ivanti neurons

Ivanti Neurons for App Security Orchestration & Correlation (ASOC)

リスクベースの脆弱性管理をアプリケーションスタックに拡張

Ivanti Neurons for ASOCは、アプリケーションの脆弱性管理をリスクベースのアプローチに進化させます。このSaaS製品により、企業は社内および顧客向けアプリケーションのセキュリティを向上させるために対応すべき方向性について迅速かつ十分な情報に基づいた意思決定を行うことができます。

リスクベースの脆弱性管理にはアプリを含める必要がある

四半期ごとにスキャンされたアプリケーションの数は、10年間で3倍になりました。スキャンの頻度は同期間に20倍に増加しました[1]。重大なリスクをもたらすアプリケーションスタックのレアな脆弱性や弱点を特定するのは、従来の脆弱性管理アプローチをとっている企業にとっては、時間のかかるプロセスであり、データに溺れてしまいます。

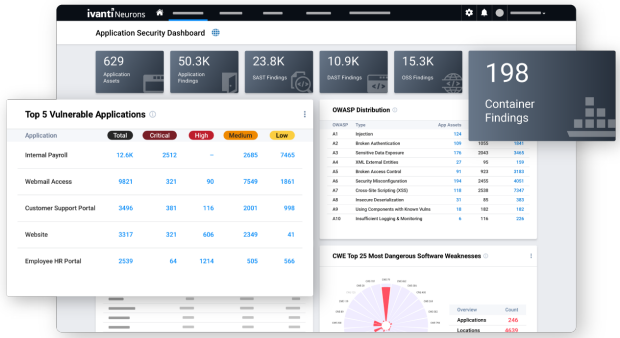
このような企業は、脆弱性や弱点の修正に優先順位を付ける前に、まずSAST、DAST、OSS、コンテナスキャナーの調査結果、脅威インテリジェンスなど、様々の異なるデータを収集、正規化し、利用可能なデータに変換する必要があります。これらのプロセスを手作業で行うと、完了するまでに数週間かかりますし、ヒューマンエラーが発生しやすくなります。

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ると、74 パーセントが CVSS v3 で「Critical」と評価されておらず、156 件が CISA Known Exploited Vulnerabilities（KEV）カタログに記載されていません。さらに、人気の高い3つのスキャナーは、合計20件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]。

さらに、サイバー攻撃からの防御における最大の課題として、関係するチーム間の協力の欠如が挙げられています[3]。このような脆弱性管理の関係者間のギャップは、修復を遅らせ、企業を攻撃されやすい状態にします。

Ivanti Neurons for ASOCとは

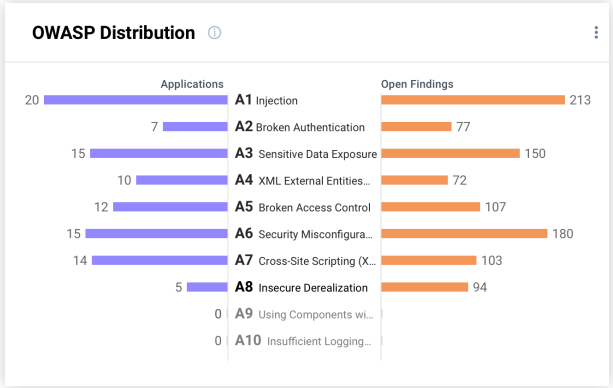
Ivanti Neurons for ASOC の機能により、アプリケーション・スタックの脆弱性管理にリスク・ベースのアプローチを採用できます。これらの機能は単一のインターフェイスにパッケージ化されているため、過去の脆弱性管理手法で定義されてきた”手作業による非効率な”アプローチを段階的に廃止することができます。



主な機能

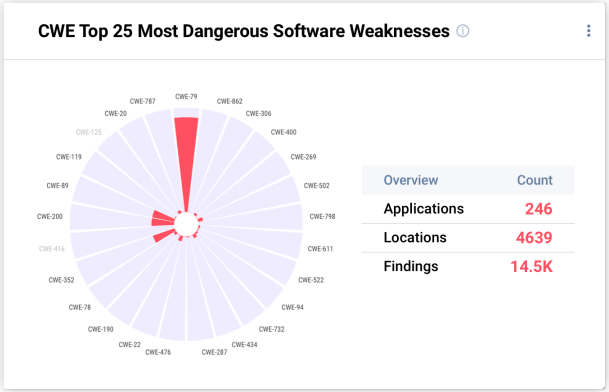
アプリケーションのリスク・エクスポージャーのフルスタックで可視化

開発から運用まで、アプリケーションのリスク・エクスポージャーをフルスタックで可視化します。Ivanti Neurons for ASOC は、SAST、DAST、OSS、コンテナなど、すべてのアプリケーション・スキャン・データを統合して、脆弱性と弱点を特定し、修復の優先順位を決定します。



Ivanti Neurons for ASOCは、スキャナに依存しないため、DevOpsが開発ライフサイクルのさまざまな部分で必要なさまざまなスキャンツールを選択できるようにします。この製品は、すべてのアプリケーションの脆弱性とスキャンの結果を正規化し、それらを現在流行しているアクティブな脅威と継続的に関連付けて、どの結果が企業にとって最大のリスクであるかをすぐに把握できるようにします。また、発見された脆弱性がアプリケーション・スタック内に存在する正確なコード位置までドリルダウンすることも可能です。

さらに、同製品のApplication Security Dashboardでは、企業を危険にさらす脆弱性、CWE、OWASPの調査結果、新しいスキャン調査結果のバランス、およびそれらの修復率を包括的に表示します。そのため、ユーザーは、セキュリティリスクへの対処におけるアプリケーション開発の進捗状況を確認できるようになります。



脅威リスクベースの即対応可能な優先順位付け

企業のサイバーセキュリティポスチャをコンテキストに基づいたリスクベースのビューで把握することで、脆弱性や弱点の検出から修復までを、数カ月ではなく数分で行うことができます。Ivanti Neurons for ASOCは、企業のアプリケーションを継続的に関連付け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付けを実施します。

- 内部および外部の脆弱性データ
- 脅威インテリジェンス
- 手作業によるペンテストと調査に基づく発見
- 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に対する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、企業は影響を正確に把握し、脆弱性が悪用される可能性を判断できます。また、Ivanti Neurons for ASOCは、リモートコード実行(RCE)、権限昇格(PE)、ランサムウェア、トレンドおよびアクティブな脆弱性を特定します。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絞ることができます。

管理ではなく修復に重点を置く

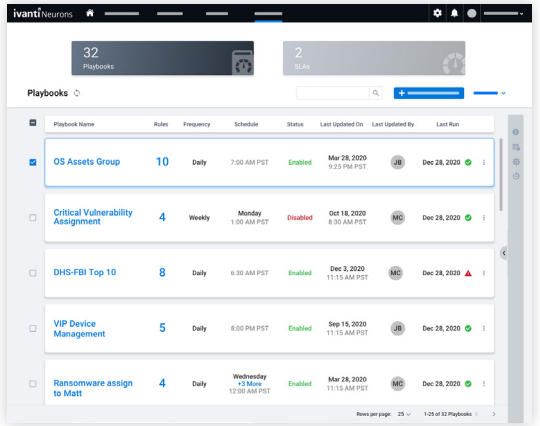
さまざまな自動化やその他の効率化機能により、従来のような時間、労力、ミスを伴うことなく、サイバーセキュリティポスチャを向上させることができます：

- プレイブックを作成して、従来セキュリティアナリストが担当し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（SLA）の自動化により、必要に応じて脆弱性の対処期限を自動的に設定
- 購読し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、ほぼリアルタイムのアラートを製品外で受信
- Ivanti セキュリティチームが推奨す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のCVEなど、最もクリティカルな脆弱性に晒されていることを明らかにするトレンド基準によって、アプリケーションやアプリケーションの調査結果を簡単にフィルタリング

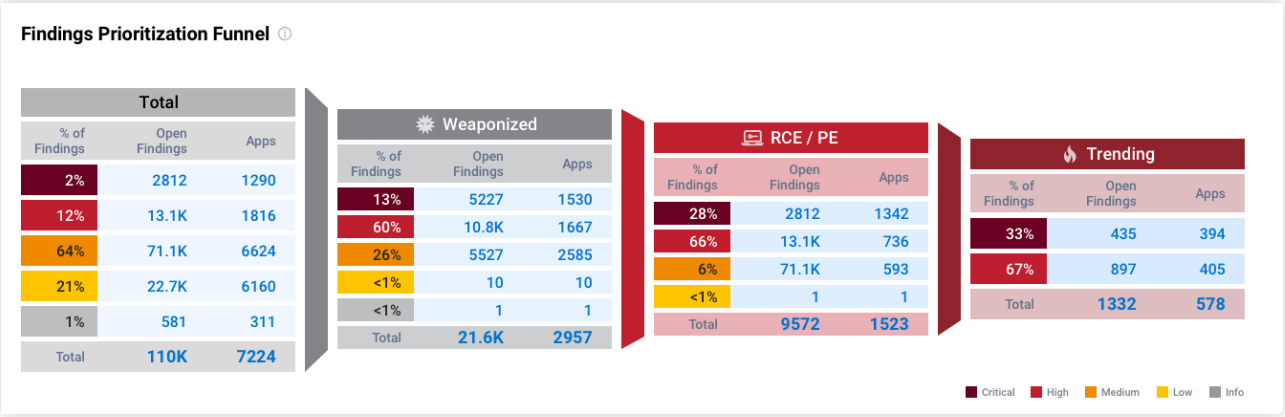
セキュリティ関係者間の連携を強化

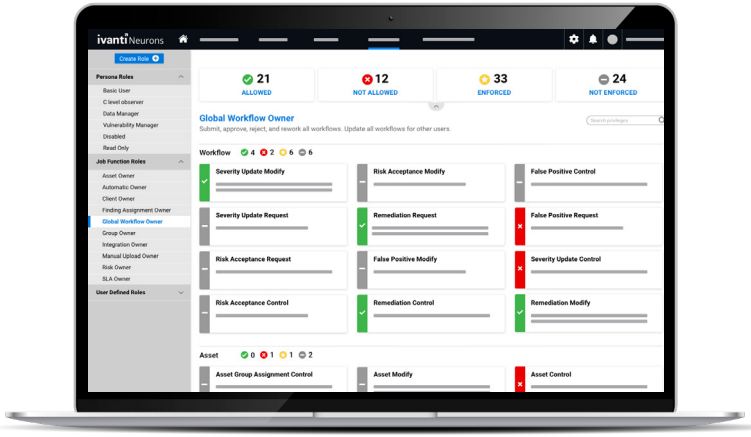
各自の役割に関連する情報をタイムリーに提供することで、組織全体のセキュリティ関係者間のコミュニケーションと連携を促進します。Ivanti Neurons for ASOCはRBACを採用しているため、該当するすべての担当者に製品アクセスを安全に提供できます。

製品にアクセスすると、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わせて変更したり、ユーザーウィジェットを活用して、異なるロールやチームの正確なニーズを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、この製品は、企業のリスクプロファイルを Ivanti RS3 スコアの形で定量化します。このスコアにより、すべてのセキュリティ関係者が、企業のセキュリティレベルについて同じ認識を持つことができます。Ivanti Neurons for ITSM のようなチケットシステムとの双方向の統合により、セキュリティレベルの向上に取り組む関係者間の連携が改善されます。





特徴と機能

特徴	機能
多様なデータソース	アプリケーションスキャナ（SAST、DAST、OSS、コンテナ）、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調査結果、およびカスタムデータソースからデータを取り込む製品により、サイバーリスクを幅広く把握することができます。
脅威エンジン	Ivanti Neurons for Vulnerability Knowledge Baseから提供される、人間が生成した脅威インテリジェンスとAI主導の脅威インテリジェンスにより、ランサムウェアに関連する脆弱性などに関する比類のない洞察を得ることができます。
Vulnerability Risk Rating (VRR)	脆弱性の本質的な属性と実世界の脅威コンテキストを考慮した数値リスクスコアにより、脆弱性がもたらすリスクを迅速に判断します。
Ivanti RS^3	VRR、資産ビジネスの重要性、脅威インテリジェンス、外部からのアクセスを考慮した独自のスコアリング手法により、企業のリスクプロファイルを定量化して表示します。
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。
アラートと通知	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り、関連するイベントを即座に認識できます。同様に、ディープリンクを使用して、他のユーザーを製品内の重要な情報に誘導します。
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	ドリルダウン機能を備えた既製のカスタマイズ可能なダッシュボードにより、資産やインフラストラクチャ全体にわたる優れた視覚的クエリとリスク発見機能を実現します。
脅威ベースのビュー	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素早く発見できます。また、独自のカスタムビューを作成して共有することもできます。
Neuronsの統合	Ivanti Neurons for ASOCとIvanti Neurons for RBVMを組み合わせることで、リスクベースの脆弱性管理を攻撃対象領域の広い範囲に拡張できます。Ivanti Neurons for ITSMとの組み合わせで、企業全体の脆弱性管理担当者が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。

About Ivanti

Ivanti は、企業や従業員がセキュリティを確保しながら「Everywhere Work（場所にとらわれない働き方）」を実現できるよう支援し、「人のためのテクノロジー」を提供しています。今日の従業員は、会社や個人の多種多様なデバイスであらゆる場所や方法で、さまざまなネットワークからITアプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivantiは、企業内のあらゆるIT資産とエンドポイントを検出、管理、保護（セキュア）する唯一のテクノロジー企業です。卓越した「従業員のデジタル体験」やITおよびセキュリティチームの生産性と効率性向上を達成するためにFortune 100の88社を含む40,000社以上の顧客は当社を採用しています。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の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 をご覧になるか、@GoIvantiをフォローしてください。

ivanti

本件に関するお問い合わせ先：ivanti.com/ja

1. Veracode, “State of Software Security v12”, 2021. https://info.veracode.com/report-state-of-software-security-volume-12.html
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/