sumo logic

次世代のSaaS型統合ログ管理ソリューションと事例

プロダクトマーケティングディレクター

広瀬　努

Sumo Logic Inc.

所在地　：305 Main Street,
　　Redwood City, CA 94063, USA

代表/CEO　：Ramin Sayar (ラミン・セイヤー)

設立　：2010年

Nasdaq上場　：2020年 Ticker Code <SUMO>

Sumo Logicジャパン株式会社

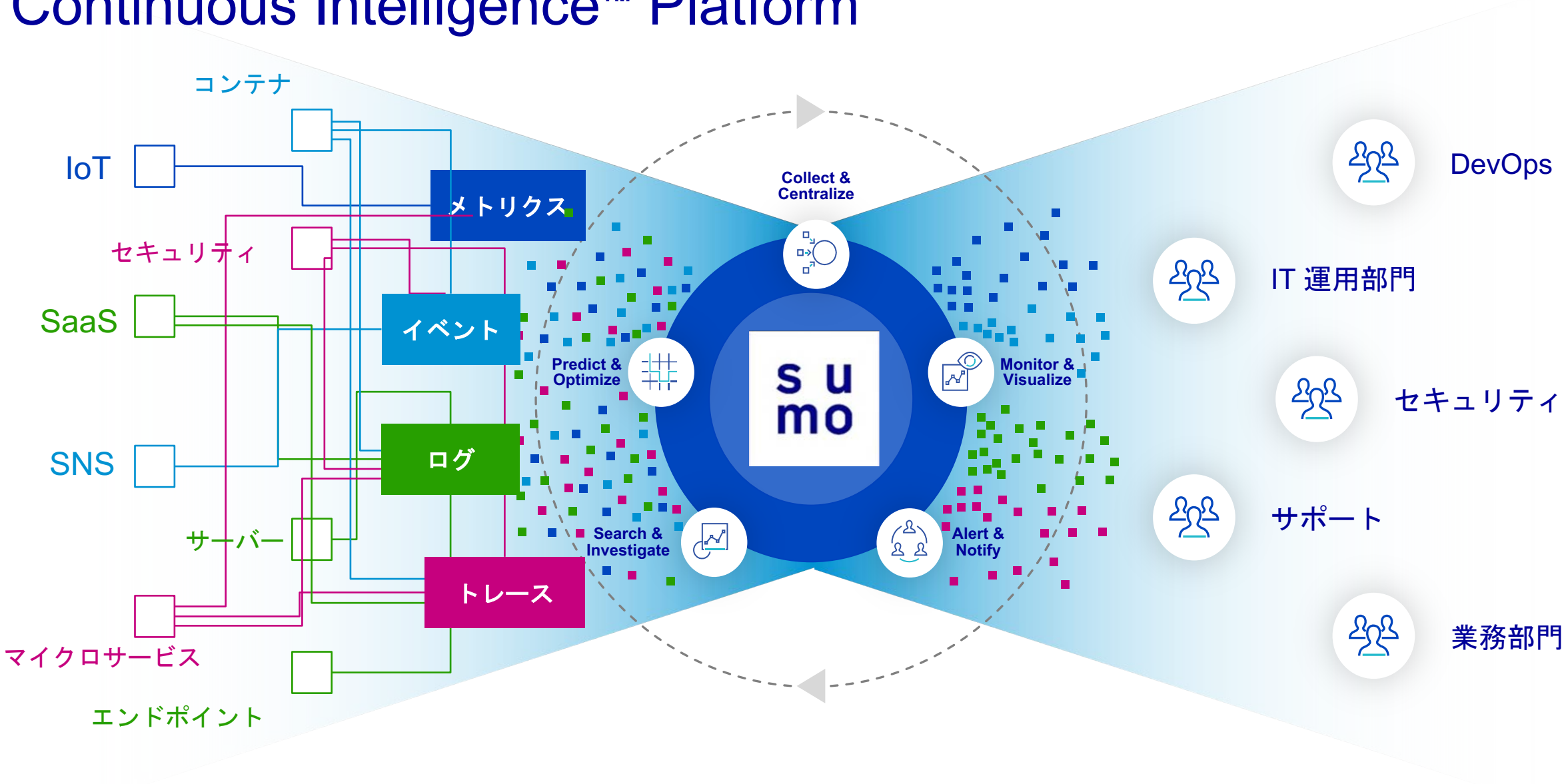
所在地　：〒100-0005
　　東京都千代田区丸の内1-6-5　丸の内北口ビル8F

代表　：河村浩明

設立　：2018年 10月

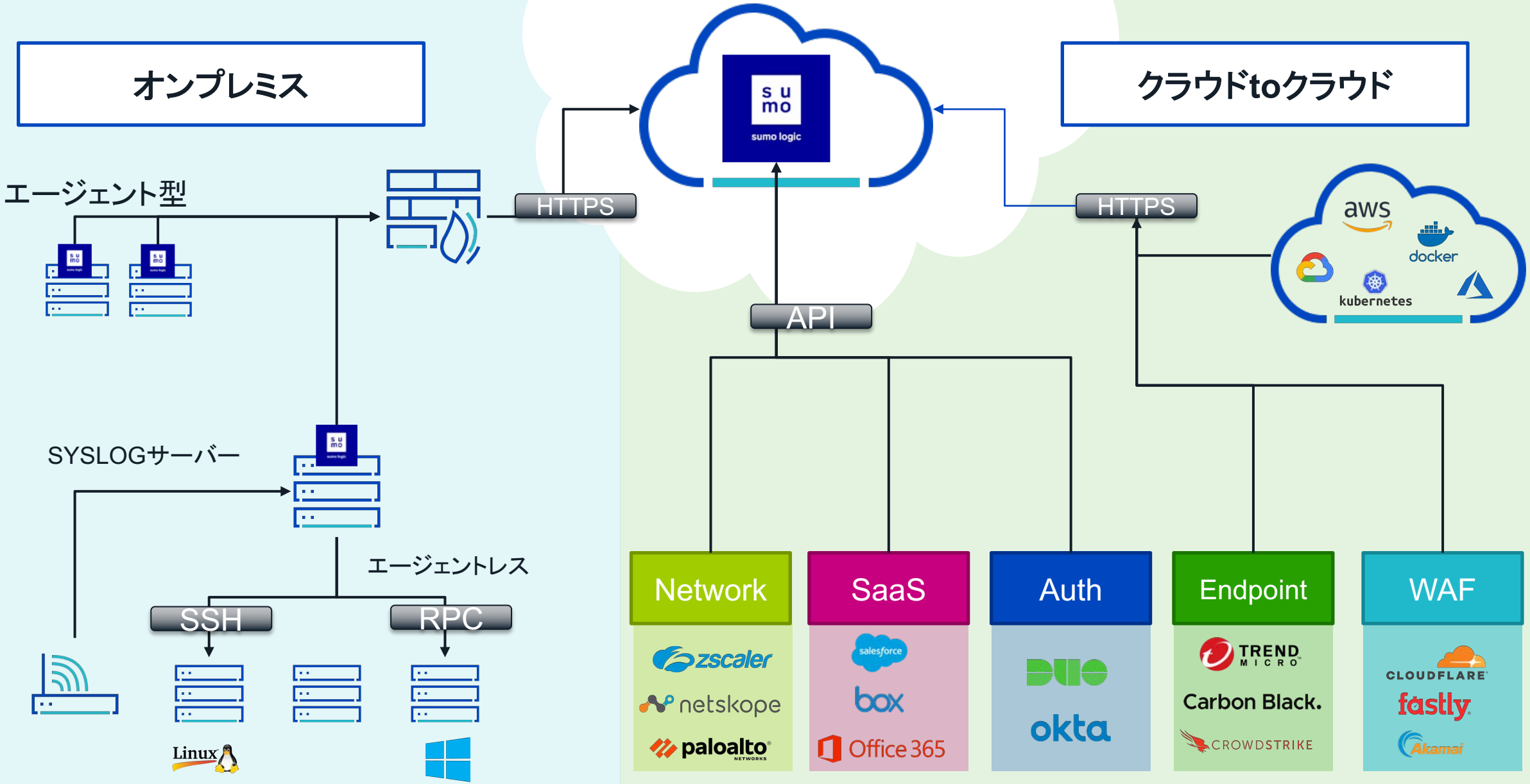
sumo logic

Continuous Intelligence™ Platform

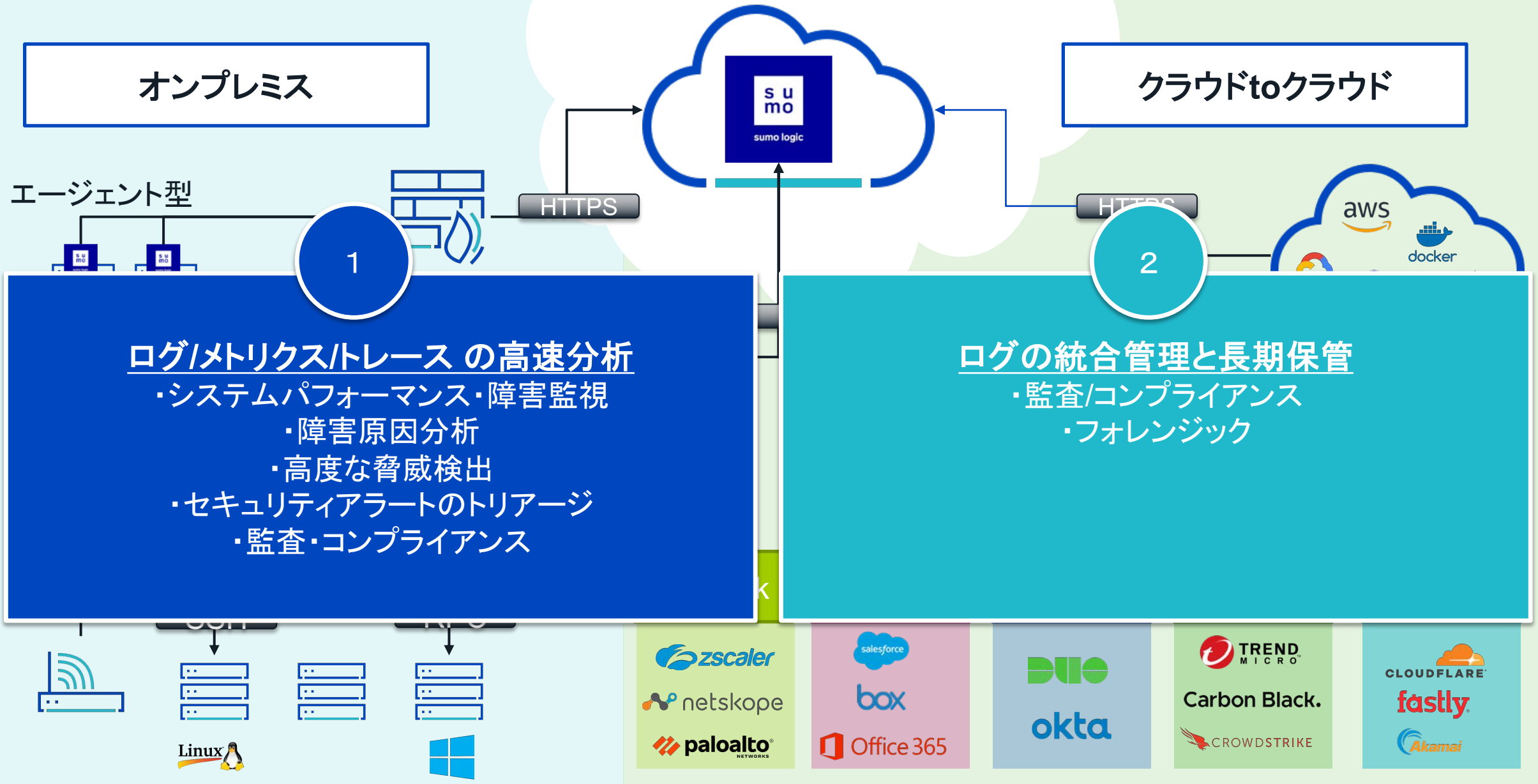


sumo logic

世界のお客様にご支持いただいています。



sumo logic

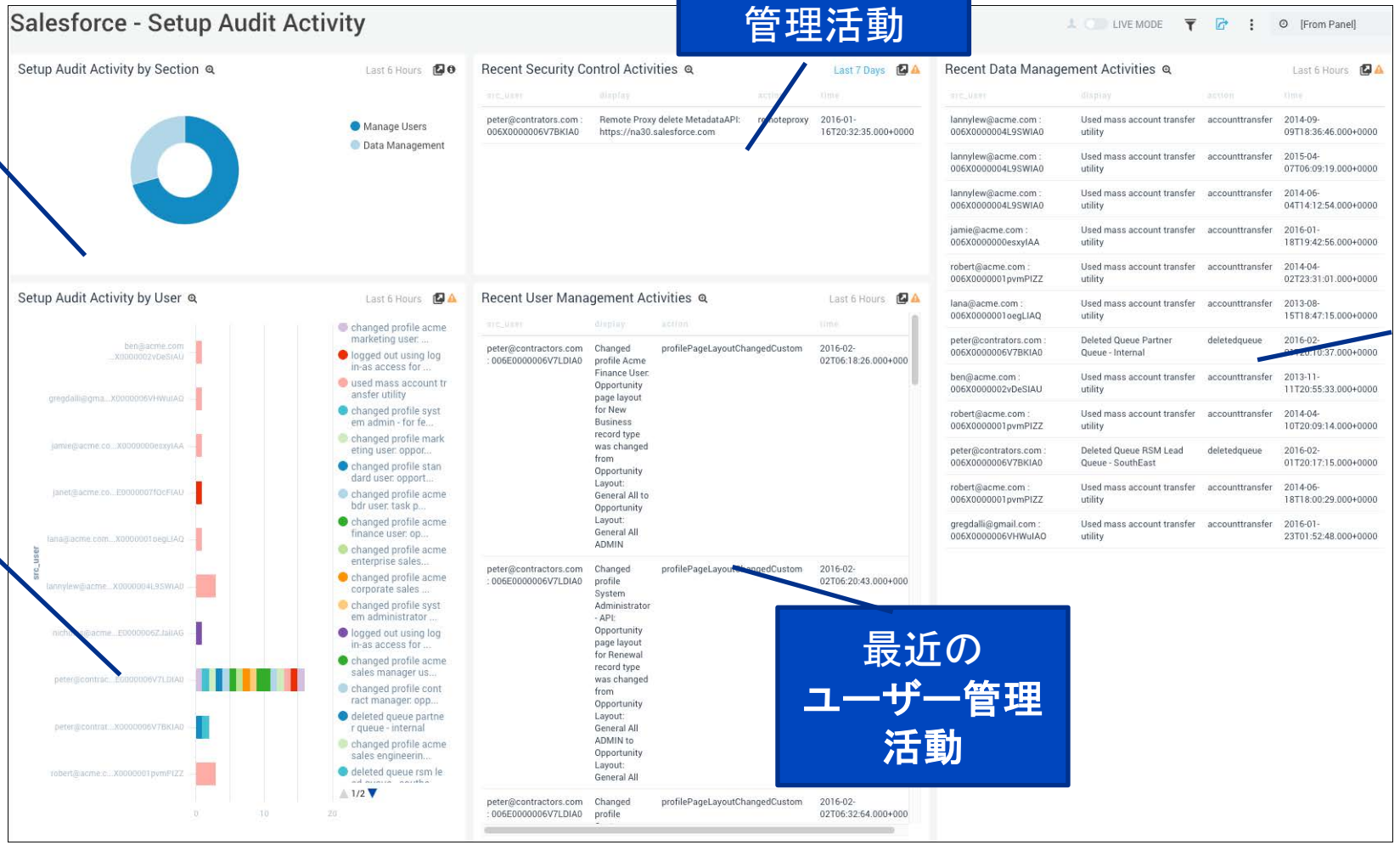


sumo logic

Salesforce - 監査アクティビティの設定

セクションごとの設定
アクティビティの監査

最近のセキュリティ管理活動

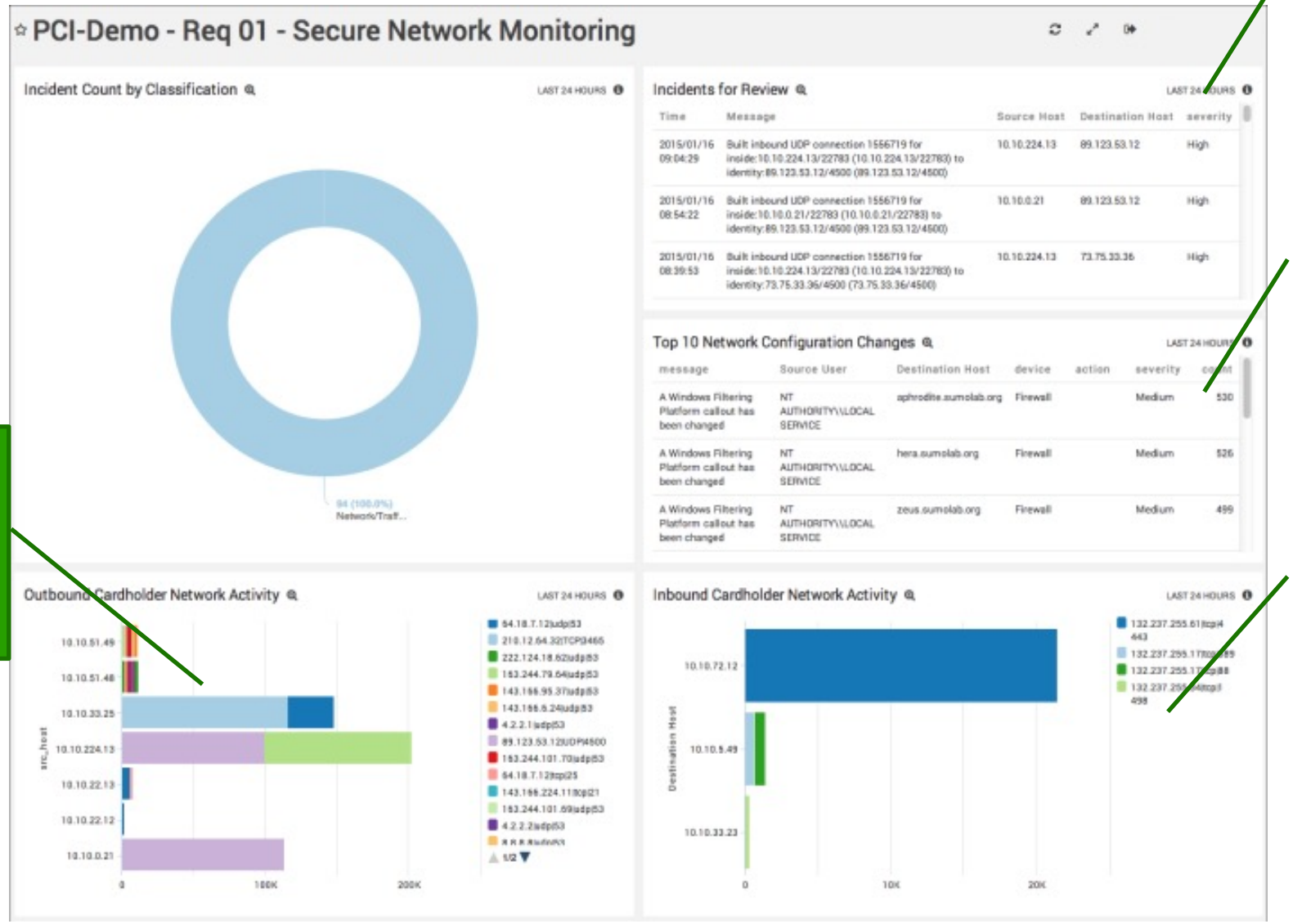


最近のデータ管理活動

ユーザーによる監査
アクティビティの設定

最近のユーザー管理活動

PCI-DSS 準拠を監視



発生した
インシデントの
レビュー

最も多い
ネットワーク
設定変更

カードホルダ
ネットワークの
アウトバウンド
トラフィック

カードホルダ
ネットワークの
インバウンド
トラフィック

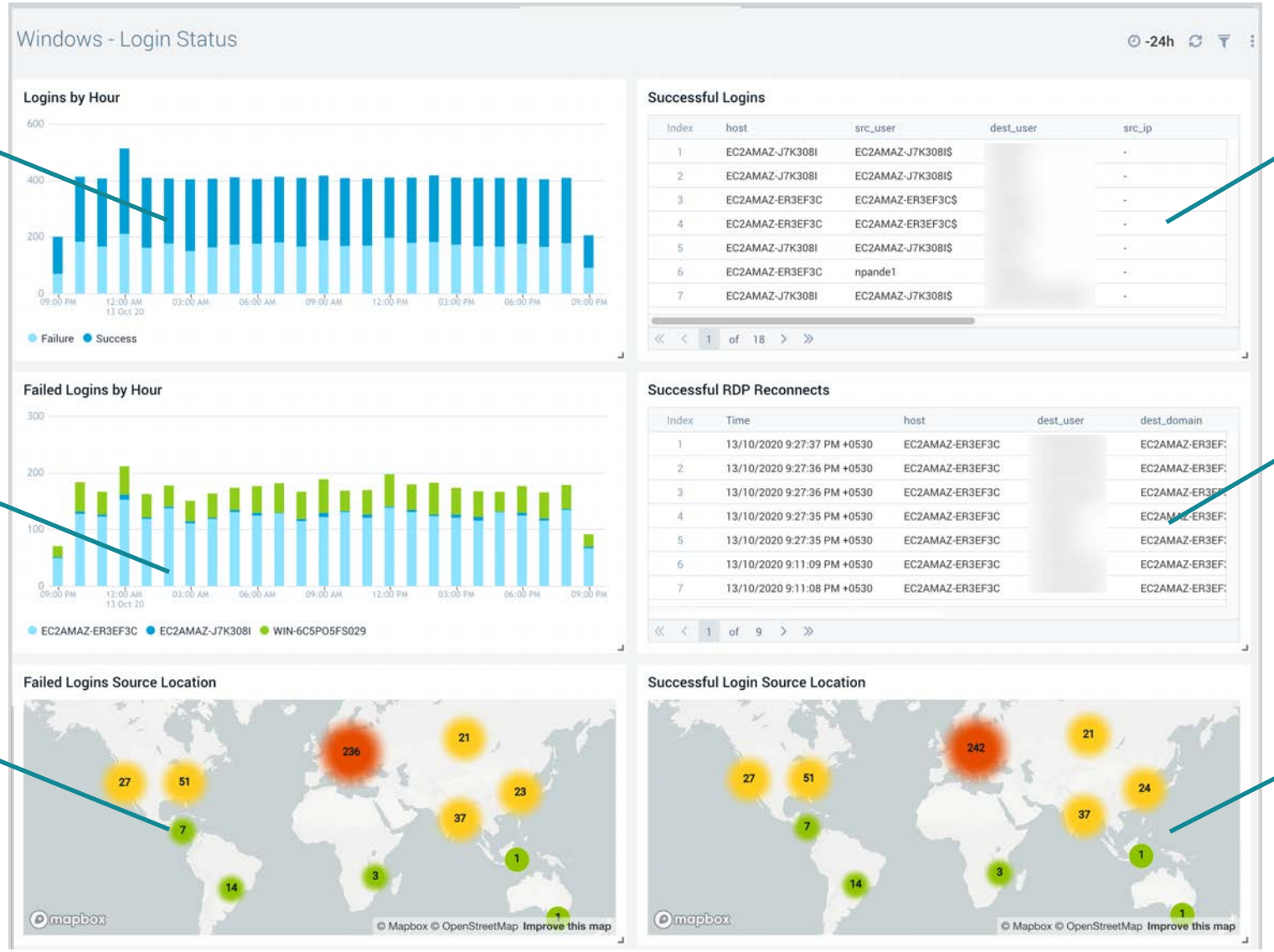
sumo logic

ユーザーの行動監視

時間別
ログイン数

時間別
認証失敗数

認証失敗
ロケーション



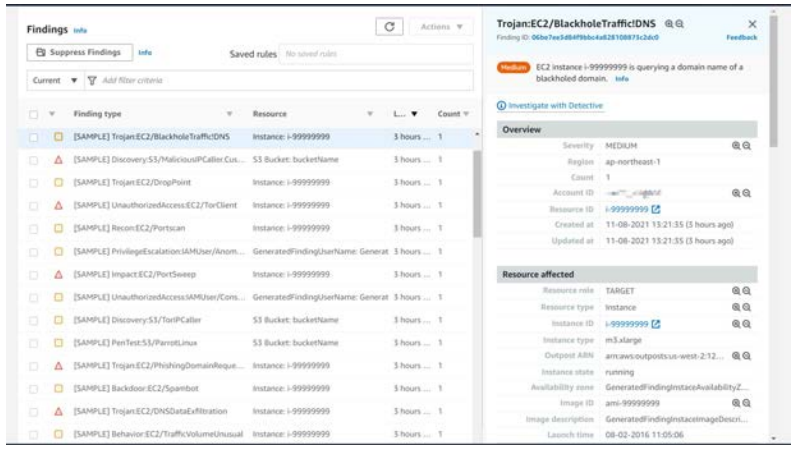
ログイン
ホスト、
ユーザー

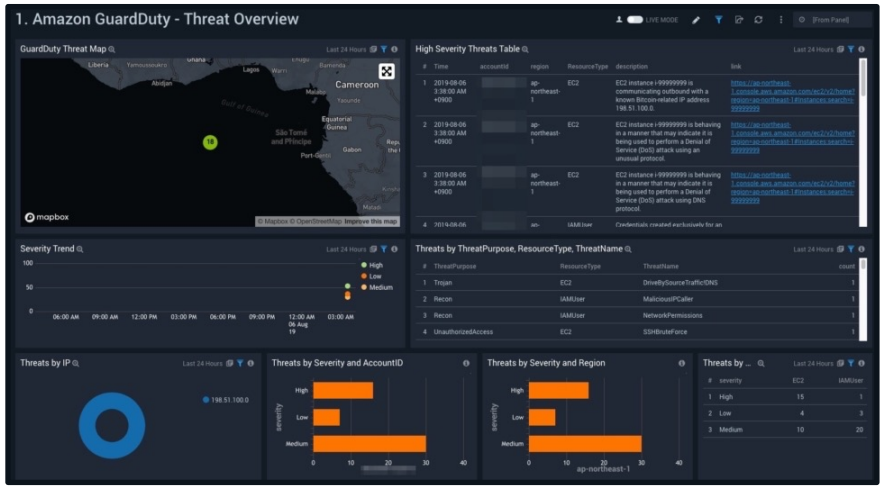
RDPリコネクト
一覧

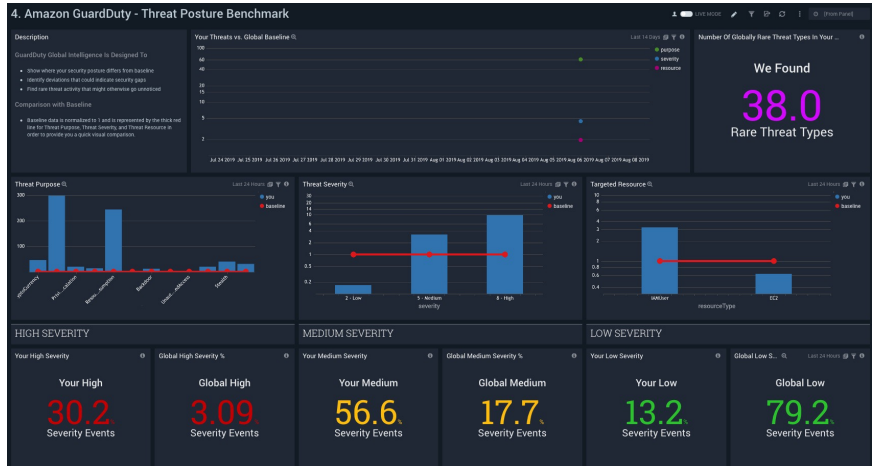
ログイン
ロケーション

Sumo Logic Apps for AWS GuardDuty

AWS GuardDuty コンソール



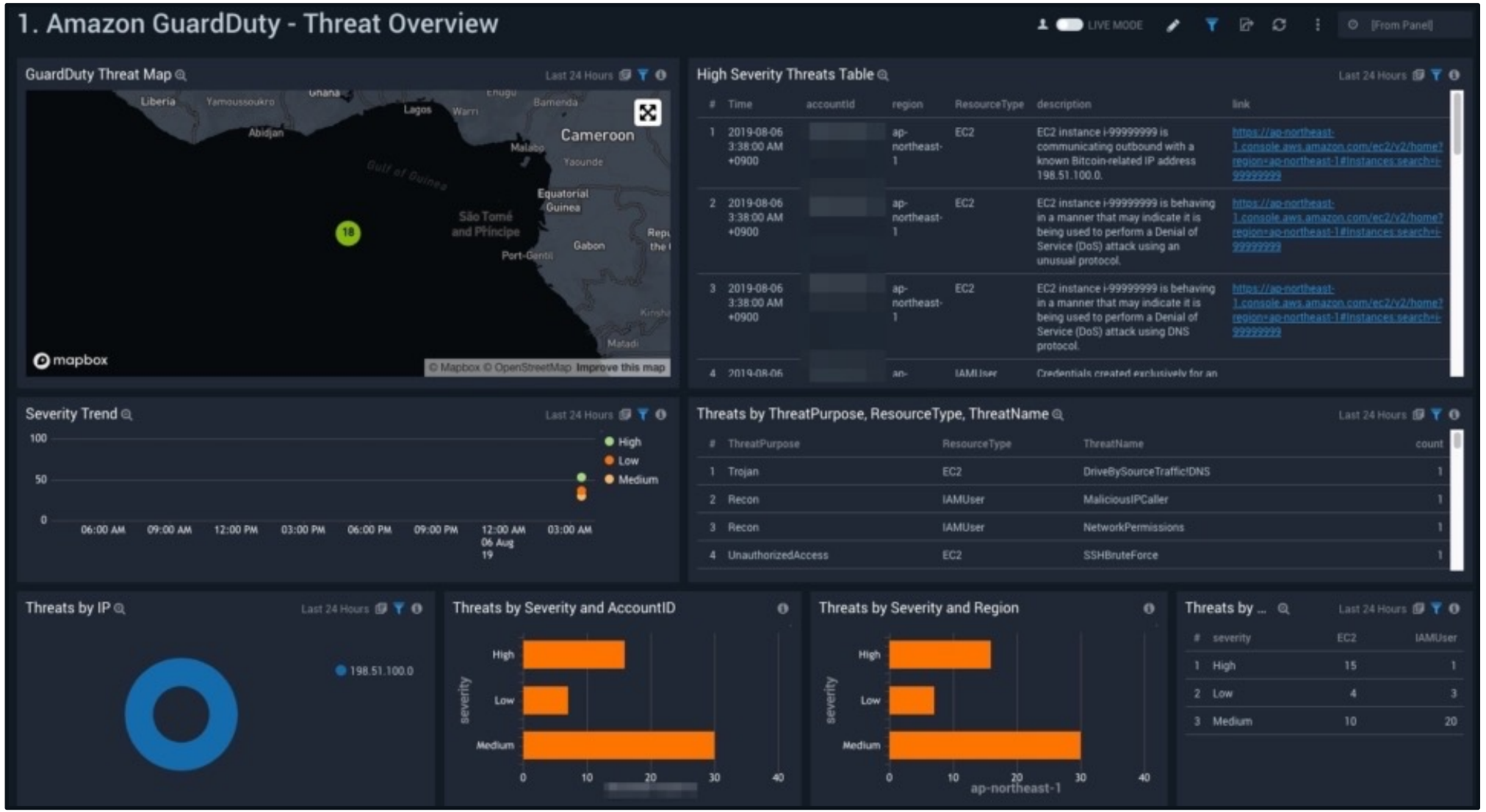




- AWS GuardDutyで脅威検出などは可能であるが、イベントが羅列されているだけなので、優先順位や傾向など把握しずらい。
- マルチアカウントの際には管理がしづらく、システム規模が大きくなると状況把握や原因分析が難しくなる。

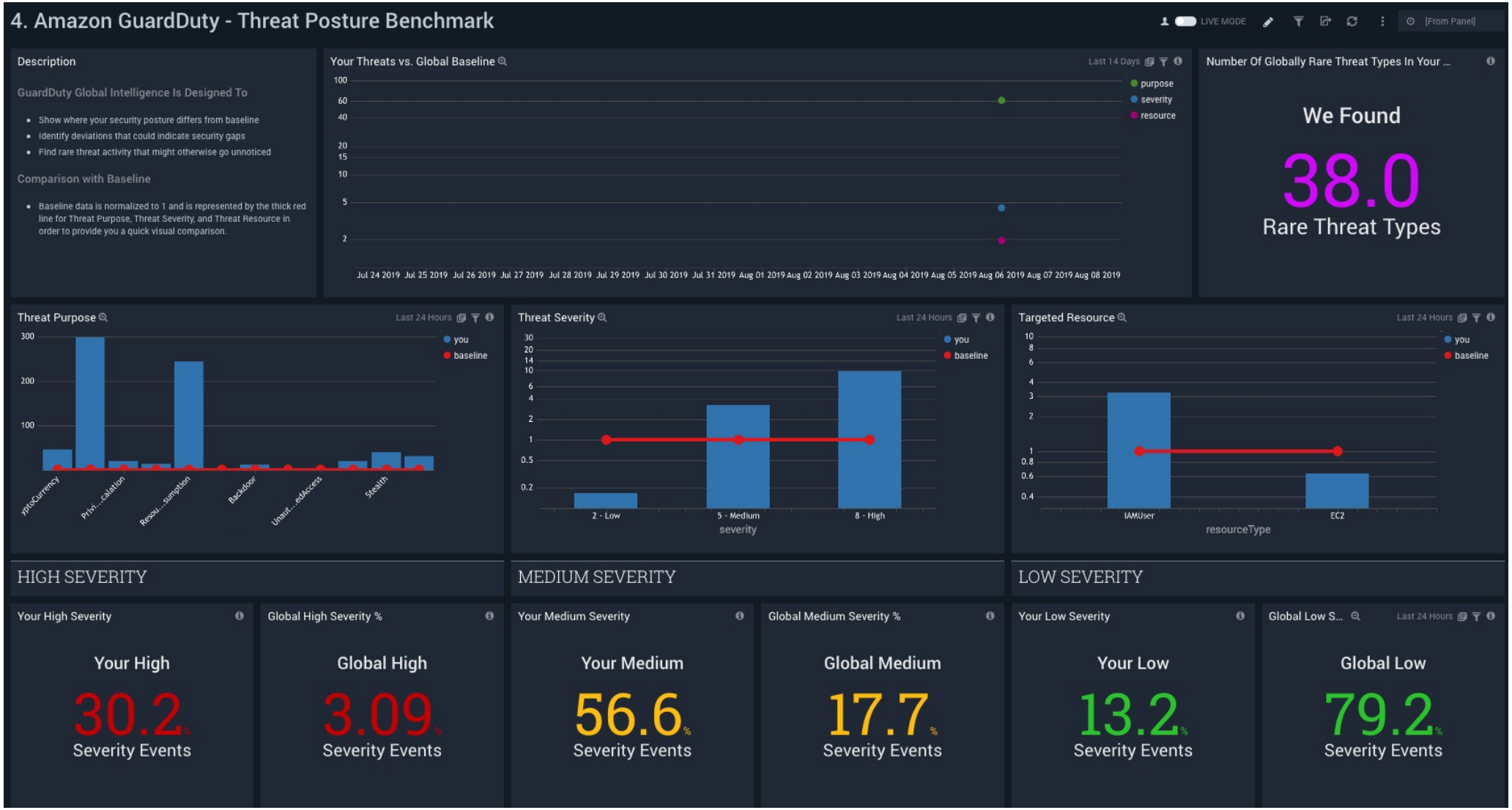
sumo logic

Sumo Logic Apps for AWS GuardDuty



sumo logic

Sumo Logic Apps for AWS GuardDuty

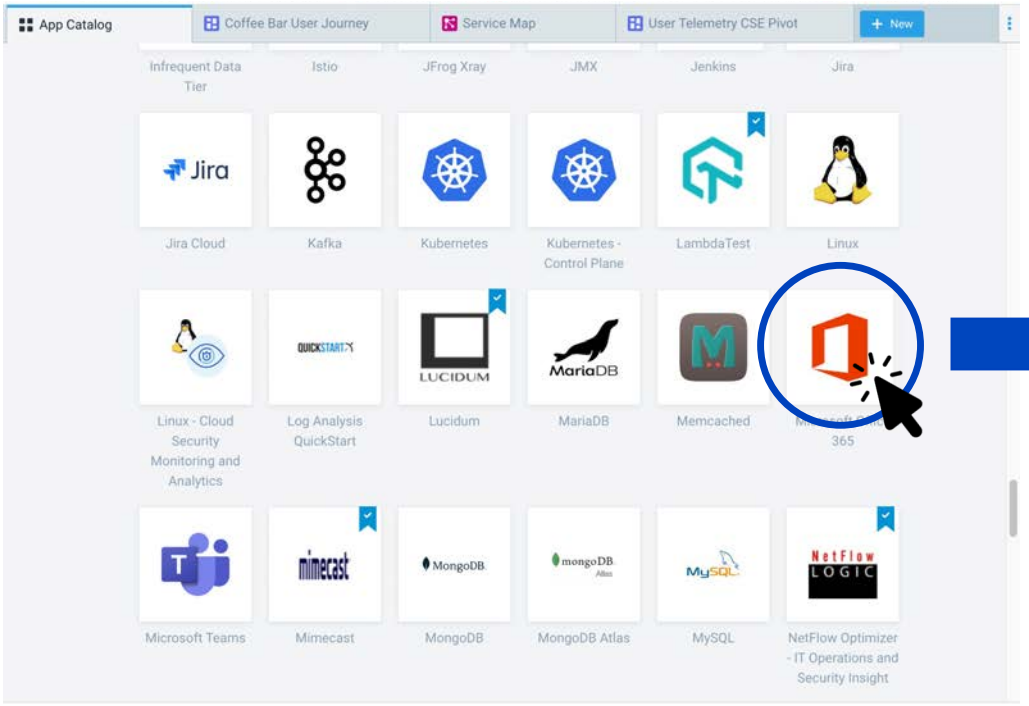


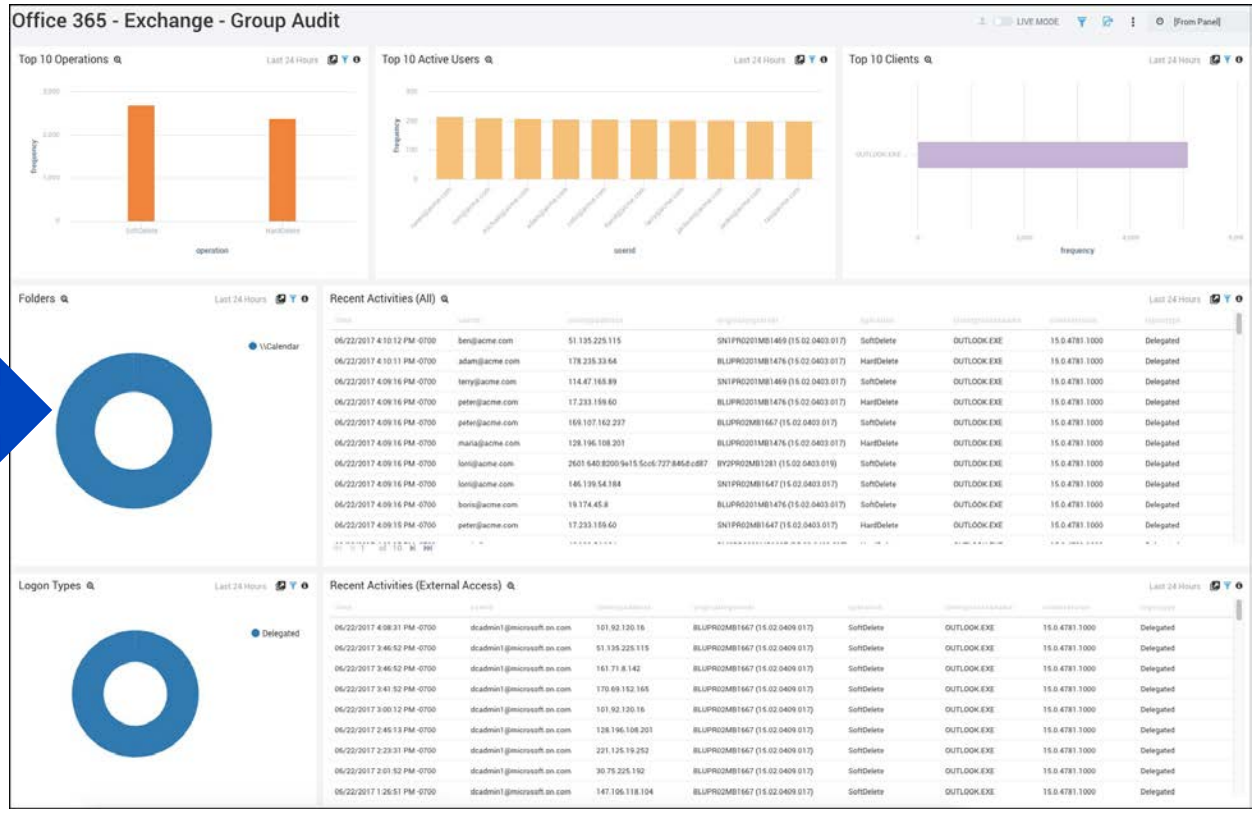
sumo logic

“ダッシュボード“ – 検索結果やログを可視化

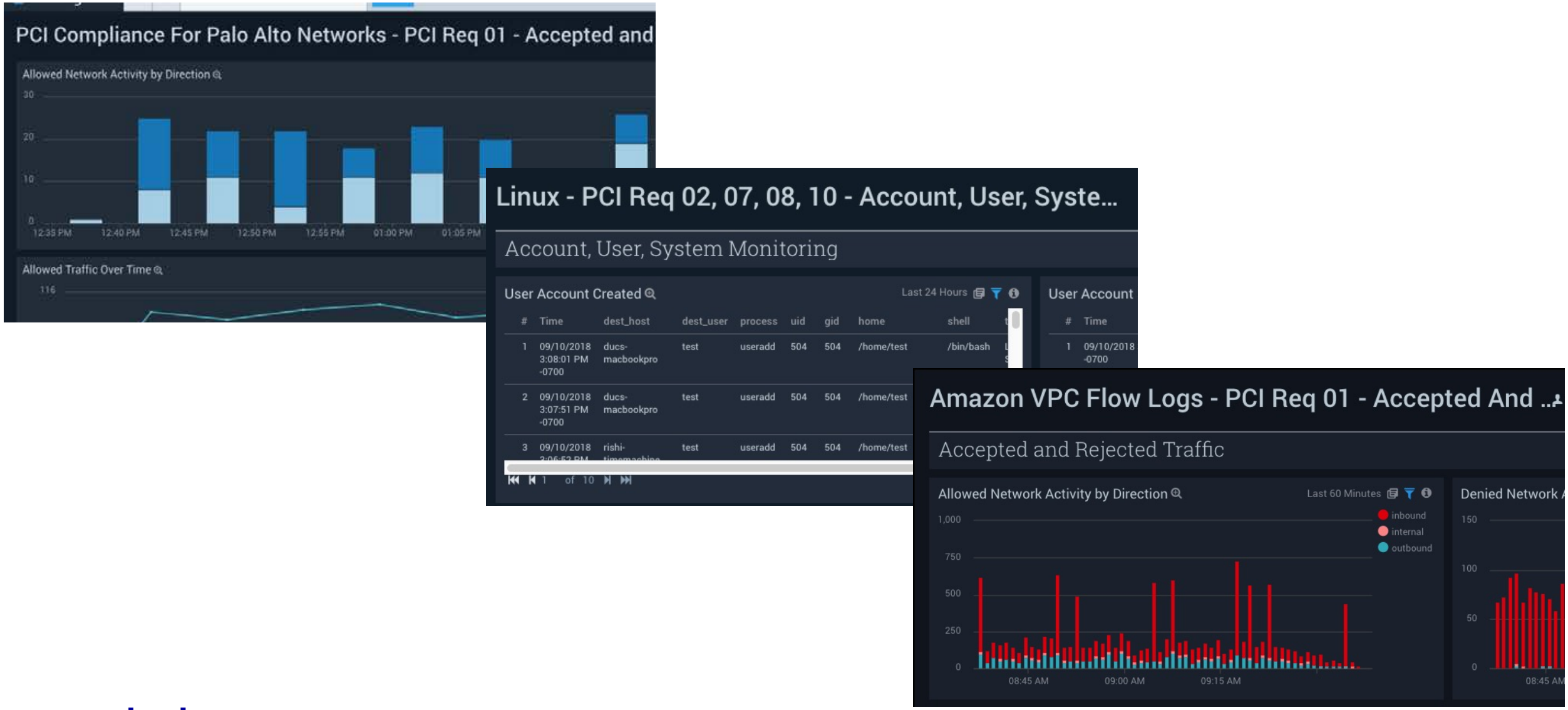
主要な製品・サービス用のテンプレートを用意

アプリケーションカタログ（ダッシュボード、クエリのカタログ）一覧
180以上の製品と連携
合計900以上のダッシュボードを用意





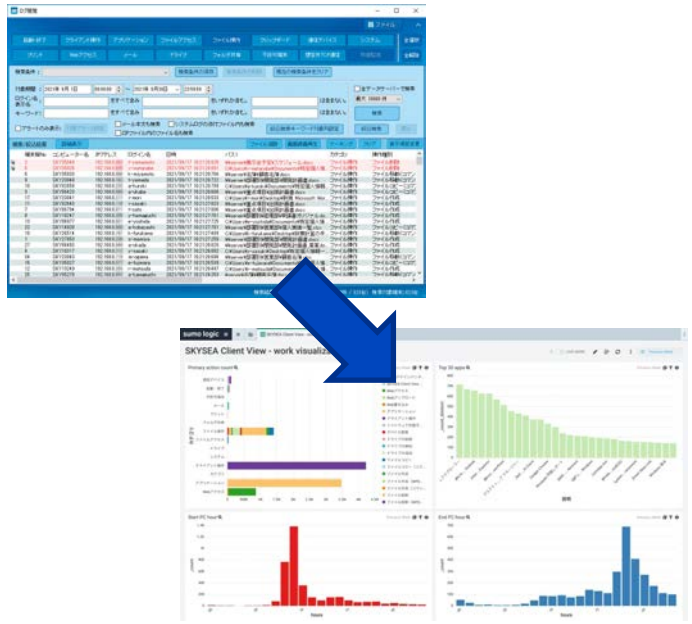
PCI DSS 可視化と監視



sumo logic

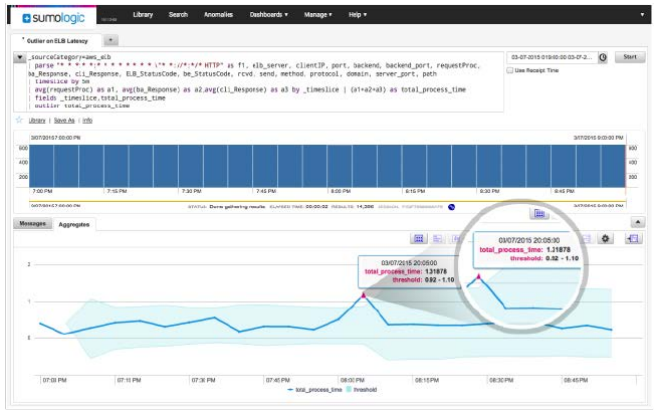
Sumo Logic 分析プラットフォーム

ダッシュボード



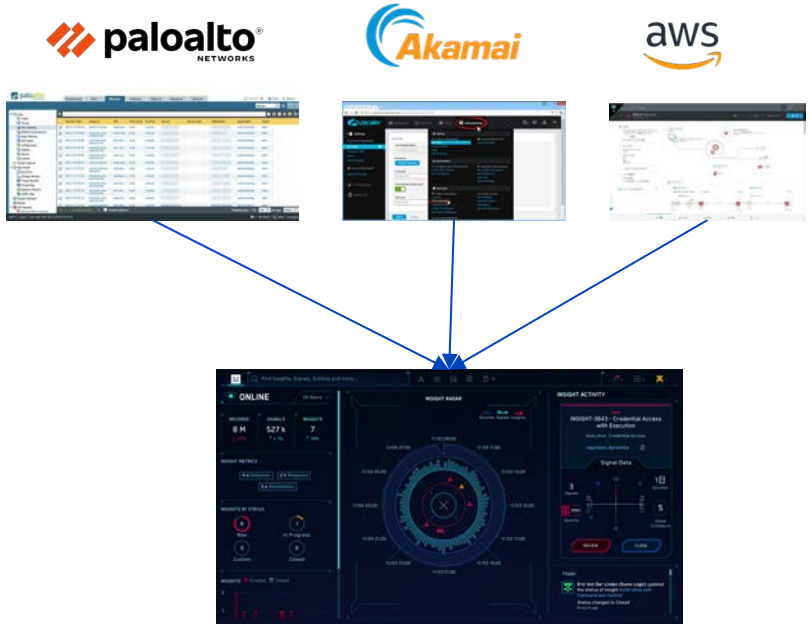
・統計とグラフ表現
・検索とアラート
・レポート

分析ユーティリティ



・アウトライアー（外れ値）検索
・予測値検索
・ログパターン分類
・ログ時系列パターン比較

相関分析

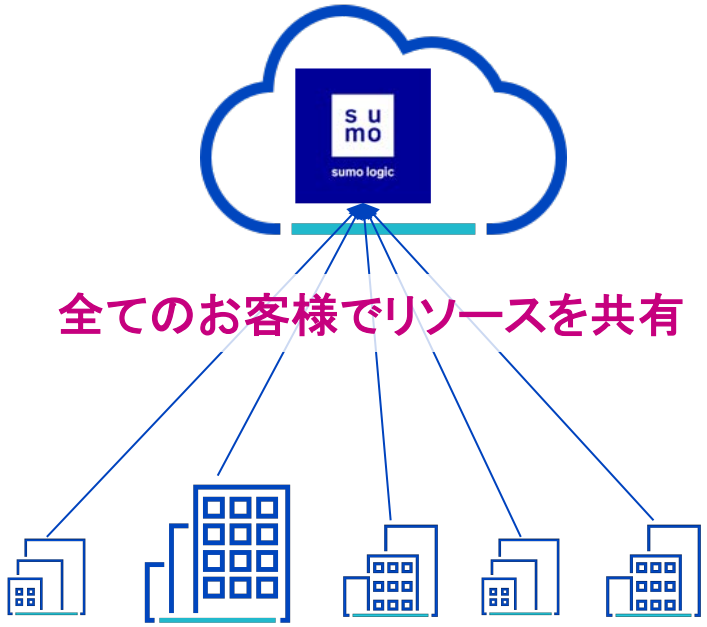


・Cloud SIEM
・Cloud SOAR

sumo logic

Sumo Logic は真のSaaS

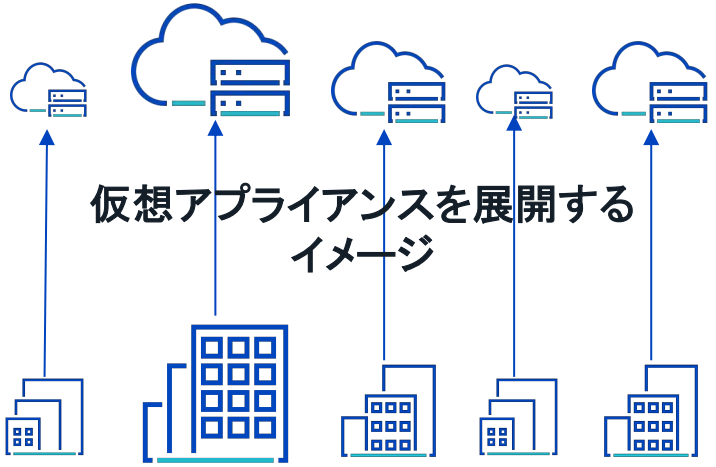
SaaS



全てのお客様でリソースを共有

なんちゃってSaaS

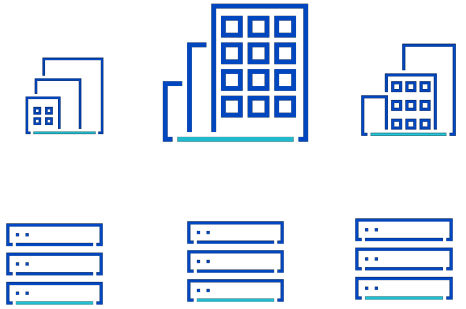
IaaSの上にお客様毎に環境構築



仮想アプライアンスを展開する
イメージ

オンプレミス

ハードウェア/
オンプレ仮想環境

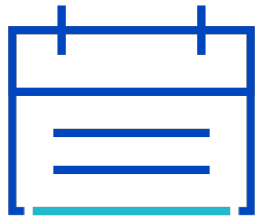


Sumo Logic 課金体系

1日に取り込む
データ量

×

保存日数

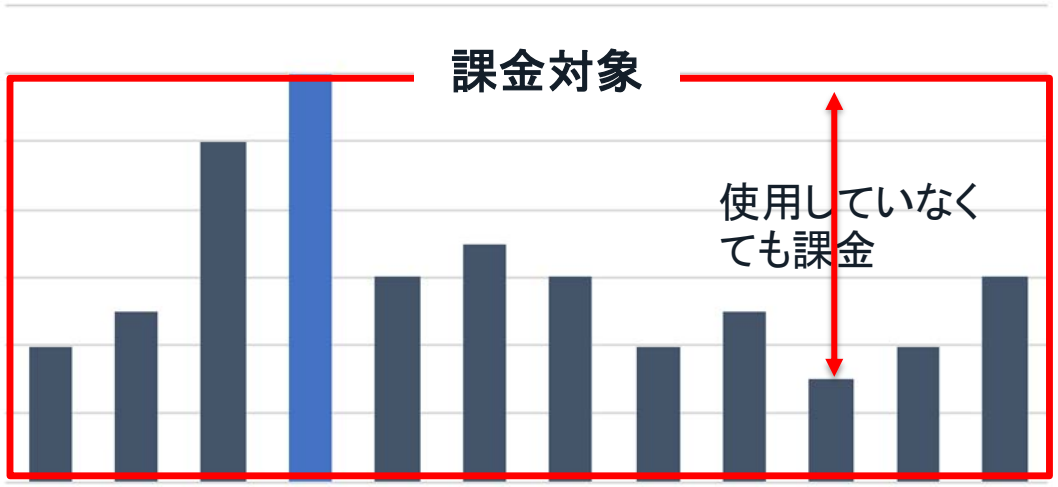


×

ライセンス料

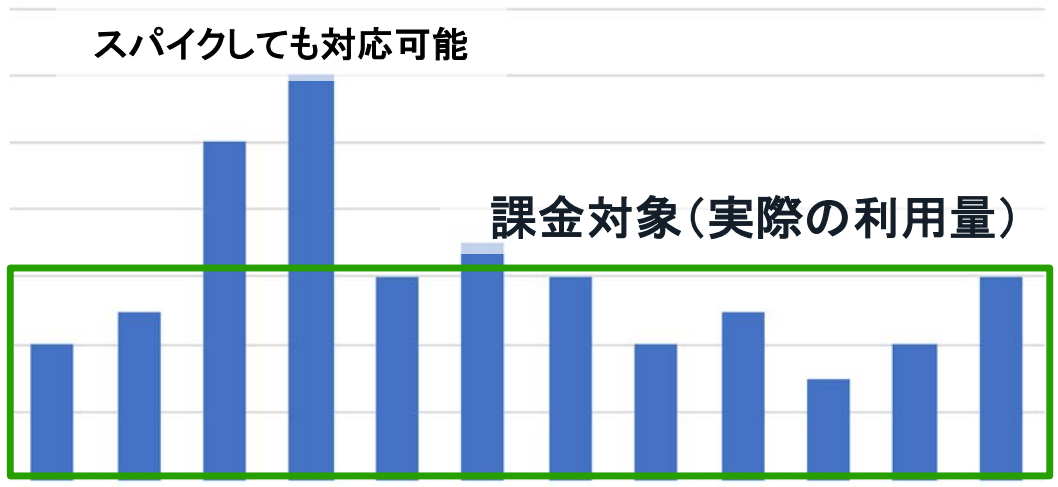
無駄のないクレジットモデル

ピーク性能で課金されるオンプレ型



- ログがスパイクした時にも処理可能なように実際の利用量より余裕（＝無駄）を持たせたサイジングが必要。
- モノリシックなデザインであるため、サーバの稼働管理や脆弱性対策など、運用管理コストがかかる。

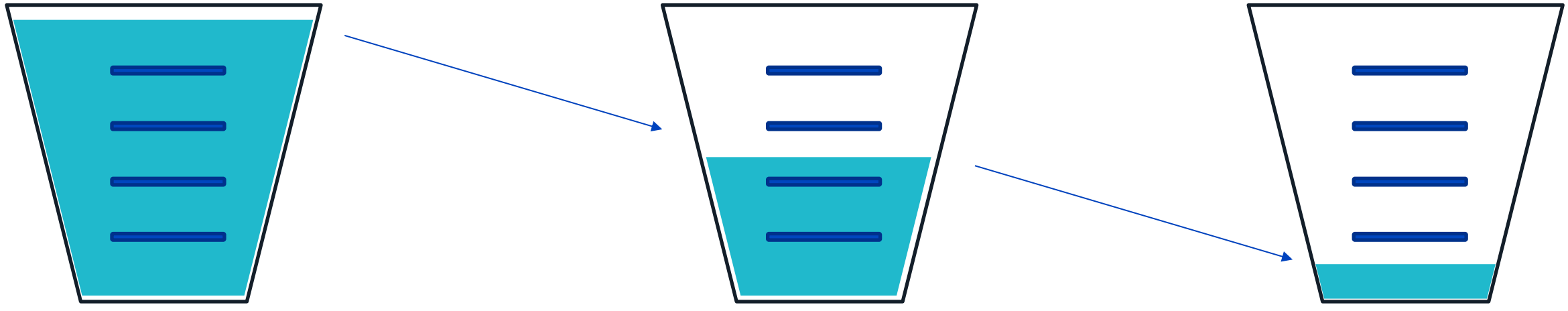
年間平均で課金される完全SaaS



- スケーラブルでサイジングは不要。
- スパイクにも自動対応。
- **交通系カードなどと同様**、予め購入したクレジットを消化したら追加ライセンスを購入するモデル。

sumo logic

Sumo Logic クレジットモデル



残り
100クレジット

残り
25クレジット

残り
5クレジット

初月

契約期間

24ヶ月

SuicaやPasmoと似たモデル。最初に購入したクレジットがなくなれば追加で購入いただく。

sumo logic

Sumo Logic ネイティブクラウドプラットフォーム

パフォーマンス
監視
障害分析

監査/
コンプライアンス

Cloud SIEM
Cloud SOAR

分析ツール
ダッシュボード

Lookup Table
(脅威インテリジェンスも
内包)

検索クエリ処理、インデクシング

パーサー 正規化

データインジェスト ・・・

マイクロ
サービス化
された
コンポーネント

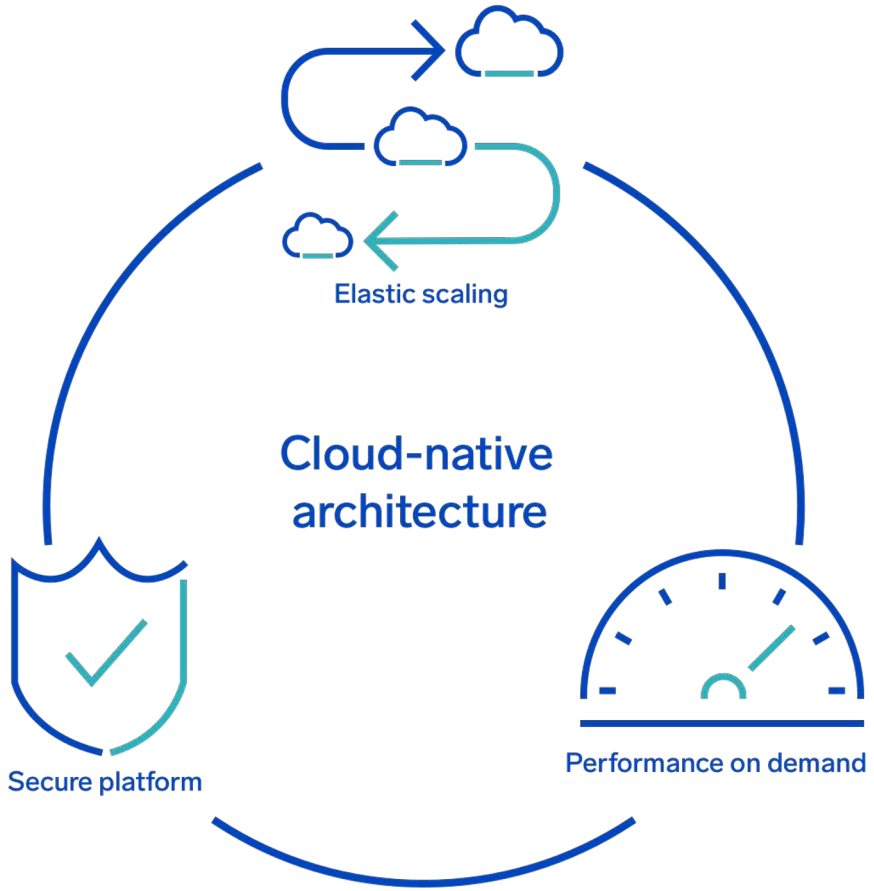
ストリーミング

ログ、メトリクス、トレース

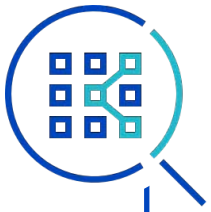
sumo logic

クラウドネイティブなアーキテクチャ

- サイジング不要
- スパイク時に破綻しないスケーラビリティ
- メンテナンスフリー
- 「データ取得」、「監視」、「分析」、
  全てにおいて高いパフォーマンス



フォレンジック調査：インシデント発生時の課題

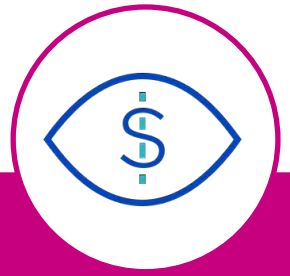


フォレンジック調査：

不正、サイバー攻撃によって発生したインシデントの調査、解析、証拠保全などの一連の作業
「盗取、窃取されたデータ」、「原因」、「影響範囲」の特定が可能
デジタルデータから法的証拠を取得

調査は時間がかかる

1週間以上



高額

数百万円以上

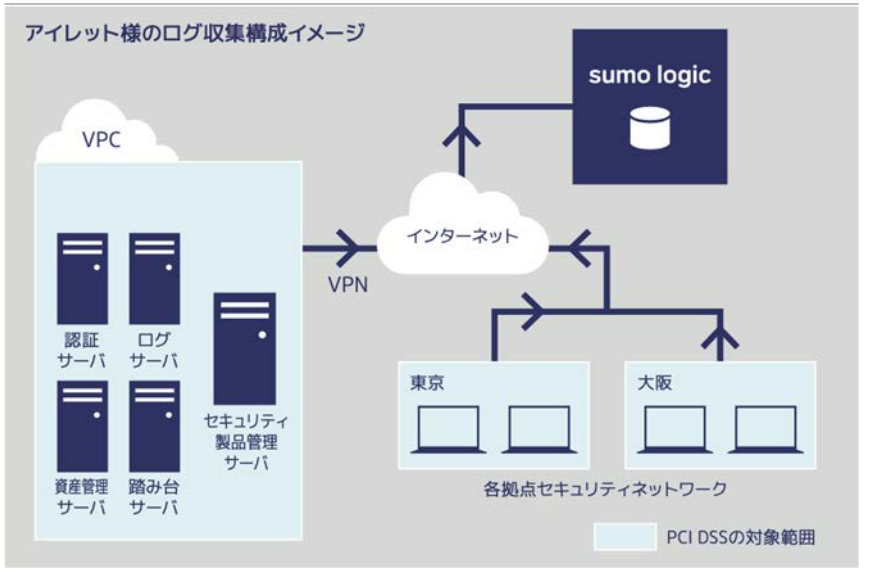
すぐには開始できない

sumo logic

Sumo Logicのお客様事例

アイレット株式会社

Sumo Logic自体がPCI DSSに対応しているのも採用の大きなポイントでした。コスト面も比較検討した他製品のクラウド版に比べ約1/4、オンプレミス版に比べ約1/8で済むのも魅力でした



課題

- コンプライアンス強化を目的とした**PCI DSSへの対応**に、アイレットは自社サービスである「cloudpack」でログ管理ツールを活用していた。これまでのツールは、PCI DSSに対応していなかったことに加えて、ログ保管期間が短いなどの課題があり、実際は他のツールを組み合わせて運用していた。そのため、システムが複雑化し運用効率も低下していた。

導入経緯

- PCI DSSへの対応に必要な機能が備わっており、あらかじめ用意されたPCI DSSのためのテンプレートも豊富であるなどの理由から、Sumo Logicにリプレース。Sumo Logic自体がPCI DSSに対応している点も採用への大きなポイントとなった。さらに無料の認定トレーニングの提供など、Sumo Logicの手厚いサポートも大きく評価された。

導入効果

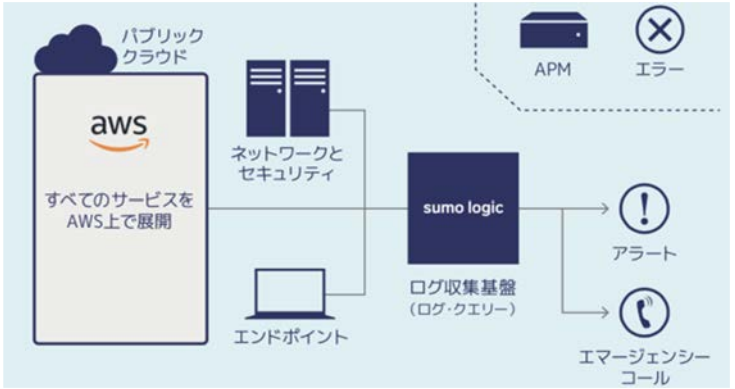
- ログ管理をSumo Logicに一元化でき、抜本的にシステムの最適化とPCI DSSの対応によるコンプライアンスの強化を実現できた。Sumo Logicのダッシュボードも1つの画面に統合できたなど、日々の運用管理業務への効率化も達成した。これにより「cloudpack」のサービスレベルも向上し、セキュリティの強化も果たしている。

sumo logic

Sumo Logicのお客様事例

コインチェック株式会社

SaaS型SIEMソリューションで ログのモニタリング体制を短期間で整備



課題:

- 2018年1月の仮想通貨NEM不正流出事故を受け、仮想通貨取引所サービスのシステムをインフラから再構築し、セキュリティの強化に取り組んでいる。その1つとして、ログのモニタリングの強化を行った。
- クラウドサービスサーバやネットワークセキュリティ機器、端末類のログを一元管理し、不正アクセスなどのログをいち早く検出して対処することで、セキュリティ事故を未然に防ぐことが狙いで、可能な限り短期間での導入が求められていた。

導入経緯:

- SaaS型ゆえに短期導入が可能な点、優れたユーザインターフェース、充実したサポートが決め手となった
- クラウドサービスのサーバ、オンプレミスのネットワークセキュリティ機器、エンドポイントの端末類のログをSumo Logicに集約
- あらゆる事態を想定し、セキュリティ事故の原因になり得る事象が検出されれば、アラートをあげる仕組みを構築

導入効果:

- システムすべてを横断的にログ管理し、膨大なログの中から不正アクセスの予兆などを検出でき、迅速な対処が可能となった
- 高いレベルでのセキュリティの担保だけでなく、さらにコンプライアンスやガバナンスを強化できた
- **Sumo LogicはSaaS型であるため、狙い通りの短期導入も実現した**

sumo logic

Sumo Logicのお客様事例

マネーツリー株式会社

Moneytree™

Sumo Logicは当社が求める高度なセキュリティと安定性の継続的な実現に欠かせないツールです クラウドとの親和性の高さもポイントであり、Sumo Logic自体もAWSにネイティブに対応しているため当社のプラットフォームに合致しています

課題

- 2700社以上の銀行口座やクレジットカード、電子マネー、マイル、ポイントカードなどの情報を集約し、法人向け金融インフラプラットフォーム「MT LINK」として提供。個人向け個人資産管理サービスにも活用している。取引明細をはじめ、承諾を得たユーザの個人情報を厳格に管理するため、高度なセキュリティと安定性が確保されたプラットフォームが必須だった。

導入経緯

- セキュリティ分析、ログのモニタリングの仕組みとして「Sumo Logic」を採用。クラウドベースで構築している「MT LINK」に対して、Sumo Logicも同じくクラウドネイティブであり、親和性の高さを評価した。クラウドとオンプレミスをハイブリッドで管理できることに加えて、リソースをダイナミックに増減できるスケーラビリティもポイントとなった。

導入効果

- Sumo Logicによって、業界標準のプラットフォームに求められるセキュリティと安定性を実現。メガバンクや金融業界におけるベンチャー企業が「MT LINK」活用し、自社単独あるいは他社とのコラボレーションによって、新しいサービスをスピーディかつ柔軟に開発できる環境を整備することで、ユーザの利便性向上、金融のデジタル化および金融業界全体の発展に貢献している。

sumo logic

お客様事例

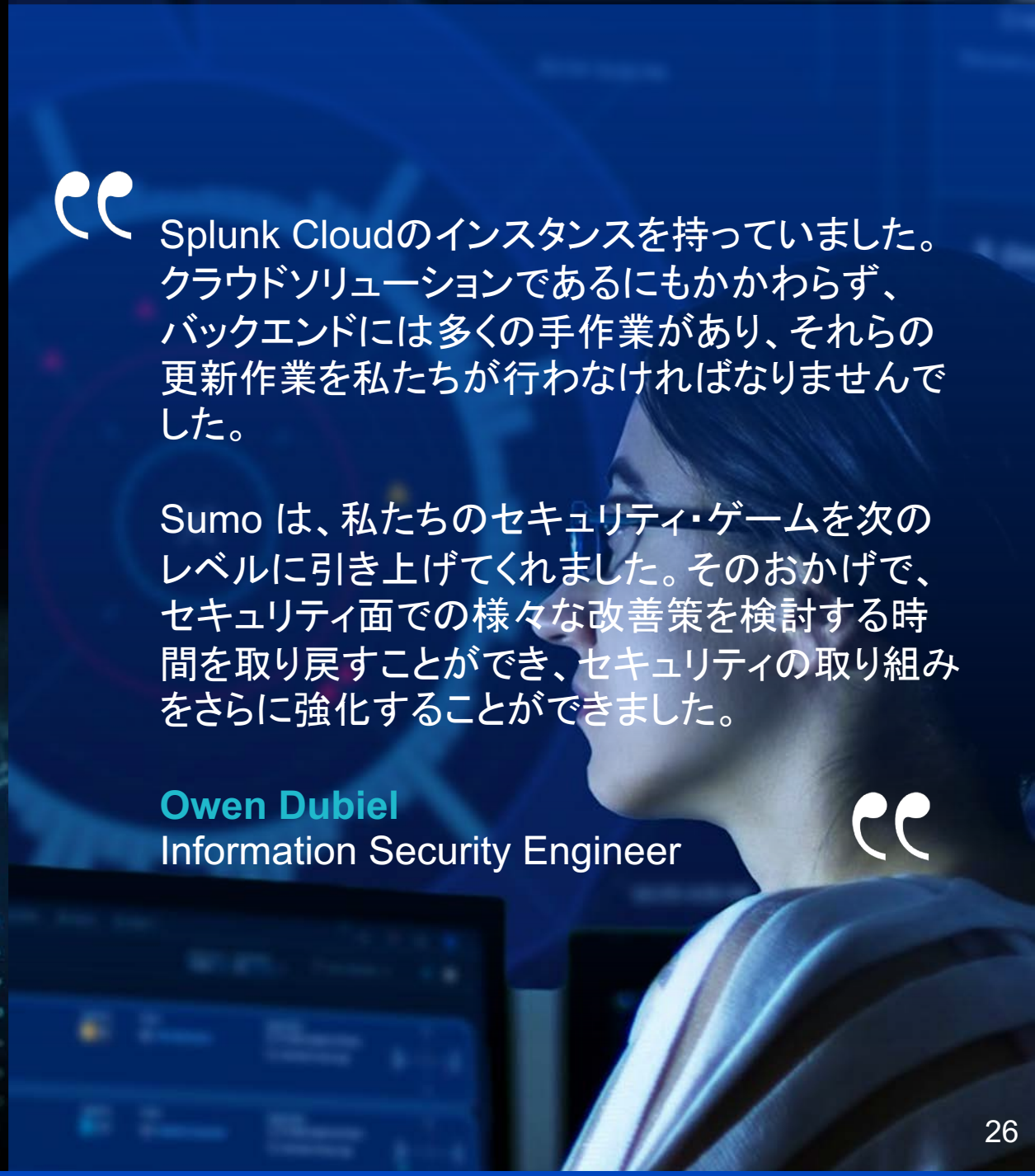
NorthAmerican BANCARD

SOC運用のモダナイズをCloud SIEMで実現

お客様課題

- Splunkは小規模SOCには使いにくい。
- SaaS版でもインジェスターの更新など運用負荷が高く、クラウドソリューションとは思えなかった。
- 長期間保存するログに対して料金が高すぎた。

Case Study: sumologic.com/case-study/north-american-bancard/



“Splunk Cloudのインスタンスを持っていました。クラウドソリューションであるにもかかわらず、バックエンドには多くの手作業があり、それらの更新作業を私たちが行わなければなりませんでした。

Sumo は、私たちのセキュリティ・ゲームを次のレベルに引き上げてくれました。そのおかげで、セキュリティ面での様々な改善策を検討する時間を取り戻すことができ、セキュリティの取り組みをさらに強化することができました。”

Owen Dubiel
Information Security Engineer

責任共有モデル　安全性の高いSaaS環境

- PCI DSS 3.2.1 Service Provider Level 1 Certified
- SOC 2 Type II attestation
- ISO 27001 certified
- CSA Star certified
- HIPAA-HITECH Attestation
- U.S. – EU Privacy Shield
- AES 256-bit encryption at rest
- TLS encryption in transit
- FedRAMP-Ready (Moderate)

Sumo Logic によるPCI DSS V4.0 への対応

可視化と監視

- ダッシュボードで監視作業を効率化
- レポーティングで監査時の負担を軽減
- 各種コンプライアンス要件をすでに満たしたSaaSで認定取得負担の低減

ログの統合管理

- 分析可能な状態でのログ、アラートの統合管理
- 3ヶ月を超えるログも分析可能な状態でありながら安価に補完可能
- 各種コンプライアンス要件を満たした安全性の高いデータ保管

脅威と異常の検出

- 設定の変更や異常をアラート
- リアルタイム相関分析による脅威の検出
- 任意のシステムからのログやアラートも収集、分析できる汎用性の高い検出

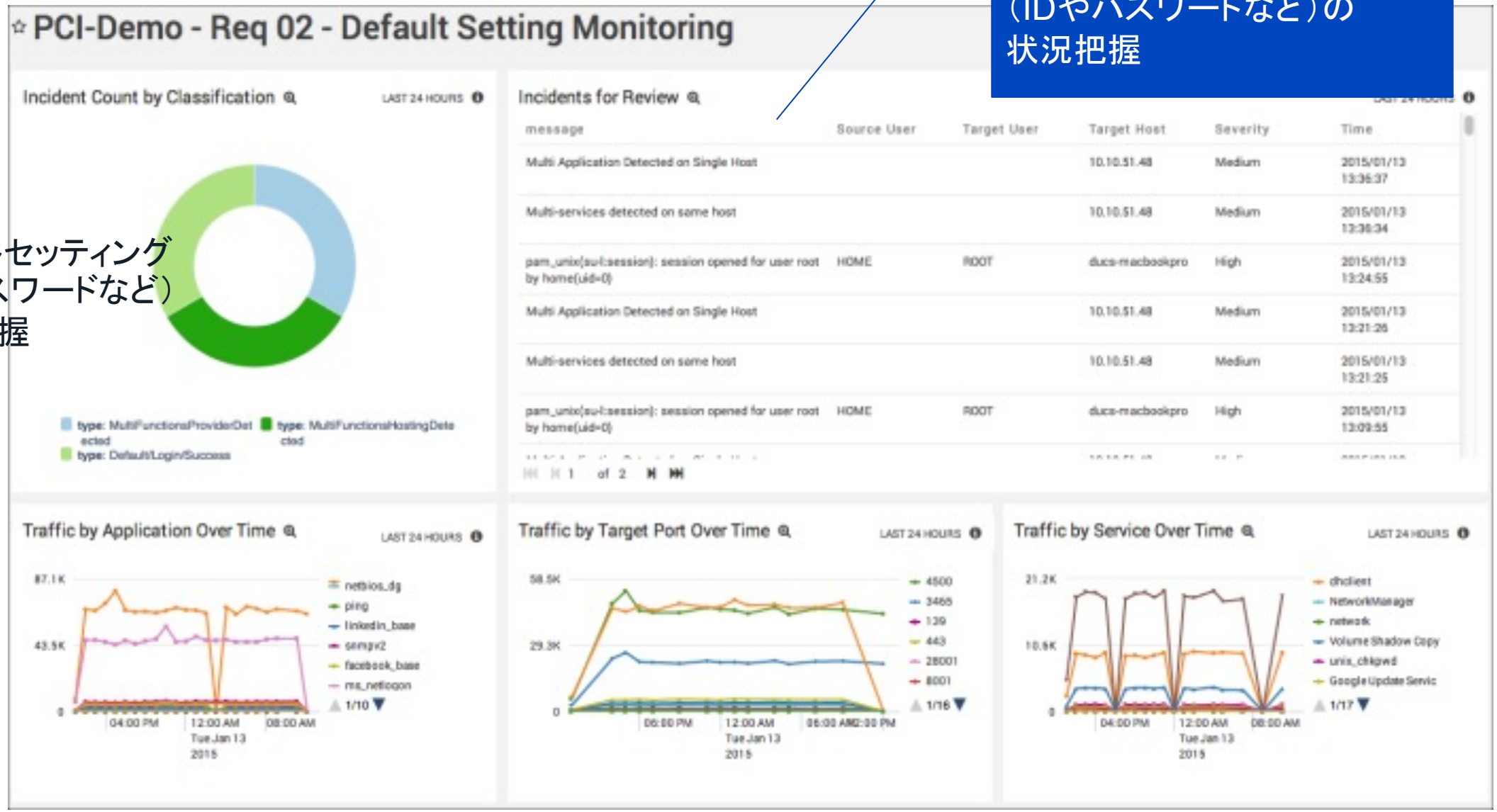
要件 1

ネットワークアクティビティの可視化、設定変更、イベントなどを監視

sumo logic

要件2

デフォルトセッティング
（IDやパスワードなど）
の状況把握



デフォルトセッティング
（IDやパスワードなど）の
状況把握

sumo logic

無料トライアルを提供


sumo logic
無料トライアルに今すぐ登録
クレジットカードは不要、数分で登録完了。
勤務先メールアドレス
アカウントの開設には会社のアドレスをお使いくだ
地域
アジア太平洋 – 東京
サービス使用許諾契約に同意します。
Sumo Logicからの連絡を希望します。
サインアップ
既にアカウントをお持ちの方。 ログイン
世界中で2,100社を超える企業がSumo Logicを採用し、クラウド上でのアプリケーションの運用とセキュリティ保護を行っています。
airbnb
ANHEUSER-BUSCH
pitney bowes
POKÉMON
SAMSUNG
WHOLE FOODS MARKET
Free
Enterprise
プライバシーポリシー 利用規約

ありがとうございました。

Sumo Logicジャパン株式会社
お問合せはこちら。
Email: info-jp@sumologic.com

sumo logic

s u

Empowering the people who power modern business

m o