sumo logic

もう夜間のアラート対応は嫌です。誰か検知/対応を自動化して！

2023/06/15

Sumo Logic Japan

Tetsuro Kanzaki, Senior Solutions Engineer, CCSP, CISSP

Agenda

1. Sumo Logicとは
2. Sumo Logicデモ
3. まとめ

Sumo Logicが解決する課題

1. Sumo Logicで**アラート対応が減る**
2. Sumo Logic相関分析で**未知の脅威を検出**

Sumo Logic：SIEM/Observability/SOAR/Monitoring SaaS
2400＋のお客様

Coincheck

「まさに当社SOCの要です」

GREE

「ログ管理の敷居が下がり労力と時間を減らせました」

Moneytree

「高度なセキュリティと安定性の実現に欠かせないです」

早稲田大学 WASEDA University

「柔軟なカスタマイズが可能である点も魅力的でした」

会社概要

会社名：Sumo Logic, Inc.（NASDAQ:SUMO）
社員数：900名＋
創業年：2010年　本社：カルフォルニア

Sumo Logicとは
Cloud Native Observability/SIEM/SOAR

ログ・メトリクス APMの統合監視

サービスの 依存関係把握

AWSやK8s専用 ソリューション

Observability

障害検知、原因調査、性能監視、APM

セキュリティ(ログ分析, SIEM, SOAR)

アラートの トリアージ

相関分析の 自動化

事後対応の 自動化

Global Intelligence: ビッグデータを活用したMTTI/MTTR削減

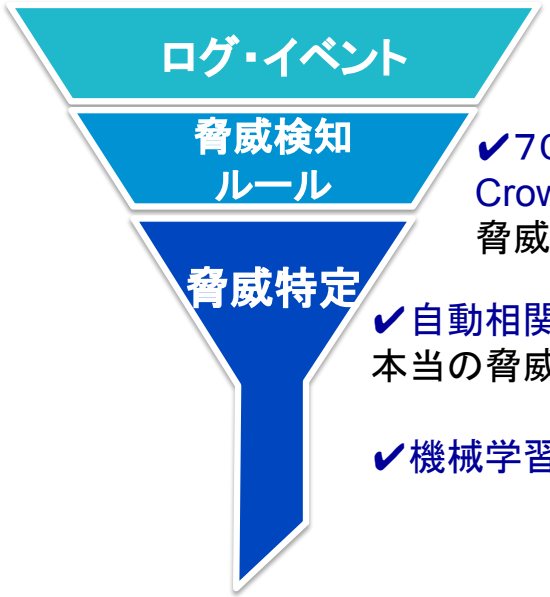
Cloud-native, Continuous Intelligence Platform™

- あらゆるマシンデータを取込可能
- マルチテナント型クラウド
- 柔軟なライセンス体系
- 次の行動への「気付き」を得られる
- 機械学習による分析
- 高セキュアなプラットフォーム

sumo logic

SIEM/UEBAとは？
脅威検知の自動化、検知後の対応の自動化

SIEM：脅威検知の自動化



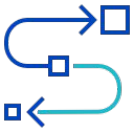
✔700＋の検知ルール、CrowdStrike IOCにより、脅威を検知

✔自動相関分析により、本当の脅威のみアラート

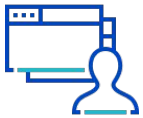
✔機械学習で誤検知防止

UEBA：ふるまい検知

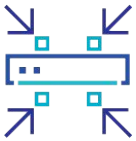
【ログインの異常値】
普段、ログインが無い国からのログイン検知



【コマンドの異常値】
普段、実行しないコマンドの実行



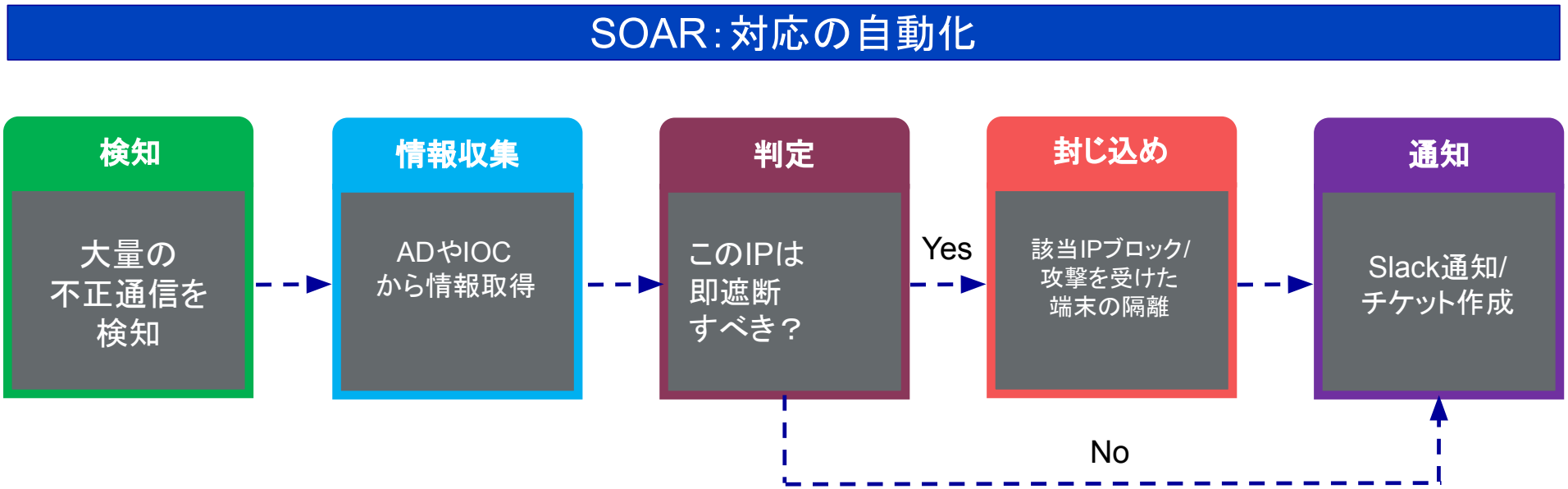
【ダウンロードの異常値】
普段よりも大量のダウンロード検知



【APIコールの異常値】
普段よりも大量のAPIコール

sumo logic

SOARとは？
対応の自動化



Observabilityとは？
あらゆるログ・メトリクス・Tracingを統合管理

サーバレス、コンテナ等を使用するAppは、リリースサイクルが早く、依存関係が複雑。そのため、従来の性能監視だけではNG。　ログ・メトリクス・Tracingを組み合わせて監視していく必要がある

Tracing

トランザクションの詳細、
依存関係情報から
「ボトルネック」を把握

Observability

イベントID、
エラーメッセージから
原因の詳細を特定

ログ

Metrics

CPU、メモリ、ディスク等を
監視

sumo logic

Sumo Logicデモ Basic編

sumo logic

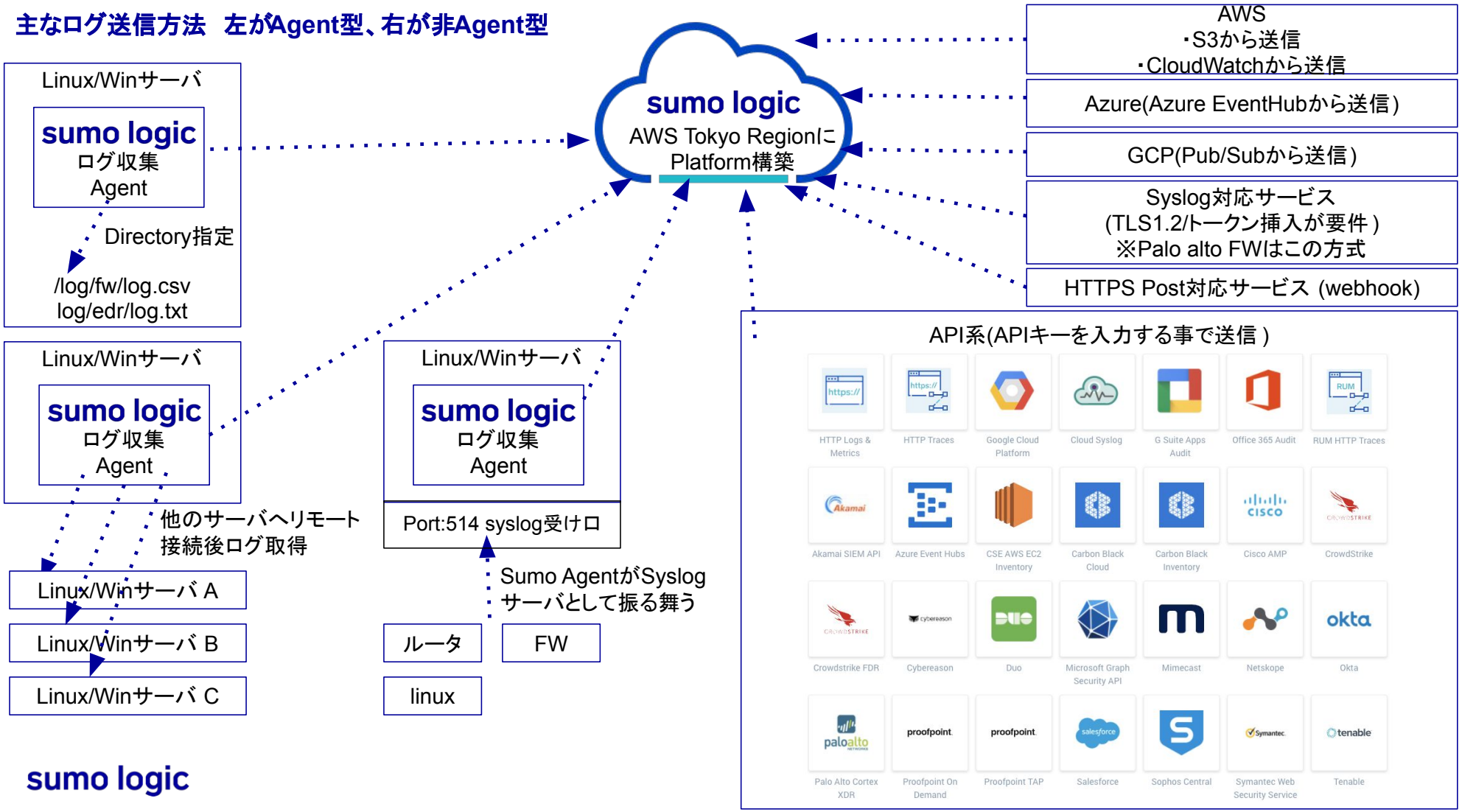
Sumo Logicデモ　Basic編

1. 簡単にデータをSumo Logicへ送信できる

2. 簡単に分析できる

3. 簡単に可視化出来る

主なログ送信方法　左がAgent型、右が非Agent型



sumo logic

SIEM/UEBAデモ

sumo logic

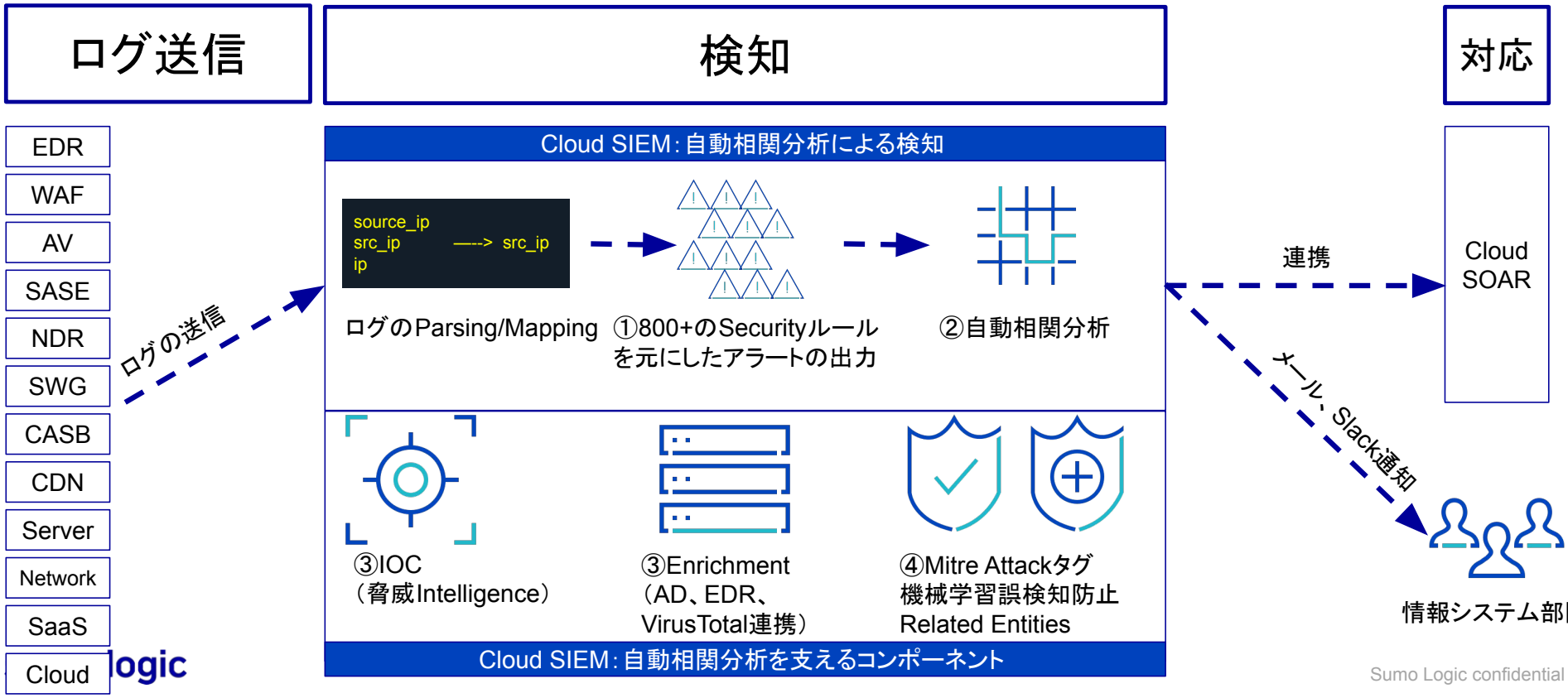
SIEMデモ

1. 自動相関分析によるセキュリティ強化

2. 800＋のルールを内蔵＋自動更新

3. アラートのトリアージにより、アラート疲れ減少

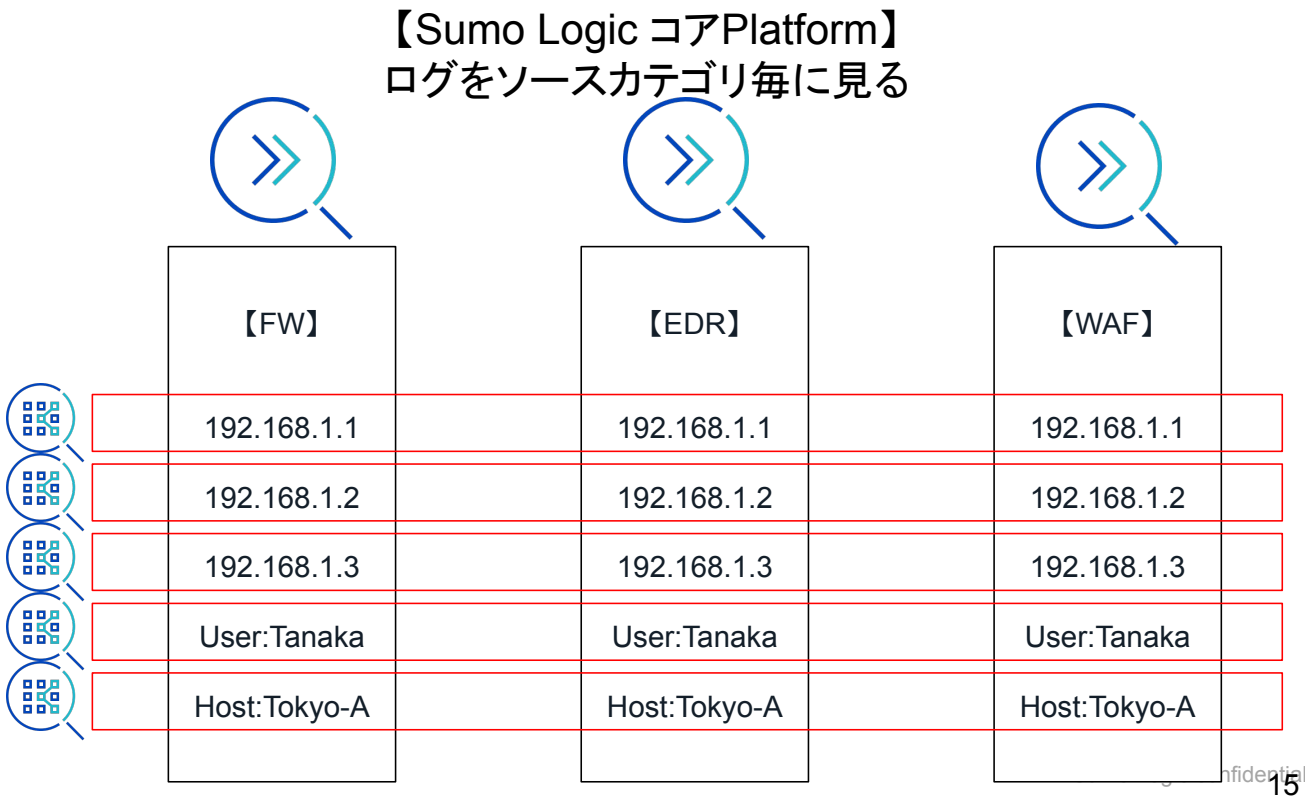
SIEMとは
検知を自動化



アラートのトリアージの仕組み
各Entityの危険度スコアを元に自動相関分析

【CSE】
エンティティ(Entity)を
自動的にクラスター化し、
各ソースを相関分析

※Entity＝IP, User, hostname等
のユニークな値



UEBAルールの例

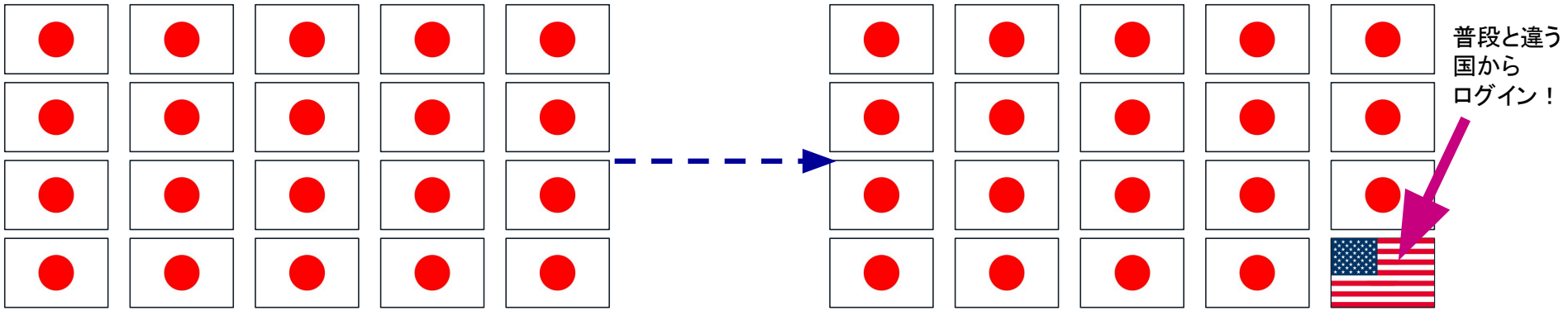
「初めて見たログ」を条件にゼロデイ攻撃や内部不正を発見

Step1.
普段の挙動をSumo Logicが学習（ベースライン作成）

ログインUserの国（1/1～1/31）

Step2.
ベースラインを元に異常を発見

ログインUserの国(2/1)



ポイント：旧来のSIEMでも「日本以外の国を検知する」という条件を書けたが、
事前に詳細な条件（この例の場合、「日本以外の国を検知する」という条件）を書く必要が有った。
このFirst Seen Ruleの場合、「今まで無かった、初めて見たログ」という曖昧な条件でも検知が可能 となり、未知の脅威や内部不正を発見しやすくなる

SOARデモ

sumo logic

SOARデモ

1．400＋のPlaybooks（台本集）やIntegrations

2．自動化も半自動化も可能

SOARとは
対応を自動化

検知

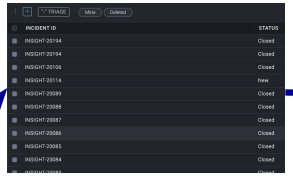
対応の自動化

EDR
WAF
AV
SASE
NDR
SWG
CASB
CDN
Server
Network
SaaS
Cloud

Cloud SIEM

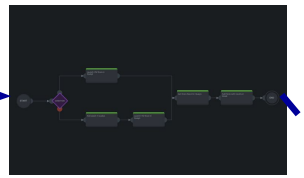
①SOARへのデータ送信

Sumo Logic Cloud SOARによる自動処理

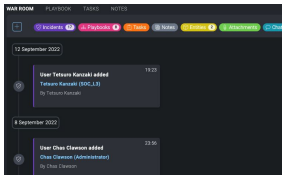


②インシデント管理/ケースマネジメント

人のアサイン



③Playbookの実行、機械学習によるPlaybook推薦



②War room

③300+ Playbook
カスタム可能

④Open Integration Framework

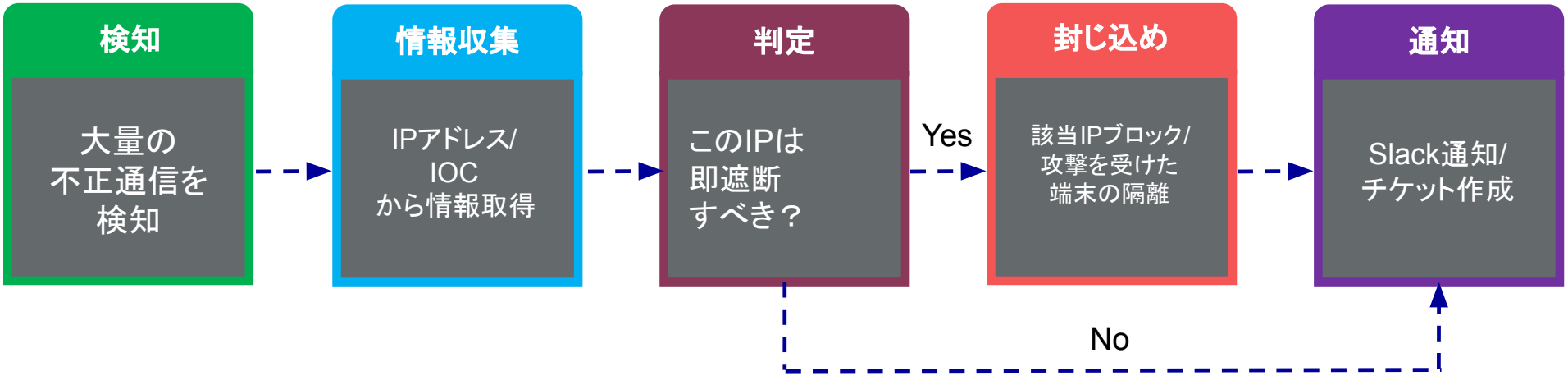
自動処理を支援するCloud SOARの機能

④アクションの実施

API/Python/Perl/Bash Powershell による隔離/遮断/削除/リセット/通知/チケット作成 etc

EDR
WAF
AV
SASE
NDR
SWG
CASB
CDN
Server
Network
SaaS
Cloud

SOARの対応例
検知～対応を自動化



よくある質問：全自動化は怖くない？
答え：
半自動化（アナリストが遮断可否を選択）も可能です。
もちろん、全自動化する事も可能です（例：Serverity：Highの通信はすぐに遮断）

今日のまとめ

まとめ　Sumo Logic

1. **Sumo Logicとは**:SaaS専業、マルチテナントCloud
2. **Sumo Logicが解決する課題**:

課題1. Sumo Logicでアラート対応が減る

課題2. Sumo Logic相関分析で未知の脅威を検出

…And more!!!:会場に居る神崎に話しかけて下さい！

次のステップ
ステッカー！無償トライアル！

ステッカー

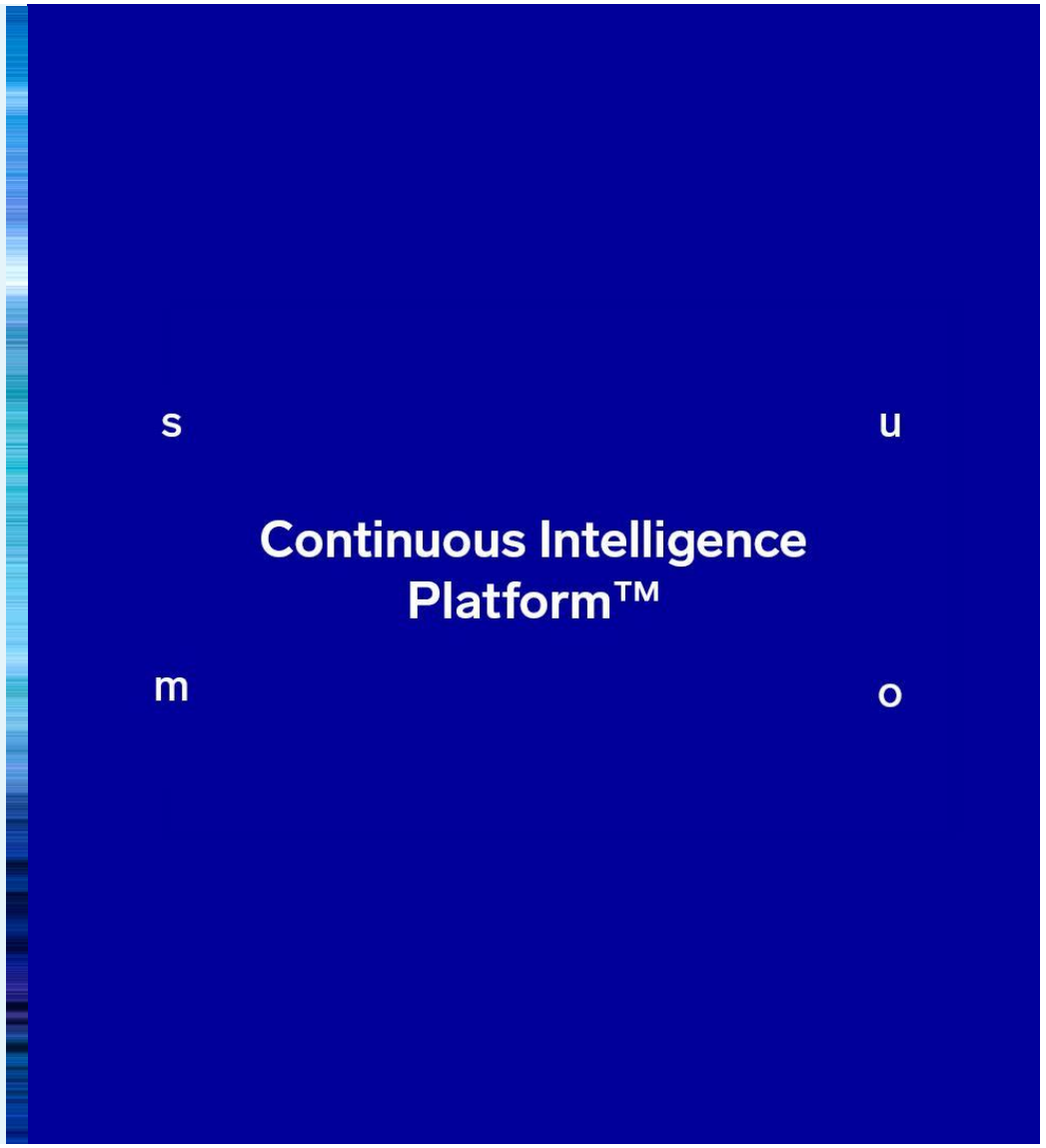
私に声をかけて頂ければ、
ステッカーを進呈します！
ぜひお声がけ下さい！

無償トライアル

無償トライアルにお申し込み下さい！
（クレジットカード不要）

https://www.sumologic.jp

Thank you



sumo logic