

SECURE SHELL HEALTHCHECK

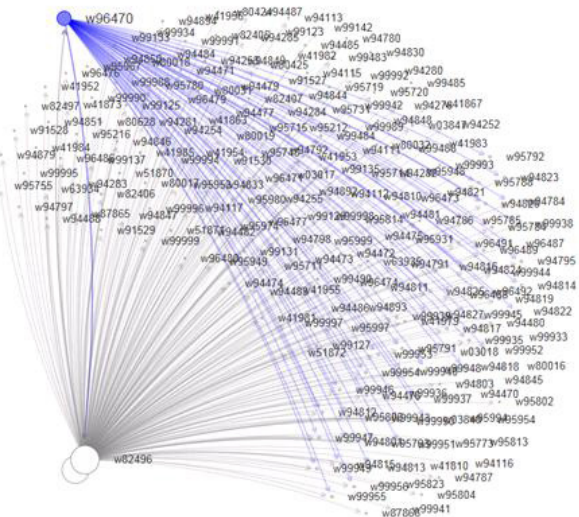
ビジネス環境の健康診断を行っていますか？

Secure Shell HealthCheck は、Secure Shell がネットワーク内でどのように展開され使用されているのかを詳細に分析するセキュリティ アセスメント サービスです。

問題点

フォレスター社の調査では、65%の企業が Secure Shell をビジネスにとって極めて重大か、重要であると回答しました。Secure Shell はシステム管理者が使用しているほか、データベース更新、ディザスタリカバリ、ソフトウェア管理、クラウドのプロビジョニングといった自動化プロセスでも使用されています。しかし、Secure Shell の管理に不備があると、組織はデータ漏洩リスクやコンプライアンス違反の危険にさらされます。

CISO (最高情報セキュリティ責任者) やセキュリティ担当者は、重要な監査の失敗やハッキングされるといった事態を招く前に、重大なリスクやコンプライアンス上の危険を特定し、解決する義務があります。しかし残念なことに、ほとんどの組織で、完全なアセスメントを行うためのツール、時間、専門的知識が不足しています。



ルートへの承認

ソリューション

Secure Shell HealthCheck は、このニーズに応えるアセスメント サービスです。高い専門性を備えた当社の技術、当社がカスタム開発したスキャンングおよびレポーティングソフトウェア、そして迅速で効率と効果に優れたサービスを数千社のお客様に提供してきた当社の幅広い経験が、Secure Shell HealthCheck に活かされています。経営層向けの実用的な情報と、技術担当者が修復計画に必要とするすべての詳細データを提供します。

- **迅速.** Secure Shell HealthCheck は、5日間で完了し、セキュリティ担当者を煩わせる時間はわずか数時間です。
- **透過的.** 当社のツールは、ソフトウェアエージェントをインストールする必要がありませんので、お客様のホストには一切変更はありません。秘密鍵を収集したり移動させることはありません。
- **包括的.** 説得力のある形で信頼関係を視覚化するなど、最重要リスクを分析します。
- **コンプライアンス.** PCI-DSS、連邦サイバーセキュリティフレームワーク、NIST 800-53、BASEL III など、お客様のビジネスにとって重要なコンプライアンスに合わせてレポートを作成します。
- **優先順位.** まず第一に重点を置くべき事項とその理由をアドバイスします。
- **安全.** お客様の環境内の情報やデータは、お客様の管理下から離れることはありません。

SECURE SHELL HEALTHCHECK

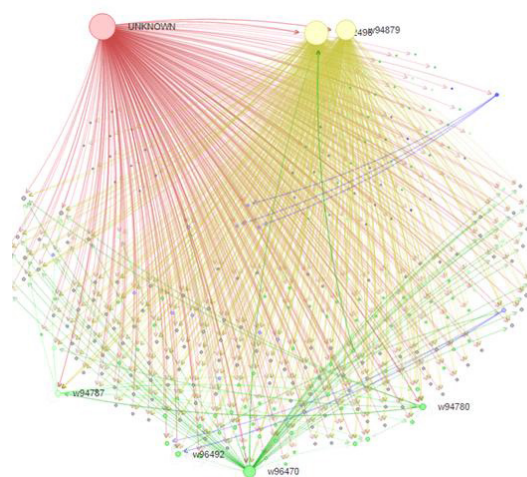
製品仕様

特長の詳細

鍵管理	公開/秘密鍵ペアのライフサイクル管理のためのポリシーおよび手順のレビューと分析。
責務の分離	開発・本番環境を横断する SSH 認証のスキャンと検出。
ルートへの承認	ルートアクセスが承認されているすべての鍵を検出。
推移的信頼の分析	どの鍵が最も広範なネットワーク・アクセスを提供しているかを分析。
鍵長のレポート	鍵長に関するレポートと統計。脆弱な鍵をハイライト表示。
鍵年齢のレポート	鍵年齢に関するレポートと統計。2年以上経過および5年以上経過した鍵をハイライト表示。
鍵保護の解析	平文で保存、および/または平文で送信された秘密鍵に関するレポート。
最小権限の分析	サービスおよびルート アカウントのアクセス承認のレビュー。
権限の昇格	現行の SSH の設定や管理が、意図しないアクセスの昇格を防止しているかのレビュー。
SSH ソフトウェア管理	使用中の SSH バージョンのレポート。アップグレードを必要とする、安全ではないバージョンを特定。
SSH トンネリング	SSH トンネリングが使用されているか、なぜ使用されているのか、また不正使用はないかの分析。
アクティビティ監視の分析	SSH の使用が適切に追跡されているかを判定するためにログの取得方法をレビュー。
ユーザー監視の分析	特権ユーザーおよびプロセスのアクティビティを適切に監視する機能のレビューと分析。
情報の保護	SSH および SSH サブチャネルからのデータ損失を検出することに対する現在の対処能力の分析。
コンプライアンス	該当するコンプライアンス (PCI DSS、NIST 800-53、MAS、BASEL III など) において想定される監査所見に関するレポート。
サマリーと推奨	多くのリスク及びコンプライアンスの問題、推奨事項、是正のための対案をハイライト表示。
現場でのコンサルティング	当社コンサルタントが直接お伺いし、調査における所見及び推奨事項をその場でレビューします。

製品仕様

本サービスで調査対象としてサポートされるプラットフォーム	<ul style="list-style-type: none">• 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
サポート対象の SSH バージョン	<ul style="list-style-type: none">• Tectia SSH 6.0 もしくはそれ以降のバージョン• OpenSSH 4.0 もしくはそれ以降のバージョン
スキャン実行時のシステム要件	全てのスキャン対象システムに Perl 5.6 以降のインストールが必要
範囲	500 サーバーまで。500台以上のシステムスキャンを実行する場合は別途お問合せください。



本番サーバーへの承認

国内連絡先

SSH コミュニケーションズ・セキュリティ株式会社

〒151-0051 東京都渋谷区
千駄ヶ谷5丁目27-3 やまとビル8F
Tel: 03-6865-6629 Email: info.jp@ssh.com



販売代理店

株式会社ディアイティ
〒135-0016 東京都江東区東陽 三丁目23番21号
プレミア東陽町ビル
Tel. 03-5634-7652 Email: info@dit.co.jp
<http://www.dit.co.jp>



© 2015 SSH Communications Security. All rights reserved. Tectia® and ssh® are registered trademarks of SSH Communications Security in the United States, European Union and in certain other jurisdictions. SSH logo is the property of SSH Communications Security and is registered in certain jurisdictions. All other names and marks are the property of their respective owners.

