better manage your risk.

This assessment will help you measure where you stand against the PCI-DSS, HIPAA, FFIEC/GLBA, FISMA, or ISO 27k standards.

## Security Health Check Options

The Security Health Check is structured as a menu of options, enabling your organization to select some or all of the services discussed above—according to your budget and unique risk compliance goals.

## Our Methods and Practices:

**Pre-engagement Planning:** At the start of our engagement, we work with you to determine success criteria, the type of testing to be conducted, and areas of focus. This includes the testing approach, black box versus gray box.

Pre-engagement activities include:

- Coordinating and conducting a scoping call
- Determining what systems and components are "in-scope" for the engagement
- Identifying points of contact for Connection
- Confirming the timeline for testing
- Identifying restrictions for testing (e.g., date and time restrictions and defining stopping points)
- Ensuring authorization to conduct testing is verified (i.e. your organization owns all IPs)
- Finalizing a Statement of Work

**Intelligence Gathering:** Once a Statement of Work has been signed, the project team is assigned and Connection will perform reconnaissance on your organization to gain as much information as possible. This information forms the basis for our attack strategy throughout the engagement. This phase includes the following activities:

- Open source intelligence gathering
  - Utilizing online public resources to gain information about your organization
- Interviewing key personnel to understand and document the organization, process and policy that makes up your risk governance strategy.
- Network and service enumeration
  - Using tools such as network vulnerability scanners to identify live hosts, enumerate open ports, and identify network services and versions. The scanners we use include, but are not limited to:

    Rapid7 NeXpose, Tenable Nessus, and BeyondTrust Retina

*Continued* 〉

- Hands-on system configuration analysis, documentation, process, and policy review
- General firewall and IDS/IPS configuration assessment
- Protocols and filters review
- Firewall and IDS/IPS rule checks
- Off-site log file review and analysis of log files including:
  - Correlation analysis
  - Attack and event analysis
  - Policy-based log management
- Physical inventory of server class machines
- Determine versions and patch levels for OS
- Identify all running services and applications
- Best practices configuration reviews
- Active Directory computer account policies
- Active Directory account detail (password age)
- DNS
- Domain Controller configuration
- Master browser details
- Time service
- Global catalog
- Forest/domain function levels
- Replication testing

**Threat Modeling:** The information gathered during the intelligence phase is used to develop a plan of attack against the targets. This stage of the engagement includes the following:

- Information is documented and classified (e.g. assets are identified as primary or secondary targets)
- Vulnerabilities are identified and documented
- Services and service versions are researched for known exploits

**Exploitation:** This phase of the engagement uses Threat Modeling to focus on gaining access to the target systems by bypassing any security restrictions that are put in place by your organization. This stage includes the following activities:

- Exploits for vulnerabilities are identified and documented
- Exploits can be identified by the following techniques:
  - Pre-built (e.g. Metasploit or Core Impact modules)
  - Manually built or scripted
- Identified exploits are executed against the target systems

**Post Exploitation and Reporting:** The final stages of the engagement include the post exploitation and reporting activities. These stages include the following activities:

- False positives for vulnerabilities are identified and eliminated
- Successful exploits are identified and classified by criticality
- A comprehensive report is developed, detailing all activities and providing suggestions for remediation

## How Is a Security Health Check Scoped?

A 30-minute scoping call is coordinated to gather basic information about your infrastructure, organization, standards, goals and objectives. After the call, a simple sizing spreadsheet is sent to acquire additional details required to size and price the assessment. Once a Statement of Work has been drafted, a 30-minute review call will be coordinated to go over the project tasks, deliverables, and pricing to ensure it meets your expectations. If all is in agreement, a simple signature from you will begin the project execution process.

## Security Health Check Timeline

The assessment typically spans a two- to four-week period, from start of external testing to completion of a final report. The timeline can vary—shorter or longer—depending on the size and complexity of the environment and compliancy goals.

## Engage Connection to Create an Effective Security Risk Protection Plan

In today's security landscape, IT organizations across all industries must navigate a complex set of regulatory, compliance, and business demands. With ever-present security risks, business and technology evolution, and tightening regulations, security compliance can be difficult to achieve and maintain. Our Security Health Check can provide you with a better understanding of your organization's current risks and help identify opportunities to protect your sensitive systems data from compromise.

**Contact an Account Manager to schedule a Security Health Check today, or visit www.connection.com/SecurityPractice**

Contact an Account Manager for more information.

| Business Solutions | Enterprise Solutions | Public Sector Solutions |
|---|---|---|
| 1.800.800.0014 | 1.800.369.1047 | 1.800.800.0019 |

www.connection.com/SecurityPractice



Connection™
we solve IT™