2022年8月5日
Ivanti Software 株式会社

Ivanti と SentinelOne が提携を発表
パッチ管理に革命をもたらし、脆弱性の評価、優先順位付け、修正の自動化を実現

サイバー攻撃リスクを低減し、脆弱性評価、優先順位付け、
修正を自動化するソリューションを提供

クラウドからエッジまで IT 資産の管理、検出、保護、サービスを自動化するプラットフォーム Ivanti Neurons を提供する Ivanti（本社：米国ユタ州ソルトレイクシティ、CEO：Jeff Abbott）と、オートノマスサイバーセキュリティプラットフォーム企業である SentinelOne (NYSE: S) は、パッチ管理に対する包括的なリスクベースのアプローチを支援し、ランサムウェア攻撃を含むサイバー脅威に対するサイバーセキュリティの強化を目的とした提携を発表しました。Ivanti と SentinelOne は、Ivanti Neurons for Patch Management と SentinelOne の Singularity XDR プラットフォームという業界最高のテクノロジーを統合することで、高速で脆弱性の評価、優先順位付け、修正を実現します。

現在、パッチ管理は依然として多くの組織にとって重要な課題となっています。多くの場合、セキュリティや IT 部門は、ソフトウェア更新、パッチの遅れ、断片化されたプロセス、多種多様なテクノロジースタック、統一性に欠けるチームに起因する脆弱性のマッピングに苦慮しています。最近の Ivanti の調査では、71% の IT およびセキュリティの専門家が、「パッチは明らかに複雑かつ厄介で時間がかかる作業だ」と回答しています。さらに、53%が、「重大な脆弱性の整理と優先順位付けに多くの時間を費やしている」と回答しています。結果として、多くのセキュリティおよび IT 部門は、新しい脆弱性や National Vulnerability Database (NVD) で公開された脆弱性だけにパッチを適用しています。しかし、現在、NVD はすべての共通する脆弱性とリスクのうちの20%を見逃しているため、この状況は、企業におけるセキュリティ ギャップの発生を招くとともに、脅威攻撃者による被害を誘発・助長する可能性があります。

従来の脆弱性管理プロセスは、明らかに組織のサイバー攻撃リスクを高めています。現在、パッチ未適用のアプリケーションおよび OS 脆弱性は、ハッカーによって悪用される最も顕著な攻撃ベクトル の1つです。攻撃者は、かつてないほどのスピードで脆弱性を悪用し、被害と影響を最大化する弱点を標的にします 。実際に、Ransomware Index Report Q1 2022では、ベンダーが脆弱性を公開してから8日以内に、高度化するランサムウェアグループが脆弱性を悪用していることが明らかになっています。つまり、すべての脆弱性は、資産全体に対する防御を強化しようとする企業と、脆弱な標的に侵入しようとする脅威攻撃者との間で、時間の戦いとなっています。

Ivanti と SentinelOne の提携により、組織は、脆弱性を迅速に検出し、組織全体で弱点をワンクリックのみで修復することが可能になることで、エンドポイントの強化、サイバー衛生の改善、攻撃性の是正など

の課題解決が期待できます。IvantiとSentinelOneの統合ソリューションは、セキュリティおよびIT部門に対して、ランサムウェアに関連する脆弱性を含む、実際に悪用されている脆弱性に対する組織のリスクに関するコンテキストと適応型のインテリジェンスを提供し、組織がこのような脅威を迅速に修正できるようにします。IvantiとSentinelOneが協力することで、特にランサムウェアに関連する重大な脆弱性といった企業のサイバー脅威を検出、発見、修正、対応するまでの平均時間を大幅に短縮し、支援します。

Ivanti、社長兼最高製品責任者であるNayaki Nayyar（ナヤキ・ネイヤー）は次のように述べています。
「SentinelOneとパートナーシップを締結することで、組織がサイバー衛生を改善し、サイバー攻撃に対する防御能力を向上することができます。IvantiのAIベースのIvanti Neurons for Patch Managementソリューションでは、企業のリスクや顕在化した脅威を検知・特定し、脆弱性の悪用を早期に警告し、攻撃を予測し、修正作業の優先順位付けを行うことができます。さらに、Ivantiは、エージェントベースのパッチとエージェントレスパッチを提供し、350以上のエンタープライズアプリケーションに幅広く対応しています。このような高度な機能により、セキュリティパッチの評価と配布、サイバー攻撃者が悪用した脆弱性の撲滅に向けて、セキュリティおよびIT部門の効率と効果が大幅に改善されます。」

SentinelOne、最高執行責任者であるNicholas Warner（ニコラス・ワーナー）は次のように述べています。
「サイバー攻撃が高度化し、件数が急増する中で、自律的な脆弱性の評価と修正は必要不可欠です。Singularity XDRでは、エンドポイント、クラウド、ID全体で、サイバーセキュリティを自動化することができます。Ivantiとのパートナーシップによって、サイバーセキュリティに対する自律的なリスクベースのアプローチを提供することにより、セキュリティ部門は、継続的に脆弱性のリスクを特定し、高速でリスクを修正できるため、自動化の利点を最大限享受できます。」

Ivanti、シニアバイスプレジデント兼戦略的アライアンス担当ゼネラルマネージャーであるMark Stevens（マーク・スティーブンス）は次のように述べています。
「SentinelOneとIvantiのパートナーシップは、世界最高レベルのサイバーセキュリティISVと協力して、パッチ管理の提供することに関するIvantiの取り組みを反映するものです。Ivantiは、SentinelOneとの関係を強化し、SentinelOneのお客様とパートナーに自動化されたパッチを提供します。パッチの管理、検出、リモート制御、アプリケーション制御、デバイス制御でIvantiのAPIとSDKを活用することは、Ivantiが独自のソリューションの強化を目指すISV向けに、堅牢なエンドポイントセキュリティ群を提供していることを実証するものです。」

Ivantiの OEM ライセンスプログラムとさまざまな OEM パッチソリューションの詳細については、こちらからご覧ください。OEM 企業は、Ivanti の OEM ライセンスプログラムを活用することで、ブランド化されたアプリケーション内で Ivanti のテクノロジーを活用するセキュリティソリューションを構築し、Time-to-market を短縮しながら、開発の負荷を増やすことなく新しい収益モデルを構築することが可能になります。SentinelOne の Singularity XDR プラットフォームの詳細については、こちらからご覧ください。

※本プレスリリースは、米国本社が8月3日（米国時間）に発表したリリースの抄訳版です。

Ivanti について

Ivanti は「Everywhere Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない働き方により、従業員は多種多様なデバイス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 Neurons 自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合 IT プラットフォームを提供します。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまで IT 資産の管理、検出、保護、サービスのために Ivanti を選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験を提供しています。
詳細については、www.ivanti.co.jp をご参照ください。

SentinelOne について

SentinelOne のサイバーセキュリティソリューションは、単一の自律型 XDR プラットフォームにより、AI を活用して、エンドポイント、コンテナ、クラウドワークロード、IoT デバイス全体の防御、脅威検知、インシデント対応、および脅威ハンティングを提供しています。

＜報道関係に関するお問い合わせ先＞
Ivanti Software 株式会社
マーケティング部：鳥羽
Email: shoichi.toba@ivanti.com
TEL: 03-6432-4180

Ivanti 広報事務局
E-mail: ivanti@jspin.co.jp