Ivanti Neurons for EASM

外部から攻撃の対象となりうるIT資産を把握し、エクスポージャーに関する実用的なインテリジェンスにより、拡大する攻撃対象領域（アタックサーフェス）に対処

Everywhere Workの普及とデジタルトランスフォーメーションの進展により、アタックサーフェス（攻撃対象領域）は拡大しています。Ivanti Neurons for External Attack Surface Management (EASM) は、インターネットに面している内部のIT資産と関連するエクスポージャーを包括的かつ継続的に表示します。これによって、リスクの高いエクスポージャーを排除し、サイバー攻撃からプロアクティブに企業を保護することができます。

未確認のアタックサーフェス

Everywhere Workへの移行とデジタルトランスフォーメーションの進展により、シャドーITとクラウドベースのツールの利用が加速しています。同時に、企業はIoTデバイスの採用を増やしており、相互接続されたサプライチェーンが増加しています。

その結果、セキュリティチームはアタックサーフェス（攻撃対象領域）全体に渡り、外部に接続されたIT資産を把握するのに手を焼いています。これらの資産に関連するエクスポージャーの可視性も欠如しています。

未知・未検証、管理されていないや、パッチが適用されていない資産は、「データ漏洩」や「罰金」、「ダウンタイムの発生」のリスクをもたらします。セキュリティチームは、企業を適切に保護するためには、アタックサーフェス（攻撃対象領域）全体を継続的に可視化する必要があります。

Ivanti Neurons for EASMについて

Ivanti Neurons for EASMは、アタックサーフェス（攻撃対象領域）全体において、インターネットに接続されたIT資産のすべてを可視化します。これらの資産に影響を及ぼすエクスポージャーに関する実用的でリスクベースのインテリジェンスにより、データ漏洩、罰金、ダウンタイムの発生などを事前に防ぐことができるようになります。

ivanti

主な機能

完全な可視化を実現

インターネットに面したすべての資産と、それに関連する企業の攻撃対象領域を可視化します。エージェントレス監視は、従来の検出ツールでは検出を回避していた資産だけでなく、セキュリティチームによって監視されていない資産も検出します。(たとえば、設定ミスのAmazonS3バケット、見落とされたQAおよび開発環境、忘れ去られたマーケティングWebサイト、誰もが廃止されたと思っていたサーバー上で実行されているJavaアプリなど) を検出します。

継続的な監視により、これらの資産をほぼリアルタイムで可視化できるため、既存の資産が曝されたり、新しい資産が展開されたりしたときに、すぐにそれを把握することができ、それに応じて対応することができます。

EASMが検出した資産タイプ	EASMが検出したエクスポージャーベクター
■ API ■ ドメイン ■ ホスト ■ ネットブロック ■ SSL証明書 ■ URL	■ アプリケーションセキュリティ ■ データ漏洩 ■ DNSヘルス ■ Eメールセキュリティ ■ ネットワークセキュリティ ■ パッチケイデンス ■ ソーシャルエンジニアリング

Workspaceの機能により、資産やエクスポージャーを部門や子会社などのカテゴリー別にグループ化できます。また、Ivanti Neurons for EASMを使用することにより、サプライチェーンパートナーなどの第三者組織の外部アタックサーフェスを監視する際にも役立ちます。

リスクの高いエクスポージャーの優先順位付け

アタックサーフェス全体のエクスポージャーに関する実用的なインテリジェンスを活用し、是正の方向性を決定します。インテリジェンスには、Ivanti Neurons for EASMが検出したすべてのCVEに対する脆弱性リスクスコア((Vulnerability Risk Score (VRS)) が含まれています。

VRSはセキュリティチームが脆弱性がもたらすリスクを定量化できるようにし、その脅威の背景を理解でき情報に基づいた意思決定をできるよう支援します。VRSは、米国の国家脆弱性データベース (NVD) からのCVSSスコアに加え、特定の環境における脆弱性の影響力を反映するなどさまざまな要素を考慮します。

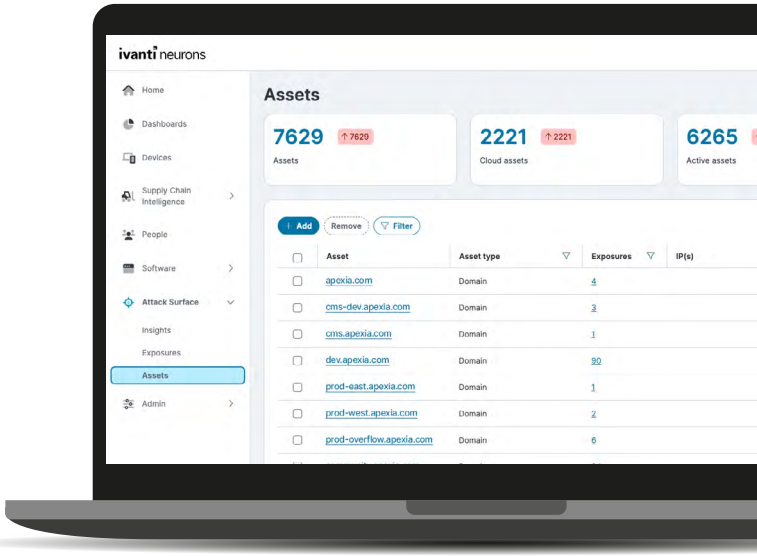
リスクに関するレポーティング

上級レベルのセキュリティステークホルダーからのレポート要件を満たし、PDFレポートを使用して、潜在的な買収先企業、パートナー、ベンダーの適正評価手続きを支援します。これらのエクスポート可能なレポートは、これらのレポートは、企業の外部アタックサーフェスに関連するエクスポージャーの詳細な概要を提供します。

アタックサーフェスのギャップに対処

Ivanti Neurons for EASMと以下のNeuronsを組み合わせることで、インターネットに接続されたIT資産に影響を与える問題への迅速な対応が可能になります。

- Ivanti Neurons for ITSM: ITサービス管理
- Ivanti Neurons for UEM：統合エンドポイント管理
- Ivanti Neurons for Patch Management：パッチ管理



EASMのユースケース

EASMのユースケース

- **デジタル資産の検出とインベントリ：**クラウド、IT、IoT、および OT 環境全体のウェブサイト、IP、ドメイン名、SSL 証明書、およびクラウド サービスから、インターネットに面した資産を検索しインベントリ化します。
- **エクスポージャーの分析と優先順位付け：**パッチ未適用の脆弱性から設定ミスやオープンポートまで、インターネットに面した資産に影響を与えるエクスポージャーの修復の優先順位付けをします。
- **クラウドスプロールとシャドー ITを抑制：**クラウドプロバイダー全体のパブリック資産 (従業員が適切な手続き以外で作成したクラウドインスタンスを含む) を特定します。
- **データ漏洩を検知：**社内や第三者が使用するコラボレーションツールやクラウドアプリを介したデータ漏洩や機密データの露出を監視します。
- **子会社、第三者組織、潜在的な買収先へのリスク評価：**システムを他の事業体と統合する前に、包括的なセキュリティチェックを実行します。
- **フィッシングおよびソーシャルエンジニアリング攻撃を低減：**フィッシングドメインを監視し、なりすましサイトを特定し、従業員や顧客を標的した潜在的なソーシャルエンジニアリング攻撃を検出します。
- **規制コンプライアンス要件の遵守：**GDPR、HIPAA、PCI DSSなど、情報開示や資産インベントリの提出を求める規制に準拠しています。

Ivantiについて

Ivantiは、ITとセキュリティ部門間の障壁を取り除きEverywhere Work（場所にとらわれない働き方）を実現します。IvantiのCIOとCISO向けに特化したプラットフォームは、ITとセキュリティ部門へ組織のニーズに合わせて拡張できる包括的なソフトウェアソリューションを提供し、セキュアに従業員体験を向上させます。Ivantiプラットフォームは、クラウドスケールのインテリジェントなハイパーオートメーションレイヤーであるIvanti Neuronsを搭載しており、組織全体でプロアクティブな修復とユーザーフレンドリーなセキュリティを実現し、ユーザーが満足するような従業員体験を実現します。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40,000社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、www.ivanti.com/jaをご覧ください。

ivanti

詳細やお問い合わせについては、
ivanti.com/jaをご覧ください。

1. Forrester, “The External Attack Surface Management Landscape, Q1 2023,” 2023年1月9日