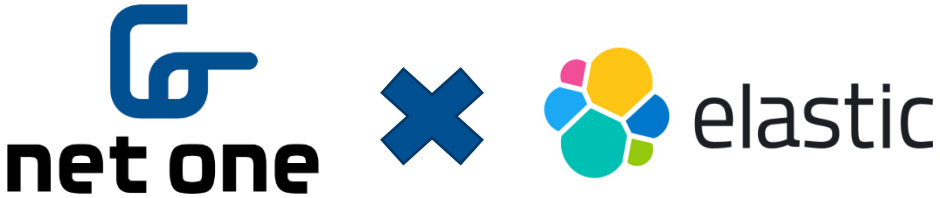


セキュリティ運用の高度化

2021年11 月 25日

ネットワンシステムズ 株式会社
西日本事業本部　第２営業部

ネットワンシステムズ　×　elastic　ポイント

1 センサー機器の新しい活用

これまでの警報検知だけでなく、ログを集約し傾向を分析できることでこれまで以上にセンサーを活用することができます。
またセキュリティ運用のDX推進の観点で　AI・機械学習を活用した自動検知から対応までのスピードアップを図ります。

2 インシデント発生時のログ確認の簡素化

ログや警報を可視化。
Web画面から簡単にログ単位の情報を閲覧することができます。

3 短期間での構築によるスピード感

サーバーの搬入から構築、運用開始までは短期間で対応可能。
既存のセンサーを活用できるので　サーバーを設置したらすぐにログデータを収集できます。

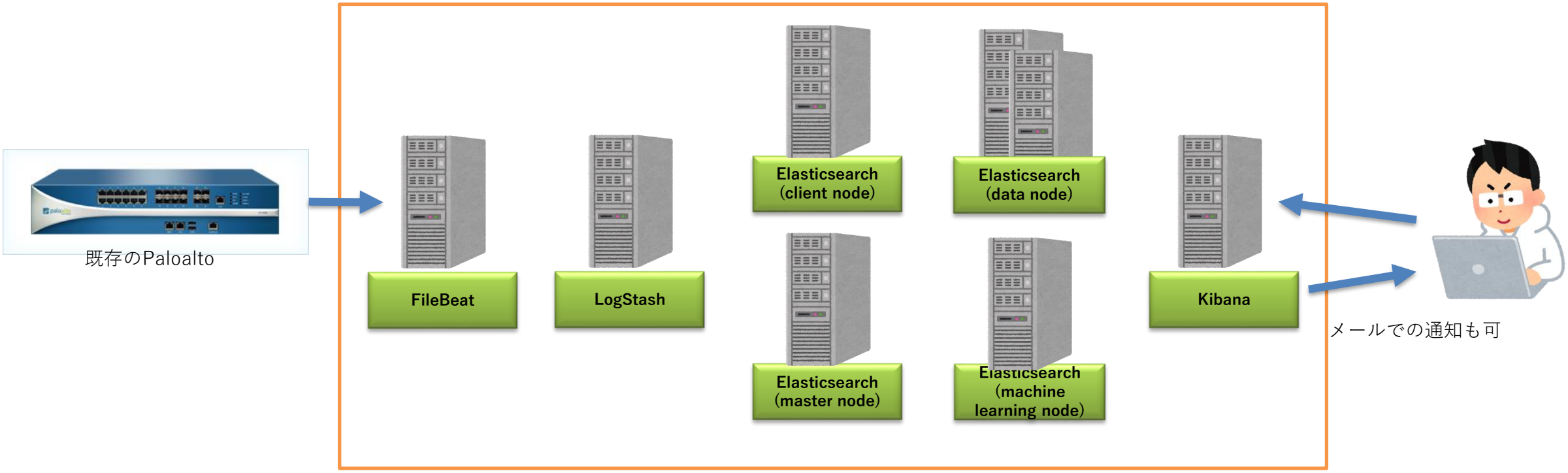
4 導入実績

NOSにて公共機関のお客様にも導入実績がございます。

Elasticsearch Machine Learningを用いた異常検知

特徴

従来の閾値ベースの異常検知システムとは違い、機械学習による異常検知を行う
正常な振る舞いをElasticsearchのMachine Learningにより学習し、異常な値や状態を通知する
正常時と異なる振る舞いを認識することにより、障害が発生する前に障害となりそうな状態を予測する



※サーバーは仮想OSでも稼働可
ログ量により台数が異なります

Elastic Security

セキュリティ運用の高度化

2021年11月

急速な変化を促すグローバルなトレンド

セキュリティの課題は急激に深刻化している

トレンド #1:

DXとクラウド移行の加速

175ZB

全世界の2025年*までのデータ増加の予測

288

平均的な企業が管理しなければならないアプリケーションの数**

トレンド #2:

敵は目的を達成することにとても意欲的

$10.5T

2025年*までに予想されるサイバー犯罪のグローバルなコスト

70%

ゼロデイや曖昧なマルウェアを含めたマルウェア攻撃

* IDC, Data Age 2025 report
** Blissfully, 2020 Annual SaaS Trends report
*** Cybersecurity Ventures, Cyberwarfare in the C-Suite report
**** Infosecurity Magazine, Evasive Malware Threats on the Rise article

elastic

セキュリティ・チームは維持するのに奮闘している

リスクを減らすのが難しい – 素早く答えが必要

ハイブリッドな視認性が乏しい

80%

の会社が過去18ヶ月にクラウドの侵害を受けている*

データのサイロが多すぎる

90%

のITリーダーが、データ・サイロがDXを妨げていると言っている**

アラート疲れは改善していない

49

平均的な企業で使われているセキュリティ技術***

非効率的なプロセスのサイロ

30%

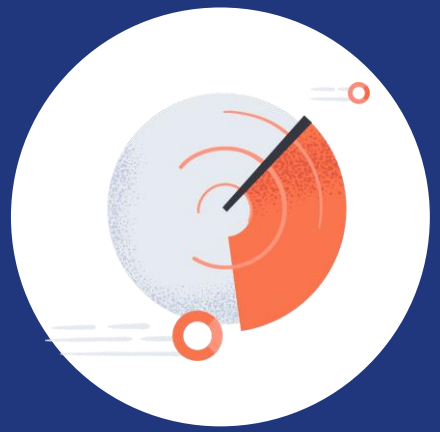
のSOCがセキュリティ、IR, 運用の間にサイロ気質を持っている****

* IDC, Cloud Security Survey: Top Identity and Data Access Risks
** Salesforce.com, IT Integration Challenges for Digital Transformation Report
*** Security Boulevard, Too Many Security Tools Can Be as Bad as Too Few
**** SANS Institute, Common and Best Practices for Security Operations Centers

elastic

Elasticsearchがもたらす価値

スピード、スケール、関係性



待ち時間をより短く、
損害を最小に

複雑な脅威を
より早く改善

調査と対応を迅速化

elastic

既存のセキュリティ対応製品の機能は限定的

スピード、スケール、関係性の欠如

	視認性	検知	調査	対応
期待	どんな データ も全て	機械学習 /異常値	簡単に 切り口を 変える	タスクを 自動化
現実	スケール しない	背景の データが 不十分	時間が かかり すぎる	日常的な タスク のみ

elastic

セキュリティ運用の高度化

いかに前進するか?

レガシーなセキュリティ運用		モダンなセキュリティ運用
集中化とサイロ	→	分散化とマルチテナント
データの集合体	→	高い忠実度の検知
アラート、クエリー、ピボット	→	情報に基づいた調査
エスカレーションに最適化	→	レスポンスに最適化

elastic

エンドポイントからのアラートを1日にいくつ受け取っていますか？

elastic

SOCからのエンドポイントのコントロールが重要

70%の侵害がエンドポイントから行われるからだけではない

	視認性	検知	調査	対応
スタンドアロンのエンドポイントの価値	細かい粒度のビュー	早期の表示	監査証跡	ビルトインの防止機能
SIEMに対するエンドポイントの価値	大規模な収集	APT検知の高い忠実性	脅威ハンティングの状況	封じ込めとブロッキン

elastic

将来に向けて

ビジネスのリスクを取り除くためのセキュリティ運用の高度化

エンドポイント駆動型SIEM = 高度なセキュリティ運用

複雑な攻撃のブロック

- 既知と未知
- 起動前のランサムウェアe
- MITRE TTPs、
  進化した脅威

→ 待ち時間の短縮

超高度に忠実な検知

- 偽陽性の最小化
- ホストとユーザーの深い背景
- 重要なビジネス状況と直接関連

→ 速いMTTD

大規模に最適化された対応

- アドホックな相関
- リアルタイムな背景情報収集
- ホストで封じ込めと行動

→ MTTI/Rを減少

elastic

Elastic Security

検知, 分析, 調査

収集

データソース

P/I/SaaS

User

Network Activity

Endpoint

Server

Wire & Flow Data

Code Repository

Connected Devices & Physical Security

収集と防御

Elastic Agent

正規化

対応

対応

Elastic Agent

SOAR

SIRP

ITSM

Custom

レポーティング

Lens + Canvas

速くスケーラブルな検索機能上に構築
データがどこであれ、検索機能を提供

高度なセキュリティや監視などの基盤

将来のハイブリッド環境のための設計

elastic

elastic

公共機関における Elastic Securityの導入事例

米国国土安全保障省は、ECS FederalとCDM Dashboard IIを構築し、連邦政府機関全体のサイバーセキュリティの脅威を監視

「連邦政府の次世代のサイバー分析エコシステムを構築する我々の最先端のサイバーセキュリティ・ソリューションと技術パートナーのElasticの革新性・完全性に自信を持っています」

– George Wilson, President of ECS

PROFILE

About:米国国土安全保障省(DHS)と一般調達局(GSA)が共同で管理するCDM(Continuous Diagnostic and Mitigation)プログラムはフェーズ3に進んでおり、連邦政府機関のネットワークアクティビティを特定して管理している。

Industry: 政府

Location: アメリカ合衆国

GOALS

- 政府全体のサイバーセキュリティの把握と監視
- ネットワークおよび境界コンポーネント、ホストおよびデバイス・コンポーネント、保存中および転送中のデータ、ユーザーの動作に対するセキュリティのコントロールを動的に監視する機能を提供

SOLUTIONS

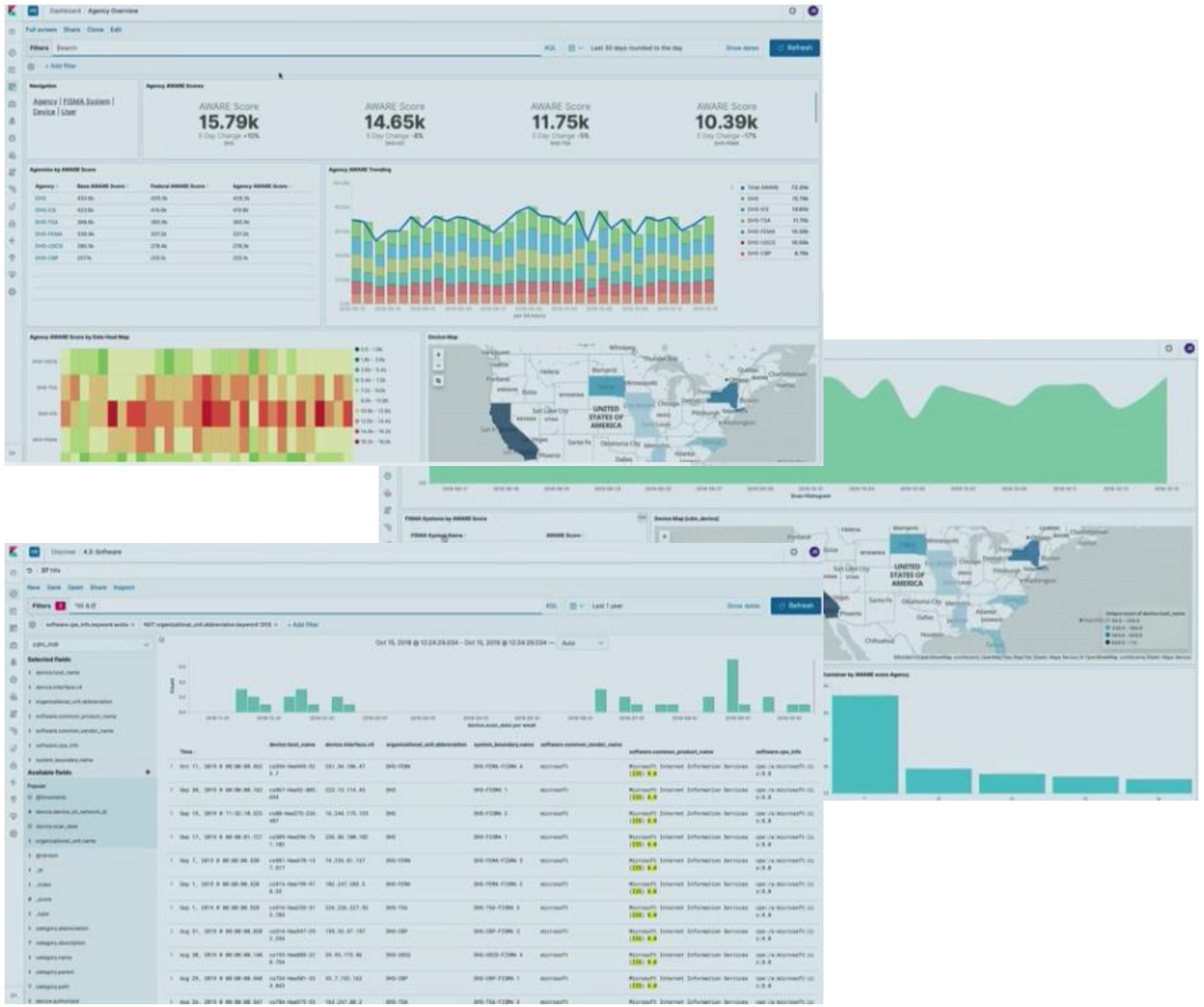
- 新しいサイバー分析エコシステムであるCDM Dashboard IIを**Elasticsearch**や**Kibana**などのElasticツールを利用して実装
- **Elastic Stack**の速度、拡張性、柔軟性、APIによる互換性により、政府機関は大量のデータを取り込んでクエリを実行し、効率的に脅威を検出

RESULTS

- 省庁はペタバイトのデータを管理し、数秒で検索結果を得られ、非構造化データに対してアドホック・クエリーができる脅威分析プラットフォームを構築
- タイムリーな脅威の検知と対応、効率的な省庁間の情報共有
- 高い相互運用性により、既存のツール既存のツールやレガシー・アーキテクチャーと連携

Watch customer video

CDM DashboardへのElastic採用理由



- 相互運用性
  - 強力なAPI
  - SOARやThreat Intelligenceといった他の機能との連携が容易
- 拡張性
  - データやソースの増加に対応可能
- 検索のパフォーマンス
  - Schema on Write vs Schema on Read
  - 構造化データ
- マルチ・テナント
  - ロール、属性をベースとしたシンプルなアクセス制御
- ライセンス体系
  - 柔軟な課金モデル

陸軍研究所通信電子研究開発エンジニアリングセンターはElastic Cloud Enterpriseをサイバー攻撃対策に活用

「データを効率的に調査し、対処のための洞察を得たり、ネットワーク内の動向を把握するのにElastic Stackを活用しています。」

–Curtis Arnold, Chief Sustained Base Network Assurance Branch

PROFILE

About: 米国陸軍の情報技術および統合システムセンター

Industry: 防衛

Location: アメリカ合衆国

GOALS

- 膨大な量のデータの取扱いと、機敏な脅威ハンティング能力の両方に優れた能力を発揮できる、スケーラブルでレジリエントかつ信頼性を備えたプラットフォーム

SOLUTIONS

- **Elastic Cloud Enterprise**による包括的なデータ・ソーシング
- **Kibana**によって、セキュリティに関する情報にあまり詳しくない人にもわかりやすい説明が可能

RESULTS

- 強化されたポリシーの適用、異常の検知、脅威ハンティング、検索の可視化、プログラム・アクセス機能

Read Customer story

Watch customer video

OAK RIDGE National Laboratory

オークリッジ国立研究所の大規模なログ監視と異常検知

「私たちのSOCやアナリストがやりたいことに費やす時間を節約でき、それがSplunkからElasticsearchに移行する価値でした」

-Larry Nichols, Cybersecurity Engineer

PROFILE

About: 基礎及び応用研究を行う研究所

Industry: 研究機関

Location: アメリカ合衆国

GOALS

- セキュリティ・ツールのコスト削減
- 研究者が利用できる、ログを中央に集約するツールを見つける

SOLUTIONS

- **Kibana, Logstash**及び**Elasticsearch**を使って暗号化されたデータ
- **X-Pack**セキュリティでロール・ベースのアクセス・コントロール

RESULTS

- エンドポイントからデータを集める能力の向上
- 検索時間を分単位から秒単位に短縮

Read Customer story

Watch customer video

Elastic Securityと機械学習についての詳細は、
こちらのオンデマンドウェビナーをご覧ください。

https://www.elastic.co/jp/webinars/machine-learning-in-security?blade=iotsymposium&hulk=3pc

elastic

ご連絡先

ご質問やご提案依頼等ございましたら下記担当者までご連絡ください。

ネットワンシステムズ株式会社
西日本事業本部 第2営業部 営業第1チーム
篠原 匠
TEL：070-4809-6099　FAX：06-6395-7349
E-Mail:s-shinohara@netone.co.jp

つなぐ ∠ むすぶ ∠ かわる

net one