キーサイト・テクノロジー株式会社
〒192-8550
東京都八王子市高倉町9-1
www.keysight.co.jp

NEWS RELEASE

PRJ06_NR20026

報道関係者からのお問い合わせ
キーサイト・テクノロジー株式会社
広報担当 土肥（どひ）
電話：042-660-8589

お客様からのお問い合わせ
キーサイト・テクノロジー株式会社
計測お客様窓口
電話：0120-421-345

2020年3月19日

キーサイトの新しいセキュリティ・オペレーション・プラットフォームにより、企業におけるセキュリティオペレーションの有効性の測定と改善が可能に

キーサイトの Threat Simulator は、脆弱性に対処するための実用的なアドバイスとリアルタイムの脅威インテリジェンスを提供

東京、2020 年 3 月 19 日発 – エンタープライズ、サービスプロバイダー、政府などのお客様がイノベーションを加速し、あらゆるものが安全につながる世界の実現を支援する、キーサイト・テクノロジー株式会社（代表取締役社長：チエ ジュン、本社：東京都八王子市高倉町 9 番 1 号、以下「キーサイト」）は本日、セキュリティオペレーションの有効性を改善するために設計されたセキュリティオペレーション（SecOps）プラットフォームである Breach Defense を発表しました。新しいプラットフォームに不可欠な要素の一つが、侵害・攻撃シミュレーションソリューションである Threat Simulator です。これにより、ネットワークおよびセキュリティオペレーション担当チームは、運用中のネットワーク上の最新の攻撃とエクスプロイトを安全に模擬し、セキュリティオペレーションの有効性を測定することが可能になります。

セキュリティオペレーションチームが直面しているのは、組織内外からの大量のサイバー脅威の絶え間ない攻撃に晒されている、高度に複雑化したネットワーク環境です。 最近キーサイトが実施したセキュリティオペレーションの有効性 に関する調査の結果では、次の内容が明らかになりました。

- **優れたセキュリティツールであっても期待どおりに保護できるとは限らない**：回答者の 50%は、侵害発生後にセキュリティソリューションが期待どおりに機能していないことが判明したと述べています。
- **多くの企業はセキュリティが正常に機能しているかどうかを検証していない**：セキュリティ製品が正しく設定され作動していることをテストで証明すると答えた回答者は 35%に留まります。
- **セキュリティテストの価値**：回答者の 86%は、企業のセキュリティ体制の脆弱性を見つけ、改善できるソリューションを高く評価するだろうと回答しています。

キーサイト・テクノロジー株式会社
〒192-8550
東京都八王子市高倉町9-1
www.keysight.co.jp

NEWS RELEASE

Sayers 社サイバーセキュリティ担当シニアバイスプレジデントである Doug Close 氏は次のように述べています。「最高のセキュリティ製品であっても、適切に設定しないと安全を守ることはできません。 自動化された攻撃のシミュレーション、セキュリティギャップの検出、詳細なアドバイスを入手ができることは、セキュリティのギャップを埋め、日常的なセキュリティオペレーションを改善する上で、お客様にとって強力な利点となります。」

Enterprise Management Associates 社セキュリティ&リスク管理部門リサーチディレクターである Paula Musich 氏は次のように述べています。「セキュリティを担保できている組織でも、ある日突然、脆弱になってしまうものです。ある時点でセキュリティ機能をテストすれば、組織の継続的なセキュリティ体制を限定的に可視化することができます。セキュリティは本質的には、人とプロセスの問題です。攻撃シミュレーションを使用して定期的に防御をテストすることで、セキュリティオペレーション担当チームは、良好なセキュリティ状態が悪用可能な脆弱性へと変わるのを、先手を打って察知・防御することができます。」

Threat Simulator により、セキュリティツールが的確に防御しているという確信を提供

キーサイトの Threat Simulator ソリューションは、組織のセキュリティ保護の有効性を判断するセキュリティツールのテスト方法を企業のセキュリティオペレーション担当チームに提供します。このソリューションは、プロダクション・ネットワーク・セキュリティ・インフラストラクチャ全体に対する継続的で自動化されたセキュリティ検査を実行し、組織がセキュリティギャップと環境に合わないセキュリティ設定（通常 IT や関連グループの誰かが悪意なく変更したもの）を迅速に特定することが可能になります。また、特許を得た推奨エンジンが理解しやすい改善手順を提供します。

SaaS（software-as-a-service）プラットフォーム上に構築された脅威シミュレータは、一連の軽量エージェントを使用し、プロダクションサーバーやエンドポイントをマルウェアや攻撃に晒すことなく、運用中のネットワーク上の攻撃を模擬します。Threat Simulator の特徴は、経験豊富なキーサイトの ATI リサーチセンター（Application and Threat Intelligence Research Center）により継続的に更新されるサブスクリプションサービスです。統合型ダッシュボードでは、評価の実施、脆弱性の特定、問題点の掘り下げを簡単に行うことができます。脆弱性を解消するための説明が手順ごとにわかりやすく提供されており、セキュリティオペレーション担当チームの問題解決を支援します。

当社ネットワークアプリケーションおよびセキュリティグループ（旧イクシアソリューショングループ）、セキュリティソリューション部門のバイスプレジデントである Scott Register は次よう

キーサイト・テクノロジー株式会社
〒192-8550
東京都八王子市高倉町9-1
www.keysight.co.jp

NEWS RELEASE

に述べています。「今日、ネットワークとセキュリティ担当チームは、継続的なセキュリティソリューションの有効性を把握できていません。セキュリティ侵害は高性能なセキュリティ製品があっても生じます。多くの場合、設定ミスやセキュリティスキルの不足が原因です。 運用中のネットワーク上で保護範囲のセキュリティギャップを調査するのは、決して容易なタスクではありません。Threat Simulator により、セキュリティオペレーション担当チームはギャップを特定できるだけでなく、ギャップを埋めてセキュリティ体制を改善する方法に関する実用的な情報を得られます。」

Breach Defense Suite -- ThreatARMOR

脅威シミュレータのほかにも、キーサイトの Breach Defense SecOps プラットフォームには脅威インテリジェンスゲートウェイである ThreatARMOR も含まれます。既存のセキュリティインフラストラクチャを補完する ThreatARMOR は、ソースレベルで最大 80%の悪意あるトラフィックを遮断して攻撃面を減らすため、セキュリティ情報とイベント管理（SIEM）アラートの数を低減します。ThreatARMOR の機能には、既知の悪性 IP アドレスからのトラフィックをラインレートで遮断、SIEM ツールから手動または自動で悪意ある IP アドレスをブロック、感染した社内デバイスが既知のボットネット C&C サーバーと通信するのを特定して阻止、トラフィックを地域別にブロック、未使用の IP スペース／未割当の IP アドレスと乗っ取られたドメインをネットワークからブロック、などがあります。

キーサイト・テクノロジーについて

キーサイト・テクノロジーは、エンタープライズ、サービスプロバイダー、政府などのお客様がイノベーションを加速し、あらゆるものが安全につながる世界を実現できるように支援しています。 当社は、お客様がより迅速に低価格で市場導入できるように、設計シミュレーションから、プロトタイプ検証、製造テスト、ネットワークとクラウド環境の最適化などのソリューションを提供しています。 当社のお客様は、世界各国の通信エコシステム、航空宇宙／防衛、自動車、エネルギー、半導体、一般電子機器エンドマーケットなど、多岐に渡っています。 2019 年度の売上高は、43 億ドルでした。 キーサイトについての詳細は、以下のウェブサイトでご覧いただけます。
www.keysight.co.jp