プレスリリース
報道関係者各位

2019 年 6 月 12 日
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

チェック・ポイント、クラウドの脅威を可視化する新たなセキュリティ分析ソリューション「CloudGuard Log.ic」を発表

CloudGuard Log.ic、脅威対策機能とセキュリティ・コンテキスト情報をパブリック・クラウドに提供し、
多様な IaaS および PaaS 上の資産を可視化。クラウド上で実行された内容の把握と効率的な調査を支援

米カルフォルニア州サンカルロス ― 2019 年 6 月 11 日--ゲートウェイからエンドポイントまで、包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ（Check Point® Software Technologies Ltd. NASDAQ: CHKP）は本日、クラウド・ネイティブの脅威対策機能とセキュリティ・インテリジェンスを提供する新たなソリューション「CloudGuard Log.ic」を発表しました。CloudGuard Log.ic は、チェック・ポイントのクラウド・セキュリティ製品ファミリーである CloudGuard に新たに加わったソリューションです。CloudGuard Log.ic を使用することにより、動的に変化するクラウド環境の全データ・フローと監査証跡が可視化されるため、クラウド・データとクラウドにおけるアクティビティの意味を把握して、効率よくフォレンジック調査を実施できるようになります。

CloudGuard Log.ic は、クラウド環境で発生した疑わしいアクティビティの確実な検出、脅威や侵入活動のブロック、コンテキスト情報に基づく可視化の機能によって、パブリック・クラウド環境で発生したセキュリティ・インシデントの網羅的な調査を支援します。

チェック・ポイントが CyberSecurity Insiders に委託して実施した、近日公開予定のクラウド・セキュリティ調査では、IT 担当者が悩まされているクラウド運用時のセキュリティに関する課題として、「コンプライアンス」（34%が回答）と「インフラストラクチャのセキュリティ状況の可視化」（33%が回答）が特に多く挙げられています。また、調査対象組織の過半数（54%）は、「運用するクラウド環境がハッキングされたことはない」と回答していますが、「侵害されたかどうか分からない」と回答している組織は実に 25%にも上っています。さらに 15%の組織は、「クラウドでセキュリティ・インシデントが 1 回以上発生した」と回答しています。

CloudGuard Log.ic の中心となるのは、VPC Flow Logs や AWS CloudTrail などの各種ソースのデータを相関分析して、パブリック・クラウド環境のセキュリティ状況を可視化するデータ集積エンジンです。セキュリティ・チームや DevOps チームは、複雑な設定なしで運用を開始できるこのソリューションを使用して、インシデント対応や脅威ハンティングの効率化、セキュリティ・ポリシーの検証、複数のアカウントにわたるポリシーの適用を実現できます。また CloudGuard Log.ic は、Splunk や ArcSight などのサードパーティ SIEM ソリューションとの統合にも対応しています。

市場調査会社 451 Research のフェルナンド・モンテネグロ（Fernando Montenegro）氏は、「クラウド環境がオンプレミス環境と大きく異なるのは、構成要素が短命であることです。仮想マシンのワークロードやインスタンス、コンテナ、サーバレス関数を運用する場合、従来は静的な情報であると見なされていた IP アドレスなどの情報は、セキュリティ調査の証拠としては役に立たなくなります。そのため企業各社の間では、クラウドにネイティブ対応し、フロー・ログやロード・バランサーなどクラウド・ネイティブのコンポーネントの情報を相関分析して内容を補強できる、新たなセキュリティ・ツールが強く求

められるようになっています。こうした要件を満たすツールがあれば、実行時の詳細なイベント情報を入手して、環境の状況を正確に理解し、セキュリティ・ポリシーを厳密に適用できるようになります」と述べています。

CloudGuard Log.ic の主な特徴は次のとおりです。

■ チェック・ポイントの ThreatCloud セキュリティ情報フィードが提供する、不正な IP アドレスなどの情報に基づく高度な脅威対策を実施。
■ 不審なネットワーク・アクティビティやユーザ・アクティビティ、コンプライアンス違反、セキュリティ設定ミスをトリガーとするカスタム・アラートを容易に作成。
■ ユーザ、グループ、ロールに割り当てられた属性を分析し、複合的なイベントを追跡。設定変更を追跡し、個々のユーザまたはロールとの相関分析を実施可能。
■ 重大なイベント、統計情報、トラフィックに基づいてレポートを生成するよう設定。電子メールでの送信や各種 ITMS ツール（ServiceNow、PagerDuty、Jira など）への転送をスケジュール設定可能。
■ CloudBots の自動修復機能を使用して、不正なアクティビティを警告する特定アラートの発生時に自動で対応。隔離や詳細調査のためのタグ付けなど、その他の操作も自動化可能。

チェック・ポイントの製品管理およびマーケティング担当バイスプレジデントを務めるイタイ・グリーンバーグ（Itai Greenberg）は、「CloudGuard Log.ic は、クラウド環境で発生したすべてのアクティビティを詳細に可視化してコンテキスト情報を提供する、エンタープライズ環境向けのソリューションです。不正な活動や侵入活動を検出する情報フィードと組み合わせることで、第 5 世代の大規模サイバー攻撃を未然に防ぐことができます。チェック・ポイントは、新たに製品ラインナップに加わったこの CloudGuard Log.ic をはじめ、クラウド環境を狙う高度な脅威を検出、防御するための最新のセキュリティ・ツールを継続的に提供して参ります」と述べています。

製品詳細はこちら（英語）：https://www.checkpoint.com/products/public-cloud-security-analytics/

本リリースは、米国時間 6 月 11 日に配信されたものの抄訳です。

■チェック・ポイントについて
チェック・ポイント・ソフトウェア・テクノロジーズ（ www.checkpoint.com ）は、世界各国の政府機関や企業など、あらゆる組織に対応するサイバー・セキュリティ・ソリューションを提供する大手プロバイダーです。業界随一の検出率を誇る先進のソリューションにより、お客様のネットワークを、マルウェアやランサムウェアなどの多岐にわたる第 5 世代のサイバー攻撃から保護します。企業のクラウドやネットワークのほかモバイル・デバイスに保存されている情報を、今日の第 5 世代のサイバー攻撃を含めてあらゆる脅威から保護するため、第 5 世代の脅威に対応するマルチレベルのセキュリティ・アーキテクチャを備え、直感的で操作性に優れた総合的かつ一元的なセキュリティ管理システムを展開しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

《本件に関するお問い合わせ先》
広報代行　共同ピーアール株式会社
担当　上瀧・花岡
Tel: 03-3571-5238 / Fax: 03-3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp