tenable network security

SecurityCenter™ CV
continuous view

「テナブルのオールインワンソリューションで、常にビジネスの目的を常に見失うことなく、セキュリティリスクの優先順位付けをし、自社のセキュリティの状況を評価できることは素晴らしい。」
– ヘルスケアサービス事業者

マーケットを創造する継続的ネットワークモニタリングプラットフォーム

IT のありようが変わり（仮想、モバイル、クラウドサービス）、サイバー空間の脅威により、ビジネスを新たなサイバー攻撃から守るための定期的なスキャンとコンプライアンス上の監査が不十分になってきています。
継続的ネットワークモニタリングは、自社のセキュリティ状況とアクティビティを継続的に評価する新しいアプローチで、自社の IT セキュリティ投資が正しく構成、運用され、ビジネスに影響を与える最も重要なセキュリティリスクに対する実行可能な洞察を常に提供します。

SecurityCenter™ Continuous View (CV) は、マーケットを定義する継続的ネットワークモニタリングプラットフォームで、企業の健全性を包括的で統合された形で表します。これは、脆弱性スキャニングや受動的なネットワークモニタリング、イベントデータをひとつにまとめたセンサーとなり、それらの情報を最新の脆弱性と脅威に関するインテリジェンス情報にまで高めます。SecurityCenter™ CV の洗練された解析エンジンは、継続的にあらゆる資産を探索し、脆弱性をもれなく見つけ出し、高度な脅威に対抗すべくリアルタイムにすべてのネットワークを監視し、コンテキストに基づいた判断を集め続けることを可能にし、セキュリティ違反に即応し、コンプライアンスを確実に遵守させます。

お客様個別のビジネスニーズに合うよう、ダッシュボード、レポート、ワークフロー、セキュリティポリシーは高度にカスタマイズ可能です。

主な特長

- 自社のネットワークにどのような、物理、仮想、モバイル、クラウド資産があるかを探索
- 既知の脆弱性や設定ミス、マルウェアに対しあらゆる資産をスキャンすることで攻撃対象領域を削減
- 不正な装置のネットワークトラフィックや不審なトラフィックを監視しブラインドスポットを解消
- ネットワークやエンドポイントからのログを関連付けし、即応できる解析で防御能力を最適化
- 警告、通知、障害チケットの発行を利用したインシデントへの素早いレスポンスを順位付け
- 上位レベルの経営目的に沿ったセキュリティポリシーに基づいてセキュリティとコンプライアンスを保証

SecurityCenter™ には業界初となる Assurance Report Card (ARC) が標準で付属します。これは、CISO や経営陣が強い関心をもつ上位レベルの経営目的とそれに応じた個別のポリシーに基づき、自社のセキュリティプログラムの測定、分析、可視化をお客様が継続的に実施できるようにします。

テナブルリサーチ

テナブルリサーチ・チームは SecurityCenter™ CV をご利用のお客様に対し、頻繁に更新される脆弱性と脅威に関するインテリジェンス、高度な解析、セキュリティ/コンプライアンス・ポリシー、ダッシュボード/レポート、Assurance Report Card を提供します。この他にはない範囲の内容は、テナブルが収集した業界およびお客様のベストプラクティスに基づいており、テナブルのセキュリティリサーチ・チームの力をお客様が必要とする形で発揮します。
この内容は、SecurityCenter™ CV のご契約者様に提供されるものとなります。

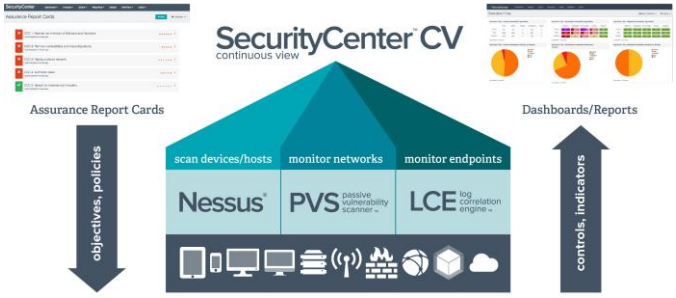
主な機能

- **Assurance Report Cards：**経営目的に基づいてお客様が定めたセキュリティポリシーの効果を継続的に測定し、ギャップが発生し得る場所を見つけ、解消します。
- **高度にカスタマイズ可能なダッシュボード/レポート：**HTML5 ベースの新しいユーザーインターフェースが、CISO やセキュリティ管理者、アナリスト、専門職/オペレーターなどが持つ固有のニーズを満たします。
- **継続的な資産探索：**ネットワーク上の携帯機器、物理/仮想およびクラウドインスタンスを探索し、不正な資産を見逃さず、セキュリティリスクを自動評価します。
- **ネットワークの健全性評価：**脆弱性のあるシステムやサービス、未知の装置、疑わしいトラフィック、ボットネット、コマンド/コントロール・サーバーなどとやりとりする疑わしいトラフィックがないか、ネットワークトラフィックを継続的に監視します。
- **リアルタイム・マルウェア検出：**テナブルのソリューションに組み込まれている脅威に関するインテリジェンスの配信（マルウェアを示すブラックリスト）を利用し、エンドポイント上の高度なマルウェアを見つけます。
- **異常検出：**外部ログソースで統計的および異常な振る舞いを分析する技術を用い、基準ラインから逸脱する行動を自動的に発見します。
- **高度な分析/トレンド追跡:**コンテキストに基づいた判断と行動に結びつく情報を提供し、あらゆる企業資産のセキュリティ状況に対応したセキュリティ上の問題を優先順位付けします。
- **迅速なインシデント・レスポンス：**管理者への警告は、メールや通知、トラブルチケット等で個別対応を促すことや、API を通じて自動化対応をとるように設定可能です。
- **ユニファイド・レポーティング：**システム構成、脆弱性、脅威、イベントデータがひとつにまとめられた複合ビューにより、担当者は企業のセキュリティ状況を測定できます。
- **無駄のないコンプライアンス：**CERT、DISA STIG、DHS CDM、FISMA、PCI DSS、HIPAA/HITECH、その他多くの業界標準や規制上の命令をあらかじめ定義した形でチェックします。
- **現行インフラストラクチャとの統合：**パッチ管理システム (WSUS、SCCM、Red Hat、IBM、Vmware)、MDM システム (Microsoft、Apple、Good Technology)、チケッティングツールおよび復旧ツールなどが含まれます。

完全に統合化されたソリューション

SecurityCenter™ は、次の製品からのデータをひとつにまとめることができる唯一の包括的で統合化されたセキュリティソリューションです。

- **Nessus®:** ネットワーク装置、システム、データベース、アプリケーション上の脆弱性や設定ミス、マルウェアを検出する、もっとも広範囲に利用されているスキャナーです。
- **Passive Vulnerability Scanner™：**ネットワークトラフィックを継続的に監視し、新しいホストやサービス、プロトコルを見つけ、脆弱性や脅威をリアルタイムに検出します。
- **Log Correlation Engine™：**ログデータを企業中のネットワーク装置、エンドポイント、アプリケーションサーバーから集めて関連付けし、即応できる解析を行います。



SecurityCenter™ エディション

SecurityCenter™

SecurityCenter™ は、次世代型の脆弱性分析ソリューションで、世界でもっとも広く利用されている脆弱性スキャナーである Nessus スキャナーを複数装備しています。これは、お客様の分散された、複雑な IT インフラストラクチャが抱えるセキュリティ状況に対し包括的な可視化手段を提供します。

SecurityCenter™ Continuous View

SecurityCenter™ Continuous View は、マーケットを定義する継続的ネットワークモニタリングプラットフォームです。これは、SecurityCenter™ に複数の Passive Vulnerability Scanner (PVS™) ネットワークセンサーと Log Correlation Engine (LCE™) を統合し、包括的な継続的ネットワーク監視を提供します。

tenable network security

より詳細な情報は：tenable.com にアクセスしてください。
お問い合わせは：メールでのお問い合わせは、sales@tenable.comまで、または次をご参照ください
tenable.com/contact