MineMeldを活用した脅威情報自動化基盤の構築

パロアルトネットワークス株式会社

Agenda

- MineMeldによる自動化基盤の構築
  - 脅威情報自動化の必要性
  - 脅威インテリジェンスの自動化を実現するMineMeld
  - AutoFocus with MineMeldによる脅威インテリジェンス自動化基盤
  - MineMeldのユースケース

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

脅威情報の課題

「脅威情報」の活用を全て人（手動）で実装するのは限界がある

- 脅威情報は新鮮である必要がある
- 設定後、ブロックして初めて意味がある
- 設定投入時は既に古い可能性がある
- 廃れた情報は随時削除してコスト削減に繋げる必要がある

セキュリティ・オートメーションが必要

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

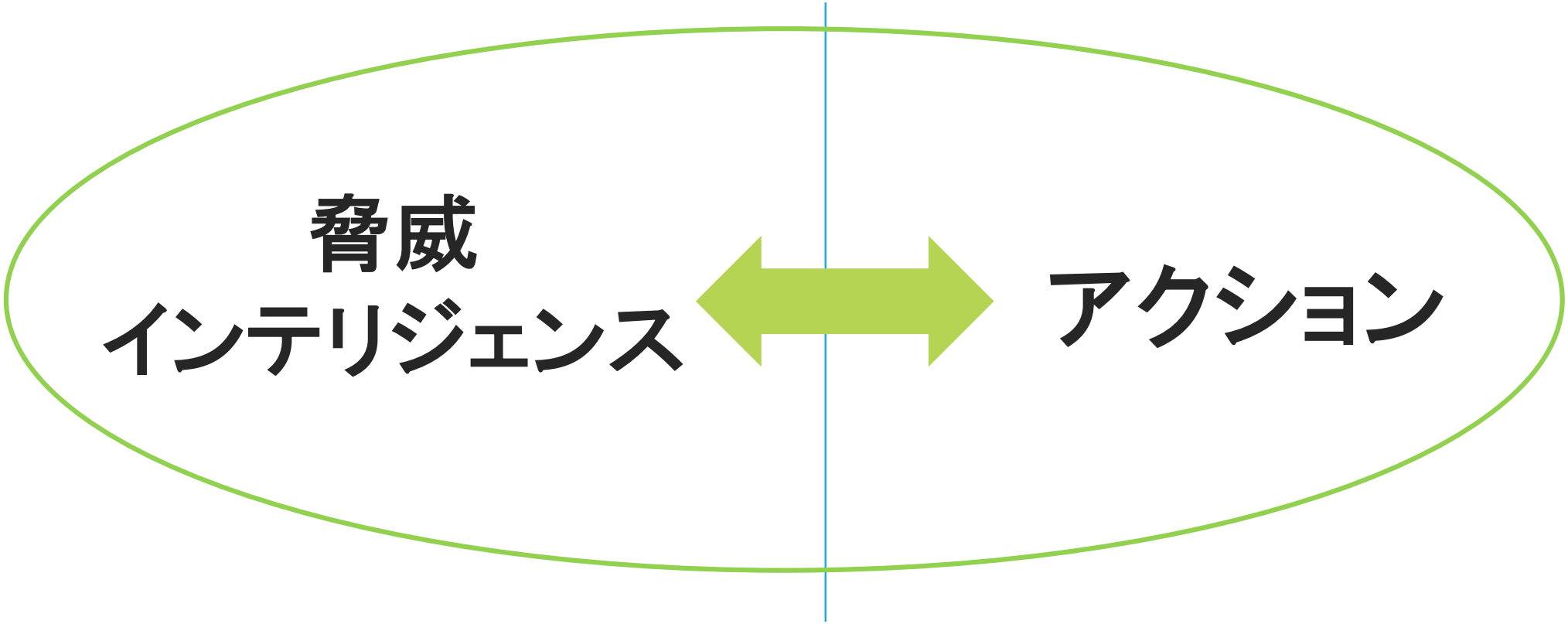
脅威情報自動化へのアプローチ

- 脅威情報について、人手による対応は様々な面で制約が大きい
  - 人的リソースの確保の必要性
  - リアルタイムでの対応は困難
  - いつ発生するか分からない新しい脅威に常に対処しなければならない

- MineMeldを活用したセキュリティオートメーションの構築
  - 脅威インテリジェンスからIOC情報の抽出
    - 不正なIPアドレス、URL、ドメイン、マルウェアハッシュ値, etc
  - 抽出した情報のセキュリティデバイスへの自動適用
  - 単一の情報ソースではなく幅広いOSINT（Open Source Intelligence）との連携が必要

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

パロアルトネットワークスが提供する「脅威インテリジェンス」とは



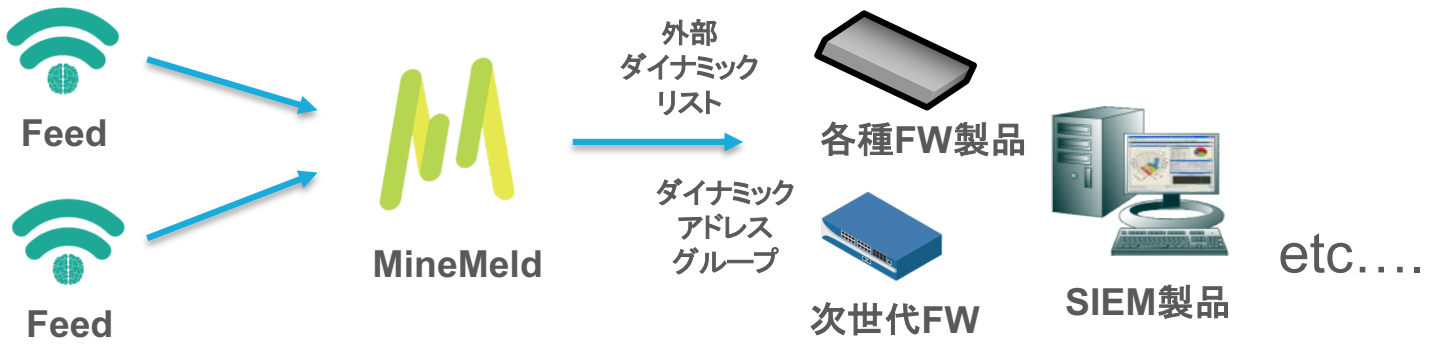
MineMeldはこの2つを紐付けて
セキュリティ・オートメーションを実現！

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

「脅威インテリジェンス」の自動化を実現するMineMeld

- MineMeldは、複数の「脅威情報」を外部のフィードから収集して統合し、それらの情報を基に各種セキュリティ機器で**ブロック**できるように出力する**脅威情報自動化ツール**
- 「脅威情報」は**不正なIPアドレス、URL、ドメイン**の他に、マルウェアファイルの**ハッシュ値、User Agent、Mutex**等をサポート

※MineMeldは無償のオープンソースのツール
サポート：コミュニティサポート（掲示板でIssueを報告、ベストエフォート対応）



 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

MineMeldで対応可能なこと

- 脅威インテリジェンスサービスからの自動収集（OSINTを活用）
- 収集した脅威情報の抽出およびセキュリティデバイスへの配信
- 配信形式のカスタマイズ
  （標準形式, CIDR, JSON, CSV, McAfeeフィード, Symantecフィード, etc）
- ホワイトリスト、ブラックリストによる制御（手動設定）
- AutoFocusとの連携によるWildFire脅威インテリジェンスからの脅威情報取得
  （AutoFocus契約が必要）
- エンタープライズ向け脅威インテリジェンスサービスとの連携
  （Soltra, PhishMe, Proofpoint, Palo Alto Networks AutoFocus, ANOMALI, etc.）

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

脅威インテリジェンス自動化基盤 – AutoFocus with MineMeld

- AutoFocus = 脅威情報の自社・業界別での動向や未知の脅威の調査・分析を迅速化
- MineMeld = 脅威情報をブラック・リスト化して外部にフィードするフローの自動化

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

AutoFocus with MineMeldによる脅威情報自動化の流れ

弊社脅威DB,
パートナー, OSINT
脅威情報をフィード

WildFire
PAN-DB
FINANCIAL SERVICES ISAC
SOLTRA
STIX
TAXII
ANOMALI
proofpoint
SPAMHAUS
PHISHME
etc…

可視化による
調査・分析

AF
MineMeld

自動的に取得した
脅威を配信

次世代FW
自動で
脅威をブロック

TANIUM
EDR製品
内部感染
高速検索

SIEM製品
ログ相関
アラート

etc.…

①収集フェーズ　②統合・分析フェーズ　③アクション・フェーズ

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

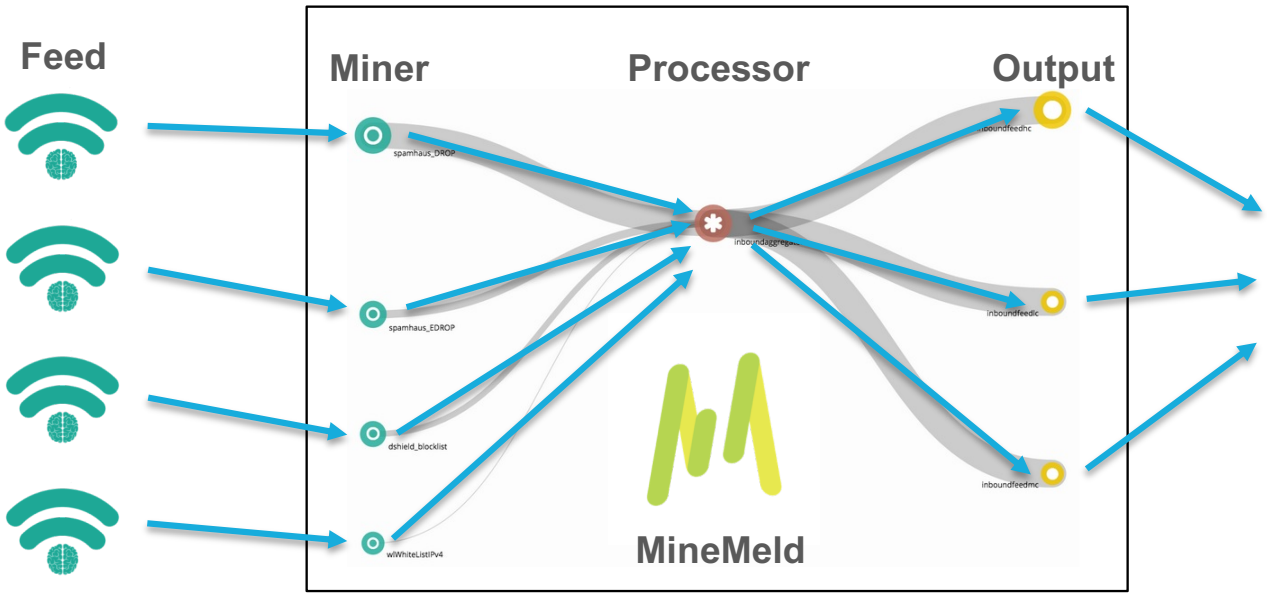
MineMeldのアーキテクチャ

- MineMeldはLinux(Ubuntu)上で動作
- AutoFocusライセンスを購入することにより、AutoFocus WEB-UI上でMineMeldを自動デプロイし、サポート付きで利用可能。また、AutoFocusの検索条件から任意のインジケーターをフィードすることも可能
- 無償版で利用する場合、サポート環境は以下の4種類
  - VMWare Desktop
  - Microsoft Azure
  - Amazon EC2
  - Ubuntu Server 14.04

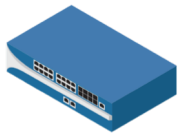
 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

MineMeldのアーキテクチャ

- MineMeldには3種類のNodeが存在する
  - Miner（マイナー）：外部Feedから脅威情報を収集
  - Processor（プロセッサ）：各種脅威情報を統合
  - Output（アウトプット）：セキュリティ機器で利用できる形に出力



複数のMinerから「脅威情報」をProcessorに取り込み、Outputからセキュリティ機器に情報を受け渡し可能



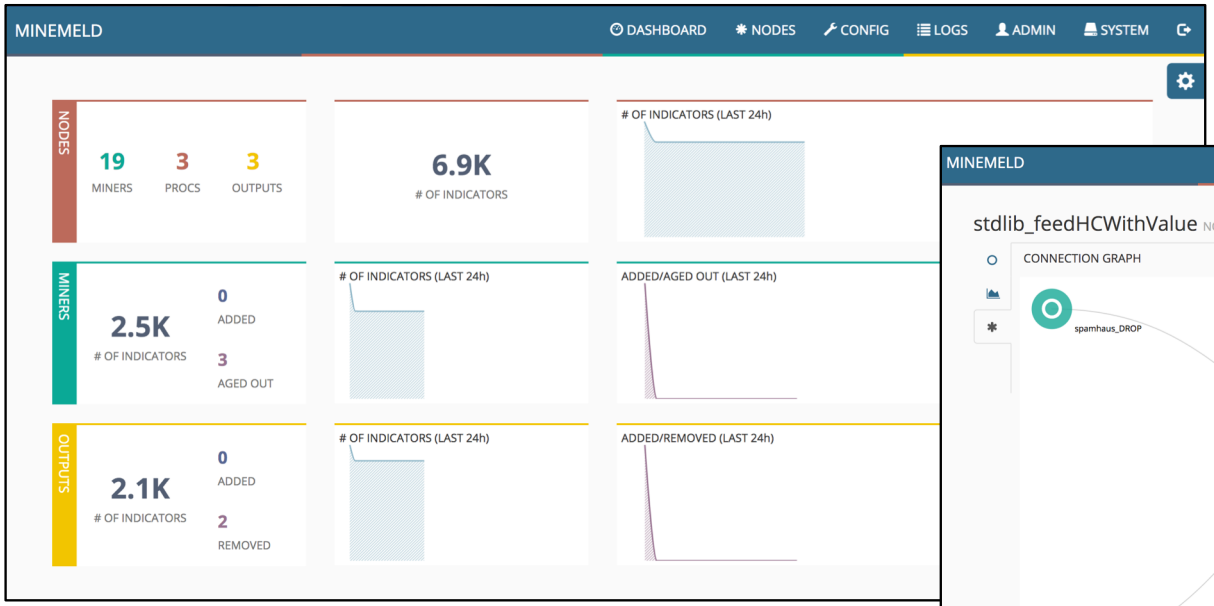
次世代FW

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

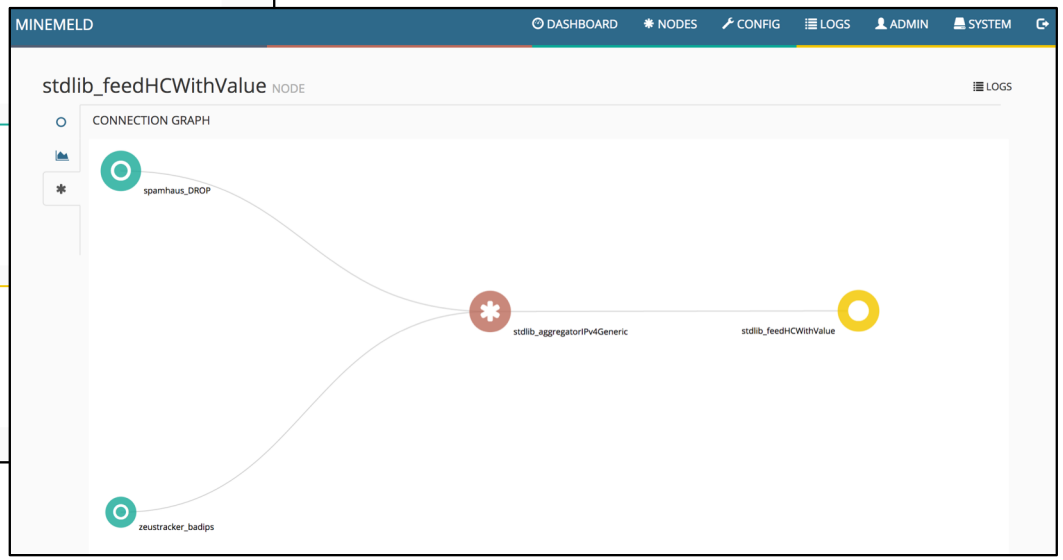
MineMeldのアーキテクチャ

- MineMeldはWeb-UIで設定・管理する（無償版）

Dashboard画面



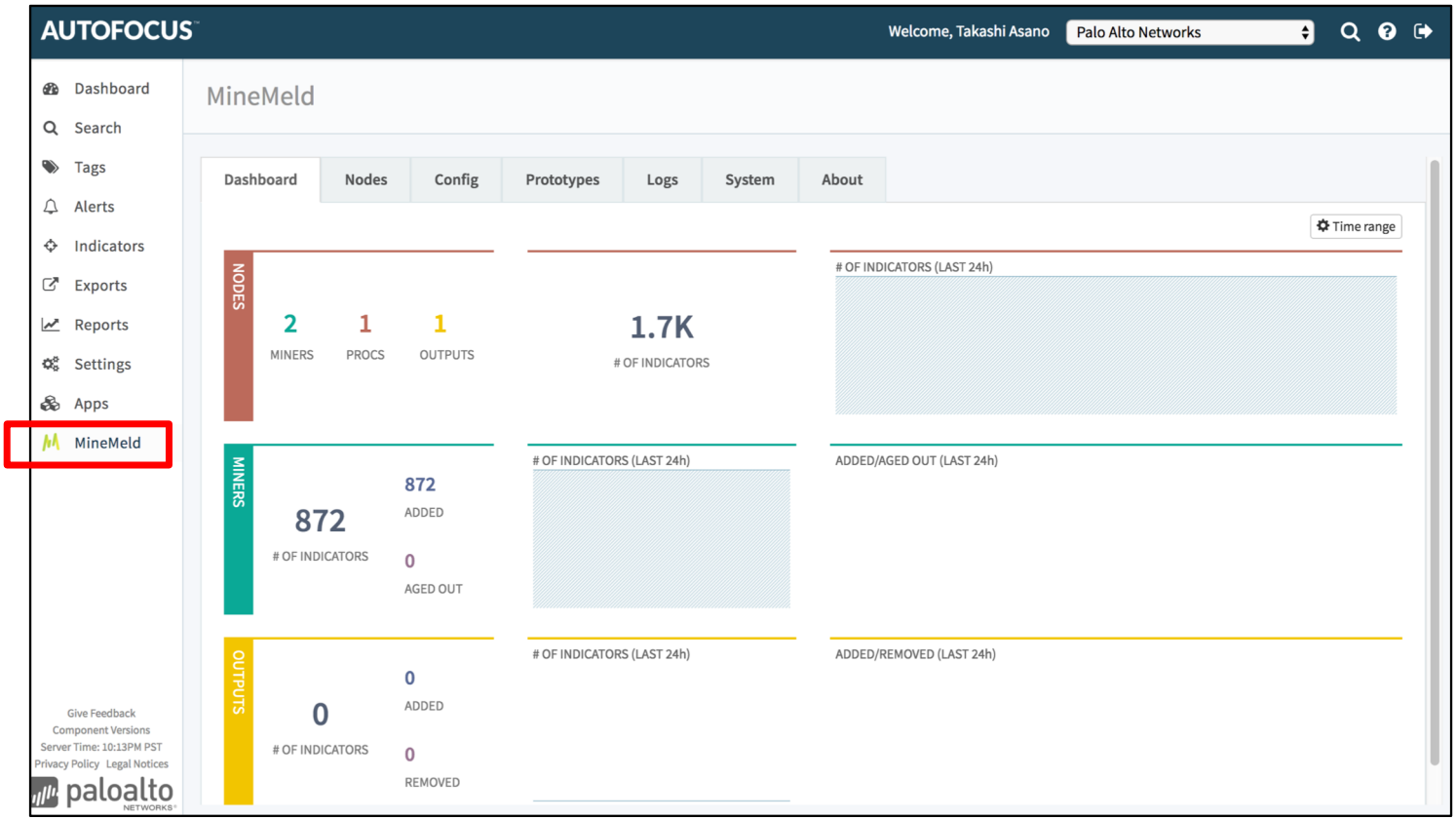
設定済み脅威情報の画面



 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

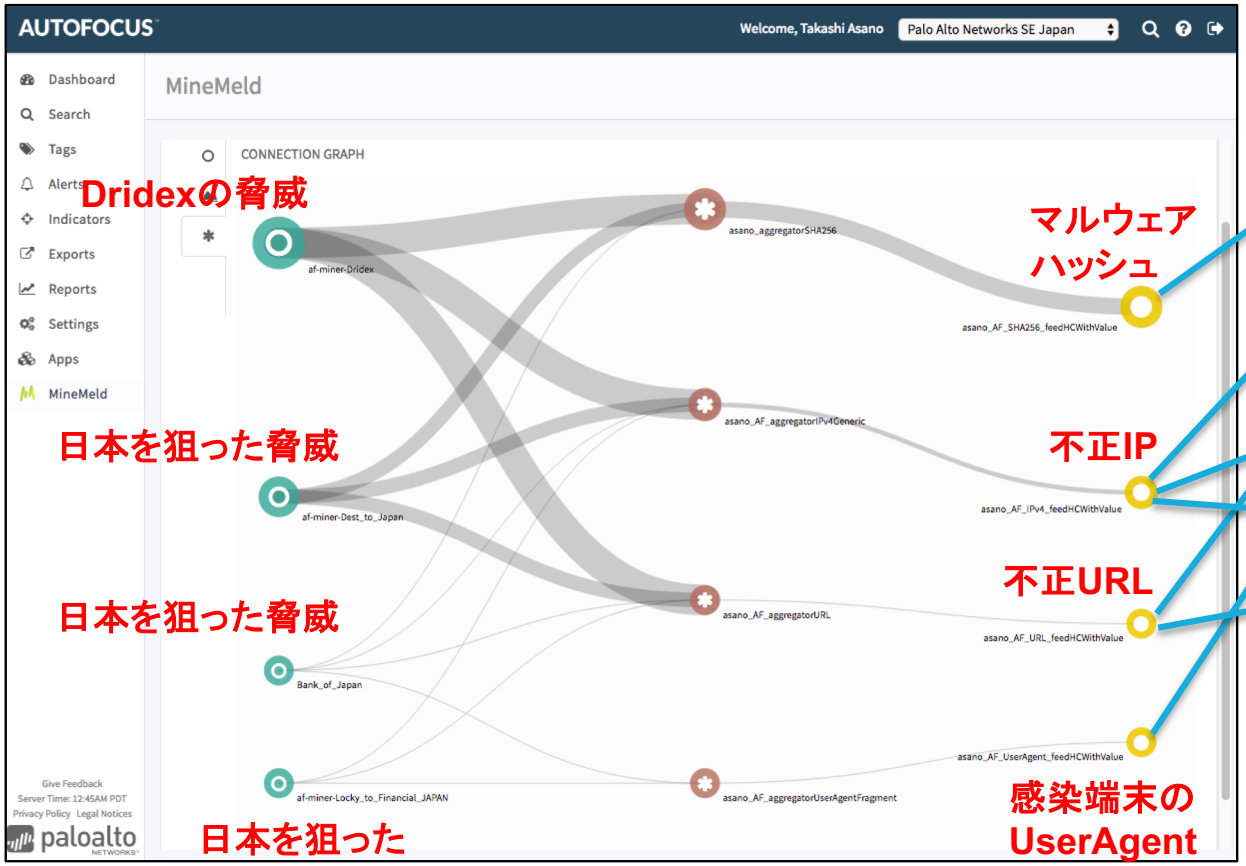
MineMeldのアーキテクチャ

- MineMeldはWeb-UIで設定・管理する（有償版）



 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

MineMeldによる自動化基盤設定例



Dridexの脅威

日本を狙った脅威

日本を狙った脅威

日本を狙った
Lockyファミリー

マルウェア
ハッシュ

不正IP

不正URL

感染端末の
UserAgent

SIEM製品

splunk> QRadar ArcSight

他社製セキュリティ
デバイス

次世代FW

次世代FW側でダイナミックリスト（EDL）を事前に設定しておくことにより、脅威情報が自動的に取得・反映され、動的にブロックする運用が開始される

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

自動化基盤でサポートする外部ソース

- サポートしている外部ソースやOutput方式　※最新のリストはgithub内のPrototypes参照
  - https://github.com/PaloAltoNetworks/minemeld/wiki/List-of-Supported-Nodes

OSINT ※無償

- AlienVault Reputation
- Bambenekconsulting
- DShield
- Emerging Threats Open rulesets
- badips.com
- Binary Defense Systems Artillery
- blocklist.de
- BruteForceBlocker
- hailataxii.com
- Malware Domain List
- OpenBL
- OpenPhish
- Ransomware Tracker
- sslbl.abuse.ch
- Virbl
- ZeuS Tracker
- Feodo Tracker

Commercial ※有償

- Anomali
- Palo Alto Networks AutoFocus
- PhishMe
- Proofpoint ET Intelligence
- Recorded Future
- Soltra
- Spamhaus Project
- The Media Trust
- ThreatQ
- Virustotal Private API

Organizations

- AUS-CERT

Cloud services

- AWS Public IPs
- Microsoft Azure Public IPs
- Google NetBlocks
- Google GCE NetBlocks
- Microsoft Office365 IPs and URLs

ホワイトリスト用途でも使用可

Output方式

Output

- JSON
- JSON-SEQ
- STIX/TAXII
- PAN-OS EDL
- PAN-OS DAG API
- Elastic Logstash
- Arcsight CEF (as external extension)

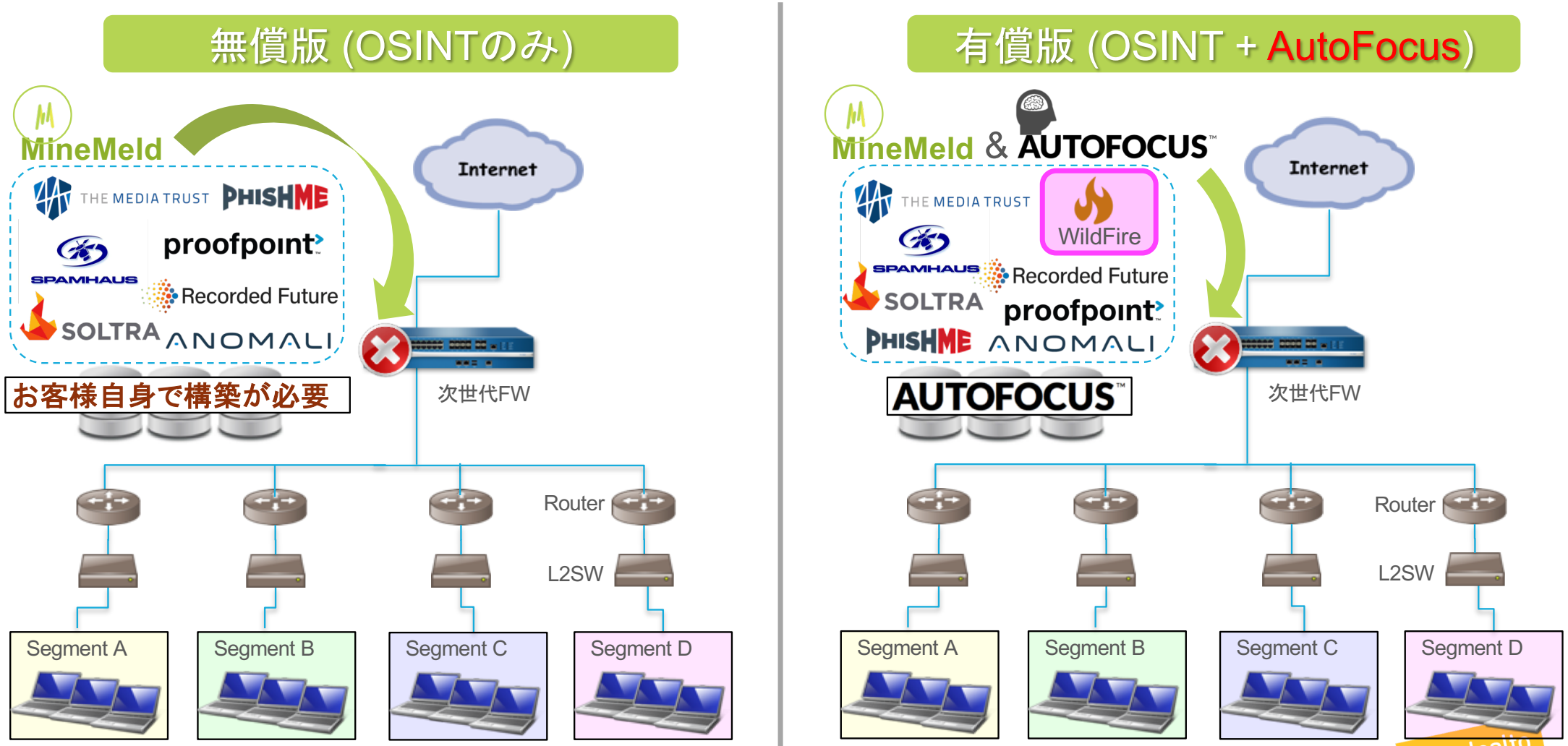
 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

MineMeldの適用モデルの差異 (無償版 vs 有償版)

	有償版	無償版
情報ソース	OSINT AutoFocus(WildFire脅威インテリジェンス)	OSINT *https://github.com/PaloAltoNetworks/minemeld/wiki/List-of-Supported-Nodes*
動作環境	AutoFocus Webサイト上で動作	VMWare Desktop Microsoft Azure Amazon EC2 Ubuntu Server 14.04
サポート有無	メーカーサポート有り	メーカーサポート無し
問合せ先	Palo Alto Networks	GitHub *https://github.com/PaloAltoNetworks/autofocus-client-library* MineMeld Discussions *https://live.paloaltonetworks.com/t5/MineMeld-Discussions/bd-p/MineMeldDiscussions*

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

MineMeldの適用モデルの差異 (無償版 vs 有償版)



 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

MineMeldのユースケース

Case1.　最新脅威情報のブラックリスト運用自動化

- BL化する脅威情報の判断、ベンダーやNW担当者への調整・指示が大変。タイムラグも発生している。
  →判断～設定反映まで全てを自動化
  →他社の脅威情報もAutoFocusに集約して自動化

Case2.　内部に侵入したマルウェアのあぶり出し、感染端末の特定

- ゲートをすり抜けて内部に侵入しているマルウェアが心配。
  →SIEM製品やTaniumなどのEDR、その他製品に脅威情報フィード
  →内部対策もカバー

Case3.　Office365アクセスのローカルブレークアウト＆ホワイトリスト運用自動化

- O365で使用されるIP/URLのリストを手動で設定しているが、運用が大変。
  →MSから情報取得～設定反映まで全て自動化

 © 2019 Palo Alto Networks, Inc. All Rights Reserved.

THANK YOU