SRA の技術情報誌
GS LetterNeo
Vol.194　2024 年 11 月

ネットワークセキュリティの今を追う

中村 託也

アドバンスドクラウドエンジニアリング事業部

はじめに

近年、サイバーセキュリティの世界では大規模な攻撃やインシデントが頻発しています。特に AI を使用したランサムウェアなどによる攻撃の高度化により、既存の技術や人の手だけでは防ぎきれない事例が増えており、セキュリティ対策は新たなステージに進むことを求められています。今回は Cisco 社が発表した最新のセキュリティ技術を説明し、現在のネットワーク業界でどのようなセキュリティ技術が開発されているのか解説します。

従来のネットワークが抱えるセキュリティ問題

従来のネットワークでは、近年発生しているインシデントに対し、対処が難しい状況にあります。それには以下に挙げる二つの大きな原因があります。

- ✓　同じセグメント内の通信を精査、制御することが困難であること
- ✓　リアルタイムでの精査、制御することが困難であること

1 つ目の原因は、通信内容の精査をするファイアウォールなどの装置が OSI 参照モデルにおけるレイヤ 3 を終端としている装置に限られているためです。同じセグメント間をつなぐレイヤ 2 のスイッチ等では、ファイアウォールを通過する通信フローの精査が不可能であり、

レイヤ 3 の装置を跨ぐ通信、つまりそれぞれ別のセグメント間での通信のみがファイアウォールでの精査対象となります。特に一つのセグメントに対し、多くの装置が接続されているような環境では、同じセグメント内での通信を精査することが困難となります。

同じ理由で、インシデントの発生時にリアルタイムでその通信を制御することは困難を極めます。これはレイヤ 3 の装置に通信が到達した際に初めて通信のふるまいについて精査が行われるためで、インシデントの発生に気付いた時にはすでに、同じセグメント内の多くのホストに影響がでてしまっているという状況に陥りがちです。

このような動作に対し、どのようなソリューションを提示できるかが今後のネットワークセキュリティの大きな課題となります。

次世代セキュリティソリューションの登場

従来のネットワークが上で述べたセキュリティ上の問題を抱える中、2024 年 4 月に Cisco 社はデータセンターおよびクラウドの保護の新しいアプローチとして「Cisco Hypershield」を発表しました。

本ソリューションの特徴としては初期段階から AI を使用した開発 を念頭において設計されており、怪しいふるまいに対し AI による自動かつ高速の対応が可能であること、また、既存のセグメント構成に囚われず、ホスト単位でのマイクロセグメンテーションでの通信制御が可能であることです。

2024/11/7 段階ではまだ開発、試験段階ではあるソリューションですが今後のネットワークセキュリティにおける転換点とも言える技術であり、大いに注目を集めています。

マイクロセグメンテーションでの管理

「Cisco Hypershield」では既存のセグメント構成に囚われないマイクロセグメンテーションでの通信の管理が可能です。

マイクロセグメンテーションとは、社内外すべての通信を信頼しないことを前提としたセキュリティ対策「ゼロトラスト」を実現するためのアプローチの一つであり、PC などの端末やサーバー、コンテナなどのホストに対して論理的に境界を設けるという考え方のもとで、単一のホストがマルウェアなどに感染した際でもネットワーク内部の同一セグメント内の通信による被害を最小限に抑える仕組みのことを指します。

このソリューションを使うと、クラウド・オンプレ・仮想・物理・コンテナを問わず、分散配置されたワークロードの依存関係を可視化することで、最適なセグメンテーションの実装を可能になります。

また、マイクロセグメンテーションを実現するにあたり、このソリューションでは eBPF という監視対象の Linux ホストをカーネルレベルの動作から監視、管理できるオープンソース技術が使用されています。

この技術の獲得のため、Cisco 社は企業向け eBPF 大手プロバイダーである Isovalent 社を買収しています。

カーネルレベルの動作を検知することが可能であり、既存のネットワークであった、レイヤ 3 の装置まで通信が到達して初めて精査できるという問題点に対して、大きなアドバンテージがあります。

AI による管理

「Cisco Hypershield」では、AI ネイティブな設計により下記のようなアクションを自動で行うことが可能です。

- ✓ ネットワーク全体の依存関係のマッピング作成、セグメンテーションの実施
- ✓ 各ホストの通信に対する情報収集
- ✓ 各ホストの通信のふるまい検知、アノマリー検知
- ✓ 各脆弱性のレベル分け、対応の優先度付け
- ✓ 違反ホスト発生時の警告の表示、通信の隔離、ブロックなどの制御
- ✓ シャドープレーンでの新ポリシーや新バージョンの検証と精査

ネットワーク全体の依存関係をマッピングする機能、各ホストの通信ふるまいからアノマリーを検知して通知、隔離、ブロックするなどの通信制御機能、そして実際にインシデントが発生した際の優先度付けから制御動作に至るまでの一連の流れなど、様々な動作を AI で管理することが可能です。

また、データを送受信するための伝送経路「データプレーン」が二つ存在しており、本番用のプロセスを実行している裏で、シャドープレーンにて新ポリシーや新バージョンを検証することが可能です。このシャドープレーンのおかげで、可用性を損なうことなく，ポリシー適用とバージョンアップに必要な工数大幅に削減することが可能です。

このような AI の動作により、ホスト単位での依存関係を考慮したマイクロセグメンテーションの実装、また、リアルタイムでの通信制御という、従来のネットワークで特に大きい課題だった点に対し、有効なソリューションを提示することが可能です。

おわりに

今回は Cisco 社の動向を通じてネットワークセキュリティの最新技術の紹介をしました。まだ開発、導入試験段階であるものの、非常に革新的な技術であり、有益なソリューションです。また機会がありましたら、その後の展開についても皆さんにお伝えできればと思います。

引用文献

[1] Cisco Japan Blog / セキュリティ / Cisco Hypershield でセキュリティを再定義、AI スケールのデータ センター向け超分散型セキュリティ (https://gblogs.cisco.com/jp/2024/07/cisco-hypershield-security-reimagined-hyper-distributed-security-for-the-ai-scale-data-center/)

GSLetterNeo Vol.194
2024 年 11 月 20 日発行
発行者　株式会社 SRA 技術本部 先端技術研究室

編集者　熊澤努　方 学芬
バックナンバー https://www.sra.co.jp/public/sra/gsletter/
お問い合わせ　gsneo@sra.co.jp

株式会社SRA
〒171-8513 東京都豊島区南池袋 2-32-8

夢を。Yawaraka Innovation
やわらかいのべーしょん