Press Release

2017 年 7 月 21 日
Core Security

Core Security がネットワーク可視化機能を向上し、より容易な調査を可能に

Damballa Network Insight に遡及型分析機能と新しい 2 つのビヘイビアプロファイルを追加

米国ジョージア州アトランタ（2017 年 7 月 20 日）発 – 脆弱性、アクセスリスク管理、ネットワーク検知および対応におけるリーダーカンパニーである Core Security® は、本日、Damballa Network Insight 6.3 のリリースを発表しました。新バージョンは本日より出荷可能です。6.3 の新機能には、デバイスが不正行為を働くようになる前の状態を「振り返る」ことができる遡及型分析機能（Retroactive Analysis）や、新しいビヘイビアプロファイルが追加されています。

Network Insight は、10 年以上におよぶ科学的調査とビッグデータの成果を応用した高度な脅威検知システムとして、実際のトラフィックから感染状態を自動的かつ正確に特定することができます。Network Insight では、デバイスが高度な常駐型の脅威やマルウェアに感染していることを確認すると、全ての証拠を掴んだ上で不正な通信を遮断してリスクに対する優先順位付けを行うため、無駄に誤検知を追跡することもなくなります。

Core Security のプロダクトマネジメント担当シニアバイスプレジデントである Stephen Newman は、次のように述べています。「常に企業は、データを不正行為から守るために、より徹底したインシデントの調査を可能にする正確で相互に関連付けされたデータを求めています。Core Security の遡及型分析機能が提供する過去のコンテキストによって、このような調査をより加速することができます。さらに、トランザクションやコンテキストプロファイルが、Network Insight に対して継続的に追加されていくため、過去に犯罪者がネットワークへの侵入に使用した無数とも言える手段やパターンを検知できる最も強力なソリューションになっています」

■Damballa Network Insight 6.3 の主な新機能

●ネットワーク通信データに対する遡及：

▼遡及型分析 – Network Insight 6.3 では、これまでに発生したコマンド＆コントロールとの通信を過去に遡りながら検知し、不正な通信先が特定できるよう、観測したすべてのインターネット通信をメタデータとして保存できるようになりました。システム管理者は、保存済みの過去のネットワーク通信メタデータを使って調査を実施することができます。

▼新規 API のサポート – RESTful API を使用することで、製品とやり取りをしたりデータを投入したりすることができます。

●高度な脅威の検知に対する革新を加速：

▼新しいトランザクションプロファイラ – パケットペイロード分析を使用した不正トラフィック検知のための技術です。

▼新しいコンテキストプロファイラ – マルウェアが正当なドメインのペリフェラル（C&C 以外、人間が使用可能）との通信に使用する関連ドメインセットを検知するための技術です。

▼DNS トンネリングおよび TOR 検知 – 機能強化された DNS トンネリングおよび TOR プロファイラーが、Network Insight の SIEM 出力および証拠タイムラインにイベントとして含まれています。

●新規導入オプション：

▼Virtual Sensor（バーチャルセンサー）– リモートやブランチオフィスへの導入に最適です。

▼重複 IP アドレス – 日本市場に多く見られる IP アドレスが重複する NAT（ネットワークアドレス変換）を用いたオフィス環境に Network Insight が適用可能となりました。

以上

Core Network Insight 6.3 の詳細やデモのご依頼については、japan@coresecurity.com までお問い合わせください。

【Damballa Network Insight について】

Damballa Network Insight は、マルウェア感染による機密情報の組織外流出という脅威から、組織におけるサーバや端末などを確実に保護するためのセキュリティ・アプライアンス製品です。感染端末を検出するだけではなく、リスク判定エンジンによって感染端末にリスクスコアを付けることで、人手による判断などの運用負荷を最小化します。アラートの嵐に晒されることなく、貴重なセキュリティアナリストを手間のかかる分析作業から解放し、SOC・CSIRT チームの作業効率化を実現します。

【Core Security Corporation について】

Core Security は 1996 年に設立、企業に対して、誰が、どのように、そして何が脆弱なのかを理解するためのセキュリティインサイトを提供しています。Core Security の「脅威アウェア」なアイデンティティとアクセス、ネットワークセキュリティおよび脆弱性管理ソリューションでは、エンタープライズ全体のセキュリティリスク管理に必要となる、実践的なインサイトとコンテキストを提供します。このような共有インサイトによって、お客様はセキュリティの全体像を包括的に理解し、より優れたセキュリティ対応のための意思決定を行うことができるようになります。また優れたインサイトによって、重要なアセットを守る対応の優先順位付けを行い、アクセスリスクを緩和するための迅速な対応が可能になると共に、セキュリティ侵害が発生した場合でも素早い対応を取ることが可能となります。

https://www.coresecurity.com/ja/about

本件に関する一般からのお問い合わせ先

Core Security
e-mail：japan@coresecurity.com
https://www.coresecurity.com/ja/

報道関係のお問い合わせ先

Core Security 広報事務局　株式会社アルサープ
担当：河端・川口
e-mail：coresecurity@alsarpp.co.jp
TEL：03-4405-8773
