ivanti neurons

Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)

Ivanti Neurons for RBVM で、脆弱性管理戦略をリスクベースのアプローチに進化させましょう。この SaaS は、データ漏洩、ランサムウェア、その他のサイバー脅威からの保護を強化するために、最もリスクの高い脆弱性や弱点を効率的かつ効果的に優先順位付けして修正できます。

脆弱性管理への新しいアプローチの時

既知の脆弱性は27万件以上もあります。[1] 幸いなことに、企業はIT環境に現れた脆弱性や弱点をすべて修正する必要はありません。しかし残念ながら、重大なリスクをもたらす稀な脆弱性や弱点を特定することは、従来の脆弱性管理のアプローチを用いている組織にとって、時間がかかり、エラーが発生しやすいプロセスです。

このような組織は、脆弱性や弱点を改善するための優先順位付けを始める前に、まず、スキャナーの調査結果から脅威インテリジェンスまで、さまざまな異種データを収集し、そのデータを正規化して利用できるように準備しなければなりません。手作業で行う場合、これらのプロセスを完了するには数日、数週間、数か月かかることがあり、常に人的ミスが伴います。

優先順位付けのプロセスも同様です。ランサムウェアの脆弱性について考えてみましょう。74%がCVSS v3でCriticalと評価されておらず、156件が CISAのKnown Exploited Vulnerabilities (KEV)カタログに登録されていません。さらに、一般的な3つのスキャナーは、合計20のランサムウェアの脆弱性に対するプラグインと検出シグネチャをまだ追加していません。[2]

その上、セキュリティとITの意思決定者は、サイバー攻撃に対する防御で直面する最大の課題として、チーム間の協力不足を挙げています。[3] このような脆弱性管理の利害関係者間の問題は、修正を遅らせ、組織が攻撃を受けやすい状態にする可能性があります。

主な機能

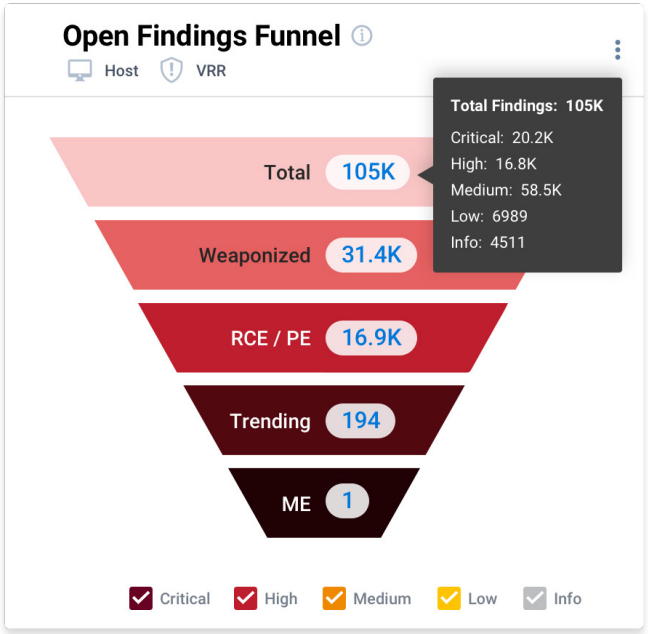
脅威リスクに基づいた優先的なアクション

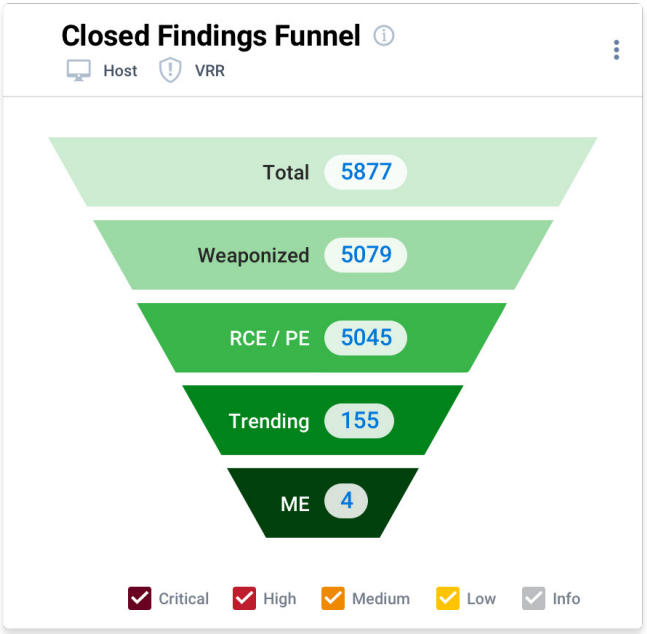
脆弱性と弱点の検出から、企業のサイバーセキュリティ体制の状況に応じたリスクベースの見解を基に、数か月単位ではなく、僅か数分のうちに修復に移行します。Ivanti Neurons for RBVMは、組織のインフラストラクチャを継続的に相関させるプロセスを通じて、リスクを測定し、改善活動の優先順位を決定します。

- 内部および外部の脆弱性データ
- 脅威インテリジェンス。
- 手動のペンテストと調査に基づく調査結果
- ビジネス資産の重要性

なにより、手作業はほとんど必要なく、十分な情報を得た上で攻撃計画を立てることができます。

さらに、CVSSとは異なり、Ivanti独自の脆弱性リスク評価(VRR) により、影響を正確に測定し、脆弱性が悪用される可能性を判断できます。また、Ivanti Neurons for RBVMは、リモート・コードの実行、特権の昇格、ランサムウェア、傾向的でアクティブな脆弱性も特定します。この情報により、企業は最もリスクの高い脆弱性に焦点を当てることができます。

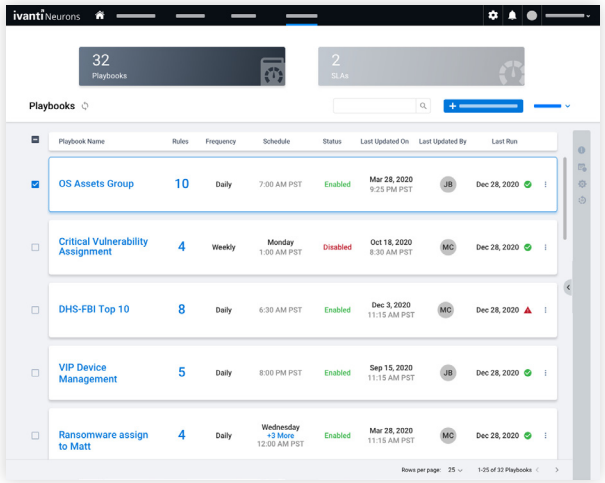




管理ではなく改善に重点を置く

さまざまな自動化やその他の効率化機能により、従来のような時間、労力、ミスを伴うことなく、サイバーセキュリティ体制を強化できます。

- プレイブックを作成し、従来セキュリティアナリストが行っていた一般的なタスクや反復タスクを自動化
- サービスレベル契約の自動化により、必要に応じて脆弱性クローズの期日を自動的に設定
- 登録されたイベントに関連する情報を含む製品ページにリンクする、製品外のほぼリアルタイムのアラートを受信
- Ivantiセキュリティチームによってプッシュされるシステムビューを使用して、ランサムウェアやトレンドCVEなどの重要な脆弱性にさらされていることを明らかにするトレンド基準によって、ホストとホストの調査結果を簡単にフィルタリングが可能
- 優先順位付けされた脆弱性をIvanti Neurons for Patch Managementに直接配信し、修正を行います。電子メールやチャットでCVE IDのCSVの送信が不要

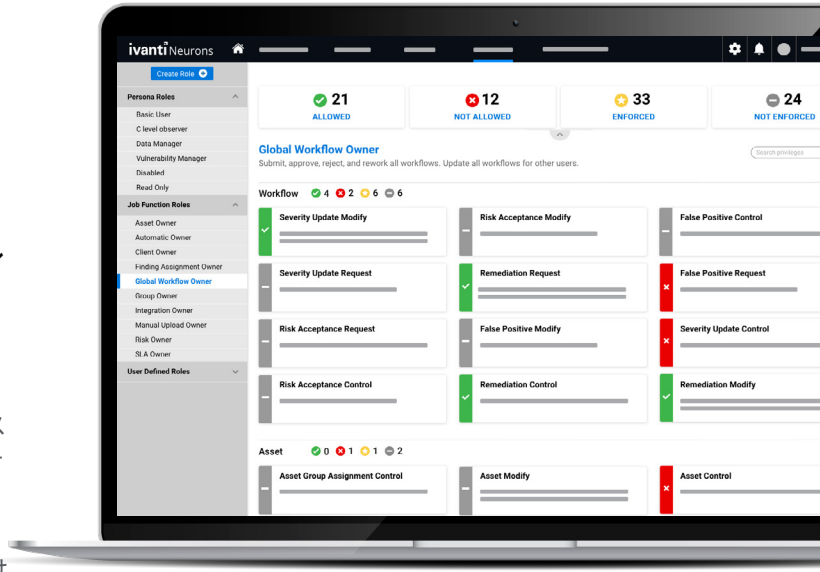


セキュリテイステークホルダー間のより良いコラボレーションを実現

各自の役割に関連する情報をタイムリーに提供することで、組織横断的なセキュリティ関係者間のコミュニケーションと協力を促進します。Ivanti Neurons for RBVMは、役割ベースのアクセス制御 (RBAC) を採用しているため、該当するすべての担当者に製品アクセスを安全に提供できます。

製品内では、ユーザーはSOCから経営幹部までの担当者向けに設計されたダッシュボードにアクセスできます。これらのダッシュボードをより具体的なユースケースに合うように変更したり、ユーザーウィジェットを活用して、さまざまな役割やチームのニーズを正確に満たすカスタムダッシュボードを作成したりすることもできます。

さらに、Ivanti RS3 スコアという形で組織のリスクプロファイルを数値化します。このスコアによって、すべてのセキュリティ関係者が、組織全体のセキュリティレベルについて足並みを揃えているかを確認できます。Ivanti Neurons for ITSM のようなチケットシステムと双方向に統合することで、セキュリティレベルの向上に取り組んでいる企業間の連携が向上します。



特長と機能

特長	機能
多様なデータソース	ネットワークスキャナー、エンドポイント、データベース、IoTデバイスからのデータ、100以上のソースからの脆弱性調査結果、調査チームやペンテストチームからの手動の調査結果、およびカスタムデータソースを取り込む製品により、サイバーリスクを幅広く把握できます。
脅威対策エンジン	Ivanti Neurons for Vulnerability Knowledge Baseから人が生成したものやAI駆動の脅威インテリジェンスによって、ランサムウェアに関連付けられているような脆弱性に関する卓越したインサイトを取得できます。
脆弱性リスク評価（VRR）	脆弱性固有の属性と現実世界の脅威の状況を考慮した数値リスクスコアを使用して、脆弱性のもたらすリスクを迅速に判断します。
Ivanti RS³	VRR、資産のビジネス上の重要性、脅威インテリジェンス、および外部アクセス可能性を考慮した独自のスコアリング手法によって、リスクプロファイルに関する定量化された意見を得ます。
自動化	さまざまな手作業を自動化することで、従業員は管理業務ではなく、改善活動や戦略的イニシアティブに集中できるようになります。
アラートおよび通知	通知エンジンから送信されるほぼリアルタイムのアラートによって、関連イベントを即座に認識できます。同様に、ディープリンクを活用して、製品内の重要な情報に他のユーザーを誘導します。
カスタマイズ可能なデータ編成	カスタムダッシュボードの作成が可能なユーザーウィジェットや、リストビューでデータをピボットする機能により、実用的なインサイトを発見できます。
ダッシュボード	脅威ベースのビューを利用することで、Log4jや Patch Tuesdayリリースに関連するような重要な脆弱性が、お客様の環境でどのように顕在化しているかをすばやく発見できます。また、独自のカスタムビューを作成し、共有することもできます。
脅威ベースのビュー	脅威ベースのフィルターを利用して、BlueKeep、WannaCry、FBI / DHS/CISAの悪用された脆弱性トップ10など、特定の脅威が自社の環境にどのように現れるかを迅速に見つけます。また、独自のカスタムフィルターを作成し、共有することもできます。
Neurons 統合化	Ivanti Neurons for RBVM を Ivanti Neurons for ASPM と組み合わせることで、リスクベースの脆弱性管理を貴社の攻撃対象領域のより広い範囲へ拡張できます。Ivanti Neurons for ITSMおよびIvanti Neurons for Patch Managementの統合化により、組織全体の脆弱性管理担当者は、より効率的かつ効果的に業務を遂行できるようにします。

Ivantiについて

Ivantiは、ITおよびセキュリティ向けに包括的なクラウドベースプラットフォームを提供するエンタープライズソフトウェア企業です。Ivantiは、顧客のニーズに合わせてスケーラブルなソフトウェアソリューションを提供し、ITとセキュリティが運用効率を改善し、コストを削減しながら、セキュリティリスクをプロアクティブに低減できるよう支援します。Ivanti Neuronsプラットフォームはクラウドネイティブで、一貫した可視性、スケーラビリティ、セキュアなソリューション提供を実現するための、統一されたサービスとツールの基盤として設計されています。Ivantiのエンドツーエンドのソリューションは、Fortune 100社のうち85社を含む34,000以上の顧客によって採用されています。Ivantiは、すべての視点が聞き入られ、尊重され、評価される環境づくりに尽力し、顧客、パートナー、従業員そしてよりサステイナブルな未来を実現するために取り組んでいます。詳細については、ivanti.com/jaや@GoIvantiをフォローしてください。

Copyright © 2025, Ivanti. All rights reserved. IVI-2673 11/25 RW/MM/DH/FG

ivanti neurons

ivanti.com/ja/neurons
03-6432-4180
contact@ivanti.co.jp

1. Data pulled from Ivanti Neurons for Vulnerability Knowledge Base on June 29, 2023
2. Cyber Security Works, Cyware, Ivanti, Securin, “2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management”, 16 February 2023. https://www.securin.io/ransomware/
3. ExtraHop, “Cyber Confidence Index 2022”, 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/