Secure Shell HealthCheck

When Was Your Last Checkup?

Secure Shell HealthCheck

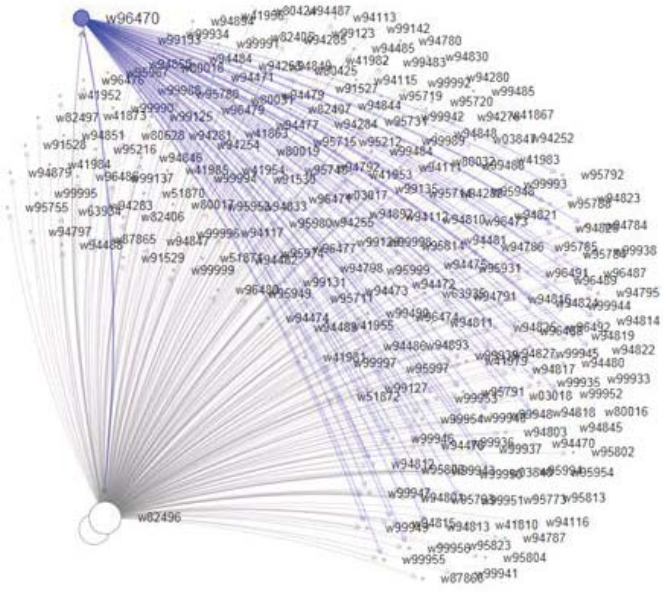
Many organizations use Secure Shell for privileged access to systems and data across the enterprise, yet few organizations have ever examined their deployments of Secure Shell for data breach risk and compliance exposures.

Secure Shell HealthCheck is a security assessment service that delivers a detailed analysis of how Secure Shell is deployed and used in your network.

The Problem

In a recent Forrester survey, over 65% of enterprises reported that Secure Shell is critical or important to their business. It is used by systems administrators and for automated processes such as data base updates, disaster recovery, software management and cloud provisioning. However, lax management controls over Secure Shell expose organizations to data breach risk and compliance violations.

CISO's and security staff have an obligation to identify and resolve significant risk and compliance exposures before they fail an important audit or much worse, before they get hacked. Unfortunately, most organizations lack the tools, time and expertise needed to do a thorough assessment.



Authorizations to Root

The Solution

Secure Shell HealthCheck is an assessment service that addresses this need. Secure Shell HealthCheck leverages our in depth technology expertise, our custom developed scanning and reporting software and our wide ranging experience with thousands of customers to provide a service that is fast, efficient and effective. You get actionable information that is packaged for the C-Suite and backed up by all the details and data your technical staff needs to plan for any needed remediations.

Secure Shell HealthCheck

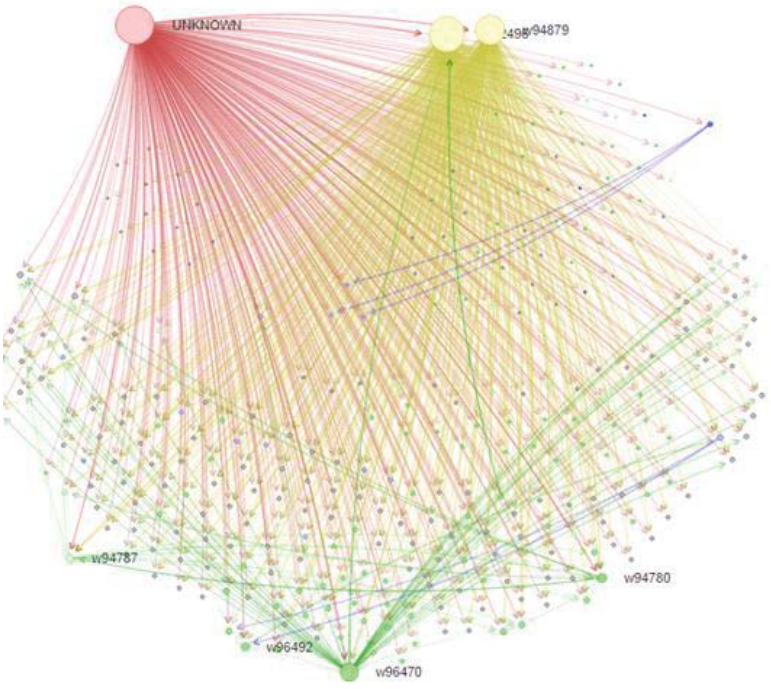
- **Fast.** Secure Shell HealthCheck is completed in 5 days and requires only a few hours of your staff time.
- **Non-invasive.** Our tools do not require software agents to be installed and do not make any changes on your hosts. No private keys are collected or moved.
- **Comprehensive.** You get an analysis of the most significant risks including compelling visualizations of trust relationships.
- **Compliance**. Our report is tailored to the compliance mandates important to your business – whether it is PCI-DSS, Federal CyberSecurity Framework, NIST 800-53, BASEL II, or others.
- **Prioritized**. We tell you what to focus on first and why.
- **Safe**. No information or data leaves your control.

Details: What You Get

Key management	Review and analysis of policies and procedures for lifecycle management of public/private key pairs.
Separation of duties	Scan and discovery of any SSH authorizations that cross dev and prod environments.
Authorizations to root	Discovery of all keys authorized for root access.
Transitive trust analysis	Analysis of which keys provide broadest access into the network.
Key size report	Report and statistics on key sizes. Weak keys highlighted.
Key age report	Analysis and statistics on key age. Keys older than 2 years and older than 5 years highlighted.
Key protection analysis	Report on private keys stored in clear text and/or transmitted in clear text.
Least privilege analysis	Review of service and root account access authorizations.
Privilege escalation	Review of whether current ssh configurations and controls prevent unintended escalations of access.
SSH software management	Report on ssh versions in use. Identifies any insecure versions that should be upgraded.
SSH tunneling	Analysis of whether ssh tunneling is enabled and why, and any indications of misuse.
Activity monitoring analysis	Review of logging practices to determine whether SSH use is properly tracked.
User monitoring analysis	Review and analysis of capabilities in place to monitor the activities of privileged users and processes.
Information protection	Analysis of current capabilities for detecting data loss through SSH and SSH subchannels.
Compliance	Report on potential audit findings for selected compliance mandate (PCI DSS, NIST 800-53, MAS, BASEL III, etc.)
Summary and recommendations	Highlight most risks and compliance issues, recommendations and alternatives for remediation.
Onsite consultation	Our consultant will meet with you to review the findings and recommendations.

Technical Specifications

Supported platforms for scanning	• HP-UX 11iv1, 11iv2, 11iv3 • IBM AIX 5.3, 6.1, 7.1 • Oracle Solaris 8, 9, 10, 11 • Oracle Enterprise Linux 5.4, 5.5, 5.6, 5.7 • Red Hat Enterprise Linux 4, 5, 6 • SUSE Linux Enterprise Server 9, 10, 11
Supported SSH versions for scanning	• Tectia 6.0 or newer • OpenSSH 4.0 or newer
System dependencies for scanning	• All scanned systems must have Perl 5.6 or later installed
Scope	Up to 500 Servers. Greater than 500 can be custom quoted.



Authorizations to Production Servers