ゼロトラストセキュリティ

– Zero trust security model–

Shishio Tsuchiya
shtsuchi@arista.com

ARISTA

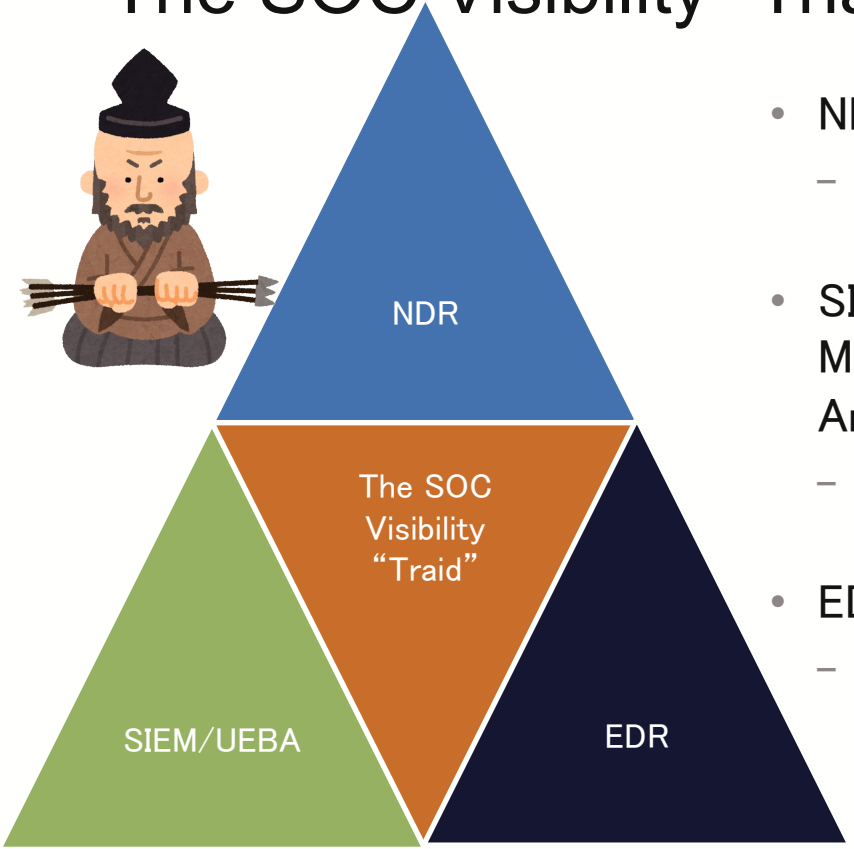
ゼロトラストセキュリティを改めて

- **社内外問わず何も信頼せず常に検証し対応する**

– 2020 Forrester Research ,John Kindervag

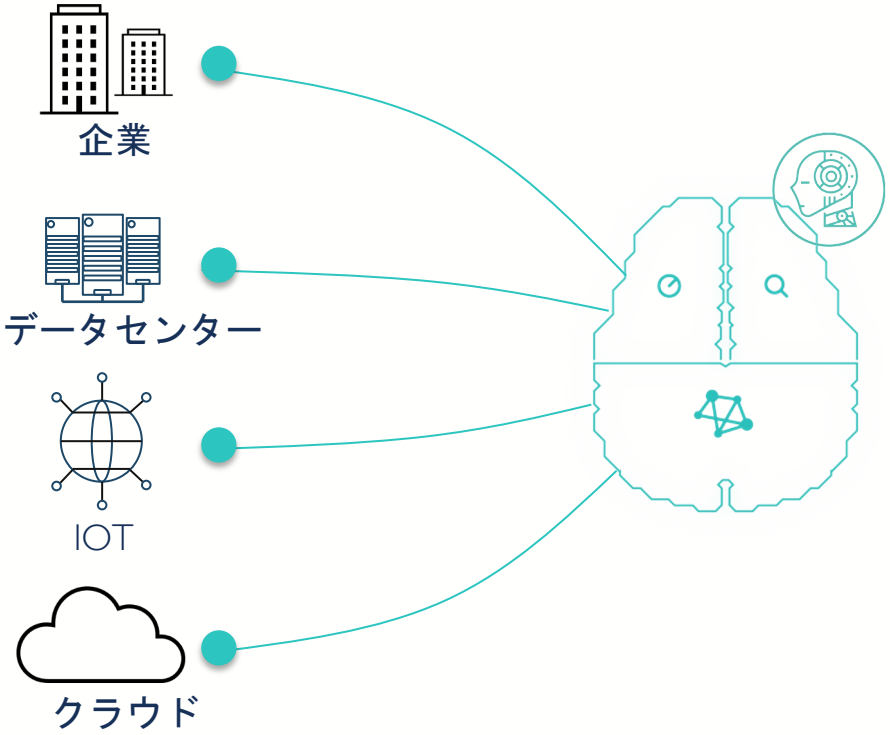
図表2:NISTによるゼロトラストの考え方

The SOC Visibility “Triad”(SOC可視化トライアド)



- NDR(Network Detection and Response)
  - ネットワークを包括的に可視化をし、脅威や不審な振る舞いを検出し、未然に対応する
- SIEM(Security Information and Event Management)/UEBA(User and Entity Behavior Analytics)
  - ITインフラ、アプリ、セキュリティツールが生成するログの収集と分析
- EDR(Endpoint Detection and Respons)
  - パソコンやサーバー(エンドポイント)でのプロセス、メモリ状態、動作設定などを分析

NDRにおけるAI/MLの活用



- 全てのネットワーク機器よりパケットを収集
- デバイス/ユーザ/アプリをプロファイリング追跡
- 複雑な脅威を検出
- トリアージ,調査,レスポンスを自動化

NDRが検知/対応したユースケース

ユースケース	業種	状況	結果
標的型攻撃の検出	銀行・証券系企業 	AWS管理者のログイン情報が盗まれ、自社のクラウド環境への不正アクセスがあった	不正なChromeエクステンションが使われ、ログイン情報を含むブラウザーの情報が盗み出されていたことが判明
ランサムウェアによる攻撃	 製造業	ランサムウェアが企業内のある地点から社内へ拡散	ラテラルムーブメントを検出し、対策を講じることで影響を最小化
内部の人間による不正	一般消費者向け金融業 	IT契約社員が、IP電話の通話を不正に録音し、社外に持ち出していた	NDRによりIP電話を特定、通常と異なる動作を検知、暗号化された録音データの社外への転送とそのデータへのアクセスを発見
企業スパイ	エネルギー 	数千台のIPカメラを含むネットワーク上のすべてのデバイスを自動的にプロファイリング、他のカメラが通信していない送信先と通信している1台のカメラを検出	問題の送信先と同じ送信先にFTPアクセスした複数のデバイスを特定し関係IT業者の所有のデバイスであることが判明、データセンタや重要インフラに設置されていた
知的財産漏洩の内部犯行	放送会社 	電子メールによるファイル送信頻度は低く、データ量も少ないため従来仕組みでは見つけることが難しかった	同じ様な業務、類似したデバイスやユーザと比較して、Low and Slowでありながら特定のデバイスやユーザが異常であると判断し法的措置へ

NDRが検知/対応したユースケース

ユースケース	業種	状況	結果
リモートデスクトップのハッキング	政府、自治体 	米国の浄水場の制御システムにロシア製RDPソフトウェアがインストール、定期的に通信され部外者にアクセスできる状態であることを NDRにて検知	セキュリティパッチが適用されていないWindowsサーバーが存在していることを警告し事態を迅速に修復した
産業システムへの不正アクセス及び情報漏洩	石油天然ガス企業 	SIEM,EDRを導入していたが、繰り返し発生する不正アクセス、侵入行為の原因特定が困難であった	NDRによりEDR、SIEMでは管理できなかった2週間に一度アクセスするIメンテナンス業者のデバイスを検出した。経過監査、トラフィック調査からHMI（ヒューマンインターフェイス）システムや複数のSCADA（産業監視制御）デバイスにアクセスを確認しサイバー攻撃と判断した。その後APT28として知られるロシアのサイバー攻撃グループによるものと判明した。

まとめ

- ゼロトラストアーキテクチャーを実現するNDRおよびそのユースケースを紹介
- ネットワークとAI/MLで追跡/脅威を検出し対応する

参考URL

- NIST SP800-207「ゼロトラスト・アーキテクチャ」の解説と日本語訳
  - https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html
- ゼロトラスト・セキュリティモデル(Wikipedia)
  - https://ja.wikipedia.org/wiki/%E3%82%BC%E3%83%AD%E3%83%88%E3%83%A9%E3%82%B9%E3%83%88%E3%83%BB%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%83%A2%E3%83%87%E3%83%AB
- Awake Security Demonstration
  - https://www.youtube.com/embed/5D4Y2V3eOEw?rel=0&wmode=transparent