

一粒で二度おいしい

Splunkを使って不正取引検知とサービス安定稼働を実現

Splunk Services Japan 株式会社
Sr Sales Engineer 横田 聡 CISSP

2019/05/30 Ver 1.0



Splunk

Spelunking:

洞窟探索

Splunking:

マシンデータの探索



マシンデータを、すべて人に、
マシンデータを、アクセス可能に、
マシンデータを、便利なものに、
そして、
マシンデータを、価値あるものに。

会社概要

会社

- ▶ 本社:
サンフランシスコ
- ▶ 社員数：5,000名以上
- ▶ 売上高（2019年会計年度）：
約\$18億（対前年比38%増）
- ▶ NASDAQ:
SPLK（2012年上場）
- ▶ 東京オフィス:
千代田区大手町

製品

- ▶ Splunk 製品ラインナップ
 - Splunk Enterprise
 - Splunk Cloud
 - プレミアムソリューション
 - Enterprise Security
 - IT Service Intelligence
 - User Behavior Analytics
 - Splunk Phantom
- ▶ 無料トライアル

お客様

- ▶ お客様数：世界15,000以上
110カ国以上
- ▶ 小規模組織から大企業まで
- ▶ Fortune 100社のうち90社
- ▶ 最大ライセンス:
 - 4PB/日以上

110カ国15,000社以上のお客様がSplunkを利用

Fortune 100社のうち85社

ケーススタディ

KPI設定で有識者でなくても状況が把握できる

システムステータスの強力な可視化に貢献するSplunk IT Service Intelligence

SBペイメントサービス株式会社

概要

ソフトバンクグループにおける決済や金融に関する中核企業として、決済代行を行った金融サービスを手掛けているSBペイメントサービス株式会社。EC運営事業者、クレジットカード決済やキャリア決済といった様々な決済手段を提供するオンライン決済をはじめ、ソフトバンク携帯ユーザー向けの通話料合算請求に関する開発・運営、加盟店審査や端末決済サービスの提供といったカード加盟店業務、カード発行業務を行っています。なかでも中核事業であるオンライン決済サービスは、40を超える決済しており、コンビニ支払いやプリペイドカード、口座振替、ポイント支払などがあります。2017年実績で取扱高が2兆5334億円、2018年度 10月実績で100,474店舗の誇る、業界屈指の決済サービスを提供しています。

ケーススタディ

口座の不正利用未然防止に向けた効率的な分析に大きく貢献

高度な相関分析で金融犯罪対策の一翼を担うSplunk Cloud



業種
金融機関

PDFをダウンロード

Mercari Engineering Blog

We're the software engineers behind Mercari. Check out our blog to see the tech that powers our marketplace.

2018/05 27 メルペイのAML/CFTシステムを支える技術

株式会社メルペイのAML/CFTチームでバックエンドエンジニアを務めているyagi5です。この記事はMERPAY TECH OPENNESS MONTHの6日目の記事です。

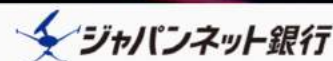
私たちメルペイが目指すのは、単なる決済手段を提供することだけではありません。「信用を創造して、なめらかな社会を創る」プラットフォームになることです。そのためには、お客様がメルペイ、メルカリを「あんしん・あんぜん」に利用できなければなりません。

メルペイにおいてその役割を担っているのが、筆者の所属する「AML/CFTチーム」です。この記事では、読者の皆さんには馴染みが薄いかもしれない「AML/CFT」について紹介すると共に、私たちが日々取り組んでいる、メルペイのあんしん・あんぜんを支える技術について書きたいと思います。最後までお読みいただければ幸いです。

ケーススタディ

株式会社ジャパンネット銀行

セキュリティが生命線のネット銀行を支える Splunk Enterprise の高精度な検知 & モニタリング



業種
ネット銀行

PDFをダウンロード
Japan Net Bank

標的型攻撃、進化するサイバー犯罪、なりすましや不正送金への対策にも使えば使うほど広がる Splunk Enterprise 活用フィールド

必要な時に、自分たちの手で、しかも高速で

高度化するサイバー攻撃に連携して対抗するため、わが国の金融業界ではサイバーセキュリティ情報を広く共有するエコシステムの考え方が普及しています。そのための枠組みとして設立された金融ISAC等を始めとする共助団体の中で、不正に使われたIPアドレス等の情報を共有しています。

マシンデータプラットフォームとして業界を牽引

あらゆる場所、種類、ボリュームのマシンデータ



様々な課題に応えるデータプラットフォーム



アドホック
検索



モニターと
アラート



レポートと
分析



カスタム
ダッシュボード



開発者
プラットフォーム

splunk>enterprise

splunk>cloud

プラットフォーム (Apps / API / SDKs)

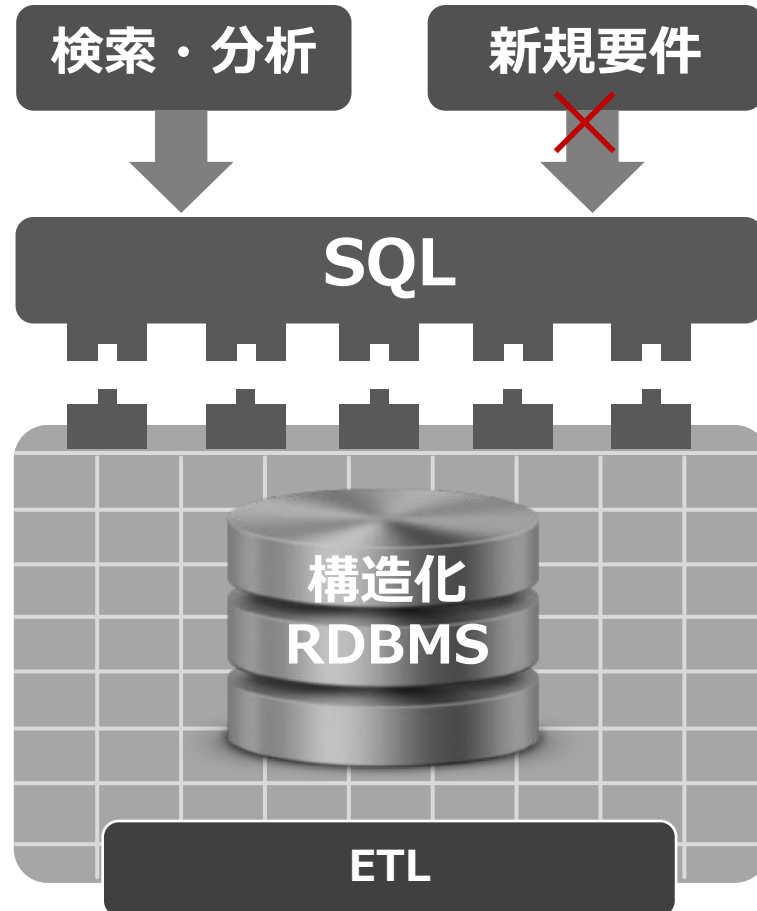
エンタープライズの拡張性

ユニバーサル・インデックス

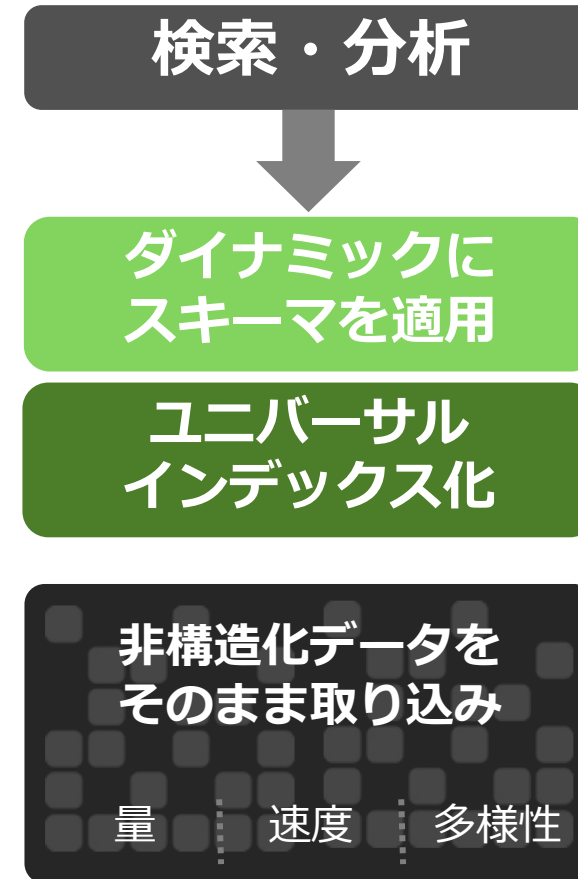
Splunk の強み

スキーマオンザフライ技術による新しいデータ分析基盤

従来



Splunk



様々なデータ同士を容易に“つなげる”事が可能

1,500種類近くのAppsを無償で利用可能



固定スキーマなし - どんなデータでもそのまま投入

マシンデータは、~~複雑~~ **VALUABLE!**

Web のアクセスログを見てみましょう！

```
10.2.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103] "GET
/product.screen?product_id=CC-P3-BELKIN-
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865
"http://shop.splunktel.com/product.screen?product_id=CC-P3-BELKIN-
BLK_BTTOOTH_HFREE" "Mozilla/5.0 (Linux; U; Android 2.3.5; FR-fr; SAMSUNG-
SGH-I927 Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like Gecko)
Version/4.0 Mobile Safari/533.1" 3875
```

マーケティング ユースケース:

例えば、言語ごとでどのプロダクトが参照されているか？

クライアントIP

10.2.1.35 **64.66.0.20** - - [21/Dec/2015 16:21:51:326103] "GET /product.screen?product_id=CC-P3-BELKIN-SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865 "http://shop.splunktel.com/product.screen?product_id=**CC-P3-BELKIN-BLK_BTTOOTH_HFREE**" "Mozilla/5.0 (Linux; U; Android 2.3.5; **FR-fr** SAMSUNG-SGH-I927 Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" 3875

参照されているプロダクト

ブラウザの言語設定

DevOps ユースケース:

新しいバージョンをリリースする前に、どの携帯端末が多く利用されているか？

10.2.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103] "GET /product.screen?product_id=CC-P3-BELKIN-SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865 "http://shop.splunktel.com/product.screen?product_id=CC-P3-BELKIN-BLK_BTTOOTH_HFREE" "Mozilla/5.0 (Linux; U; **Android 2.3.5**; FR-fr; **SAMSUNG-SGH-I927 Build/GINGERBREAD**) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" 3875

携帯端末のモデル

プラットフォーム

IT オペレーションユースケース:

エラーの発生している Web ページは？

Web サーバのIP

クライアントIP

10.2.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103] "GET
/product.screen?product_id=CC-P3-BELKIN-
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865

ステータスコード

ページリク
エスト

"http://shop.splunktel.com/product.screen?product_id=CC-P3-BELKIN-
_BTTOOTH_HFREE" "Mozilla/5.0 (Linux; U; Android 2.3.5; FR-fr; SAMSUNG-
H-I927 Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like Gecko)
Version/4.0 Mobile Safari/533.1" 3875

ブラウザ

セッションID

クライアントに返され
たサイズ

セキュリティユースケース:

不正アクセスされているWebサイトは？

クライアントIP からのロケーションを取得

時刻情報

10.2.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103] 'GET

ステータスコード

/product.screen?product_id=CC-P3-BELKIN-

SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865

"http://shop.splunktel.com/product.screen?product_id=CC-P3-BELKIN-

BLK_BTTOOTH_HFREE" 'Mozilla/5.0 (Linux; U; Android 2.3.5; FR-fr; SAMSUNG-

SGH-I927 Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like Gecko)

Version/4.0 Mobile Safari/533.1 875

携帯端末のモデルは？

怪しいブラウザじゃないか？
セキュリティパッチの適用
されていない古いバージョンで
はないか？

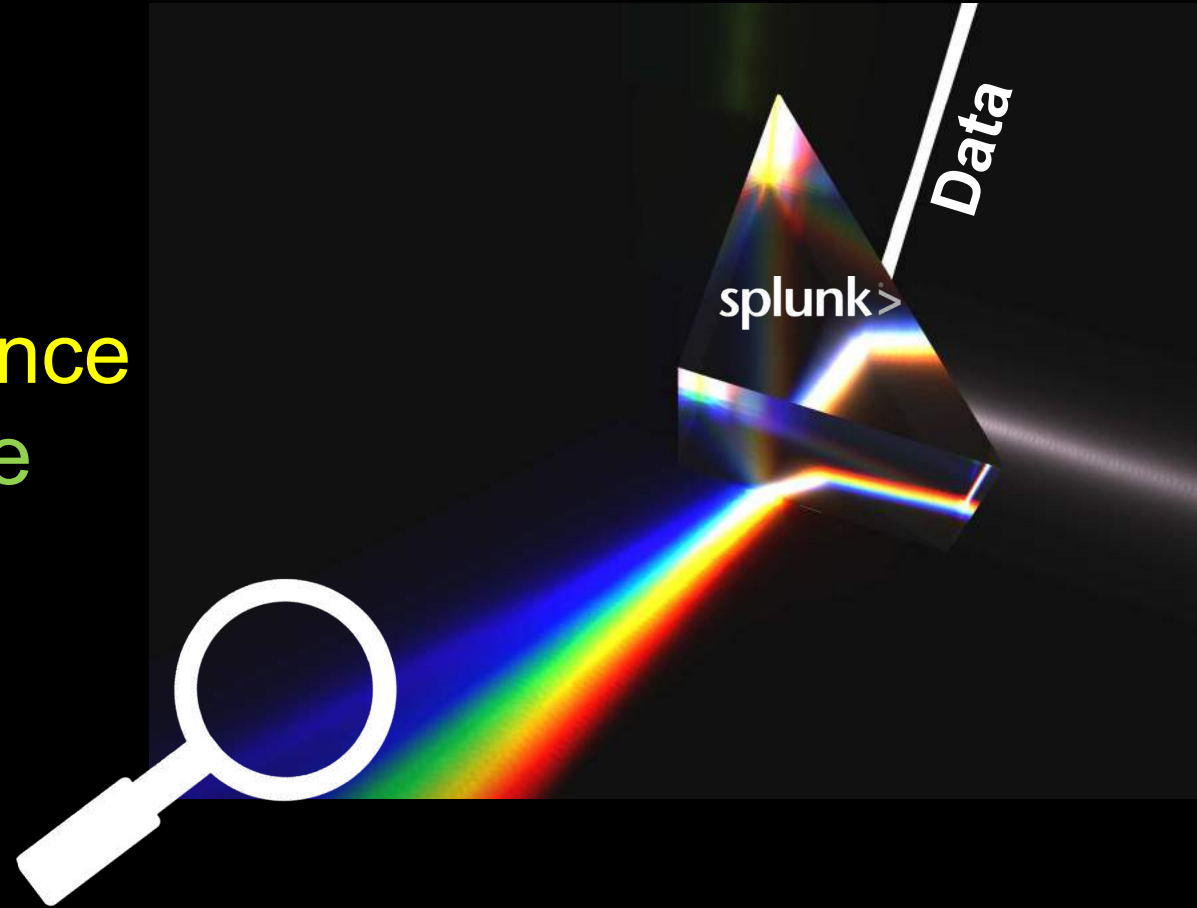
利用OSは？
セキュリティパッチの適用
されていない古いバージョン
ではないか

言語は？
想定していない言語を使っ
ていないか？
IPのロケーション情報と異
なっていないか？

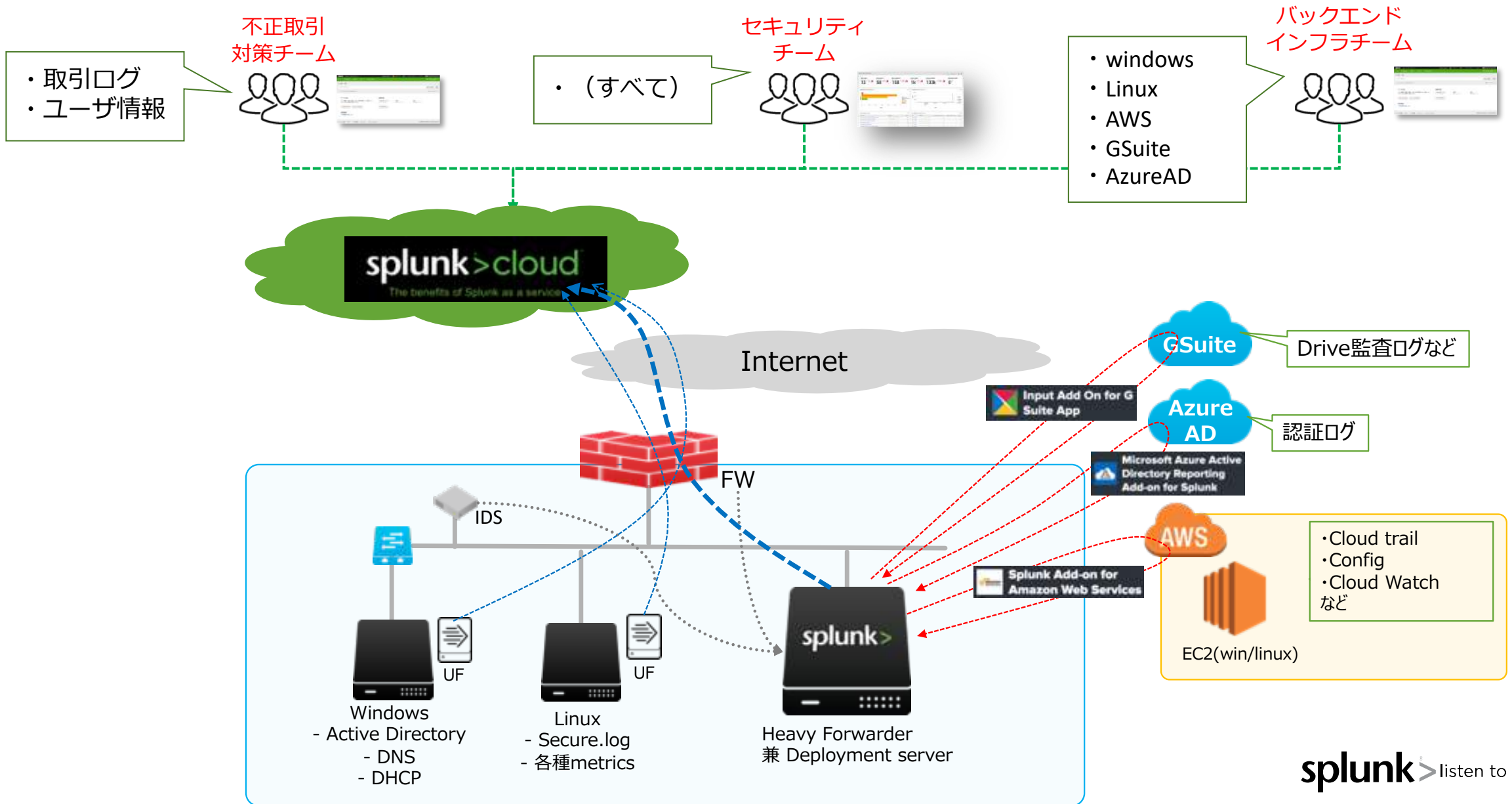
同じデータ, 違う切り口

同じデータを違う視点で、様々な角度から有効利用することができる

IT Operations
Security
Customer Experience
Risk & Compliance
Performance
Internet of Things



Splunkに取り込んだデータは複数の部門で横断的に使ってOK



FinTech ユーザ事例

不正取引対策 (AML)



分析データ

- インターネットバンキングのアクセスログ
- 勘定系システム内の預金取引に関する情報
- 銀行口座開設時の情報
- FraudAlert（カウリス社）による不正アクセスの判定結果
- 電話番号の履歴情報
- 自社作成のリストデータ

課題

- 複数のログを相関的に見て判断できるような高度な分析が必要に
- 人手でのアナログな処理によって業務負担が急増していた
- ビジネスの成長や、環境変化に合わせて、人員を増やさざるを得ない状況にあった
- 個別の仕組みでは横断的または複雑なルールが作りにくく、データ取り込みなど柔軟性に欠けていた

導入効果

- 必要なソースが柔軟に追加でき、検知の精度や幅が広がる
- システムによってリアルタイムな検知が可能な基盤が整備できる
- 職人肌になりやすい分析作業が標準化できる
- 効率化によって人員を増やさずともビジネスの成長に追随できるようになる
- データ取り込みが容易になり、トライ&エラーしやすい環境が整備できる

Splunk内で相関検索を行い疑わしい取引の検知

取引トランザクションログを元にした分析イメージ

User/ Account	IPアドレス	User-Agent	言語	国	キャリア	取引内容	取引日時	金額
user-001	202.***.***.15	123	ja-JP	Japan	so-net corporation.	購入	2019/05/01 16:05	200000
user-001	202.***.***.18	abc	ja-JP	Japan	so-net corporation.	購入	2019/05/01 16:05	1000
user-002	202.***.***.18	abc	ja-JP	Japan	so-net corporation.	購入	2019/05/01 16:10	1000
user-003	202.***.***.18	abc	ja-JP	Japan	so-net corporation.	購入	2019/05/01 16:15	1000
user-111	202.***.***.54	des	ja-JP	Japan	so-net corporation.	購入	2019/05/01 19:05	800
user-111	202.***.***.54	des	ja-JP	Japan	ntt corporation.	購入	2019/05/01 19:05	100
user-111	114.***.***.192	623	zh-CN	China	ntt corporation.	購入	2019/05/01 19:10	100
user-333	202.***.***.15	123	ja-JP	Japan	so-net corporation.	購入	2019/05/01 20:05	100
user-333	202.***.***.15	123	ja-JP	Japan	so-net corporation.	購入	2019/05/01 20:06	100
user-333	202.***.***.15	123	ja-JP	Japan	so-net corporation.	購入	2019/05/01 20:07	100
user-333	202.***.***.15	123	ja-JP	Japan	so-net corporation.	購入	2019/05/01 20:08	100
user-333	202.***.***.15	123	ja-JP	Japan	so-net corporation.	購入	2019/05/01 20:09	100

複数アカウントを用いて、
同じsrcIP(同じUA)の取引を検知

一定金額以上の取引の検知

1時間以内に複数の小額取引の累積
が500(例)を超えるものを検知

1つのアカウントから複数の
srcipを用いた取引を検知、

ITサービス安定稼働



分析データ

- 外部接続用のGW機器のログ
- アプリケーションサーバーログ
- DBサーバーログ
- Webサーバーのログ

課題

- ログを相関的に分析、原因究明までに膨大な工数が発生していた
- サーバーステータスを目視で監視せざるを得ず、非効率だった
- システム全体のステータス把握が困難だった
- 有識者でないと障害原因の特定が難しかった

導入効果

- 自動的にログ収集、効率的な分析が容易になり、依頼にも迅速に対応可能になった
- グラフィカルにサーバーリソースが可視化できるようになった
- KPIを設定し、色でステータスが一目で把握できるようになった
- 詳細情報までドリルダウンでき、障害原因のあたりが簡単に付けられるようになった

インターネットバンキングのセキュリティ



分析データ

- 社内OA環境
ファイアウォール、次世代ファイアウォール、プロキシ、アクセスログ、フィルタリングログ
- インターネットバンキング
アクセスログ、お客様取引ログ、リクエストヘッダ、レスポンスヘッダ、IP アドレスの地理情報、レスポンスタイム、WAF の検知情報など

課題

- 標的型攻撃対策のため社内OA環境のFW／プロキシログのサーチ・検索
- 不正アクセス対策のためWebアクセスログの素早い集計・分析
- なりすまし・不正送金対策のためお客様の取引ログ、リクエストヘッダ等の高精度なモニタリング

導入効果

- 従来は半日～1日かかっていたサイバー攻撃時の分析&対応を数分に効率化
- Splunk Enterprise を含む総合的な取組みにより、不正送金被害0件（2016年度）を達成
- Splunk Enterprise 活用により CSIRT メンバーがスキルアップし社内 SOC（セキュリティ運用センタ部門）が誕生

参考資料

- ▶ メルペイのAML/CFTシステムを支える技術（メルペイ）
<https://tech.mercari.com/entry/2019/05/27/112028>
- ▶ 口座の不正利用未然防止に向けた効率的な分析に大きく貢献（セブン銀行）
https://www.splunk.com/ja_jp/customers/success-stories/seven-bank.html
- ▶ セキュリティが生命線のネット銀行を支えるSplunk Enterprise の高精度な検知 & モニタリング（ジャパンネット銀行）
https://www.splunk.com/ja_jp/customers/success-stories/japan-net-bank.html
- ▶ KPI設定で有識者でなくても状況が把握できる（SBペイメントサービス）
https://www.splunk.com/pdfs/ja_jp/customer-success-stories/sb-payment-service-case-study.pdf

Thank you