ゼロトラストのその次へ
- サイバーハイジーンのためのマルチクラウド基盤の考え方

日本マイクロソフト株式会社
Chief Security Officer
河野省二, CISSP

Microsoft

ゼロトラストの整理を簡単に・・・

APT攻撃による境界型防御の限界

TCP/IP v4を利用するにあたってネットワークのアクセス制御をファイアウォールで行っていた

アプリケーション層からの攻撃はフィルタリングできず、新たなフィルタリングを検討しなくてはならなくなった

ネットワークセキュリティを拡張する形とエンドポイントセキュリティを充実させる形の2つに分かれ、SASEとゼロトラストにつながっている

さまざまなゼロトラスト

ゼロトラスト
ネットワーク

境界防御の限界

ゼロトラスト

静的アクセス制御の限界

ゼロトラスト
アーキテクチャ

リアルタイムガバナンス

IT部門やセキュリティ部門の都合の良い解釈で遠回りした数年間・・・

ゼロトラストの目的はガバナンスとサイバーハイジーン

サプライチェーン全体でこれらの対策を実施することで、攻撃に強い社会を作ることができる

どんな攻撃があっても事故が起きないようにするには

事故が起きるのは「脆弱性」があるから

脅威

様々な攻撃や災害など

×

脆弱性

攻撃の対象

攻撃が増加しても、巧妙になっても、攻撃の対象となる「脆弱性」がなければ、攻撃は成功しない

事故が起きるのは「脆弱性」があるから

攻撃が増加しても、巧妙になっても、攻撃の対象となる「脆弱性」がなければ、攻撃は成功しない

脆弱性を許容できる範囲に維持する

攻撃が増加しても、巧妙になっても、攻撃の対象となる「脆弱性」がなければ、攻撃は成功しない

脆弱性対策アプローチを一元化するために

ソフトウェアの脆弱性管理

Common Vulnerabilities and Exposures (CVE)

脆弱性 **放置されている**

ソフトウェアに脆弱性が見つかったら、修正プログラムを適用する。修正プログラムができていない、もしくはパッチが充てられていない状況を確認するためにCVEがある。マルウェア対策などには有効だが、攻撃全体を見ることは難しい

クラウドサービスの脆弱性管理

Cloud Security Posture Management (CSPM)

セキュリティ対策の状態

クラウドサービスは修正プログラムをユーザ側で適用する必要がないため、CVEのような概念は必要ない。その代わり、セキュリティ対策が期待通りになっているかを確認することで、脆弱性管理を行う。マルチクラウドにおけるセキュリティに課題がある

侵入に対する脆弱性管理

Attack Surface Reduction (Management)

攻撃が成功するポイント

ネットワークセキュリティや多層防御においては攻撃されるポイントを明確にし、それらを削減していくことで脆弱性のない環境を構築したいと考えていた。Surfaceといいながらも、その考え方はPoint的なものが多い

サービスレベルの脆弱性管理

多層防御 + サイバーキルチェーン

対策の単位を定義

単体のソフトウェア対策では十分ではないことから、レイヤーセキュリティを前提としたセグメントを定義し、それぞれのセキュリティ対策を計画。レイヤー間の関連性については十分に対応できなかった

ここまでやってるのに事故が起きてるのはなぜか

ゼロトラストによるセキュリティ対策の統合アプローチ

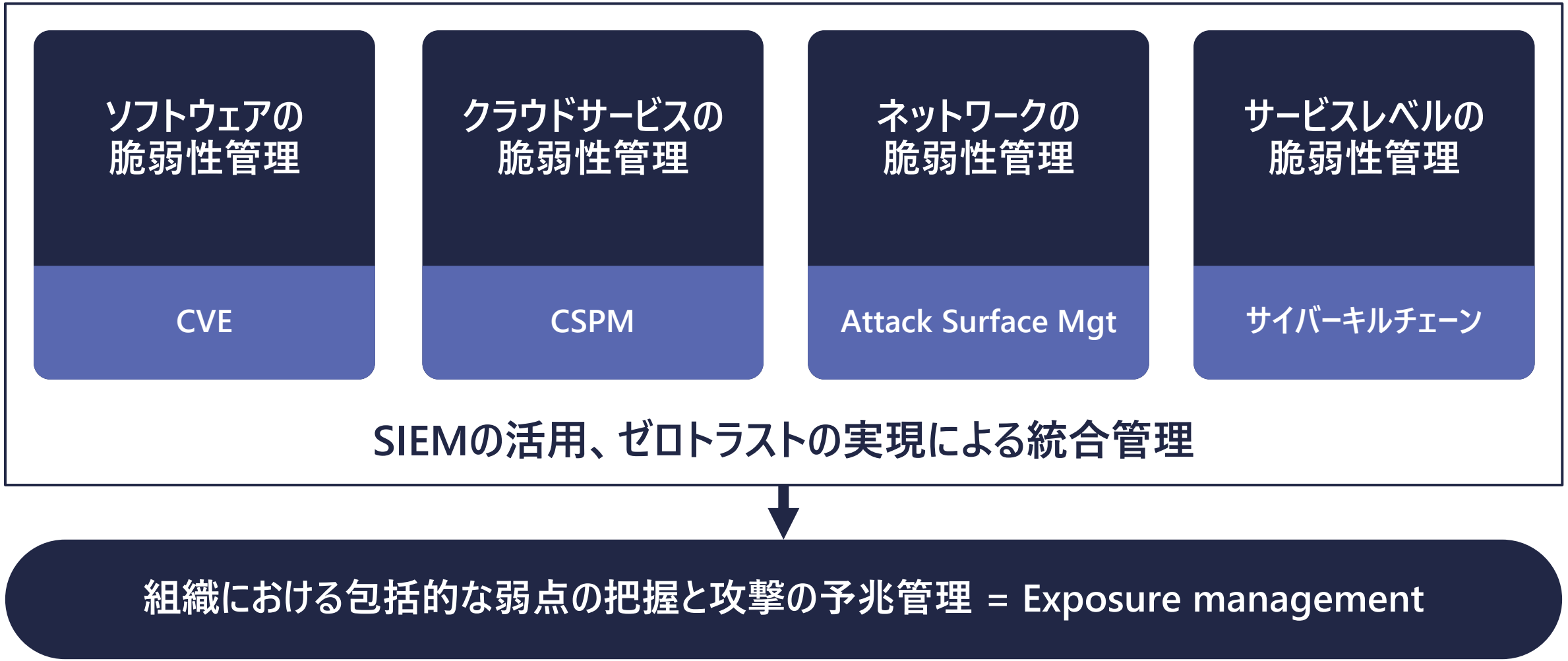
ゼロ トラスト アーキテクチャー

常に信頼できる状態

これまでばらばらだった様々な管理をまとめ、常に信頼できる状態を維持していくことを目的に、脆弱性管理の関連性を明確にした。しかし、境界防御の代替手段として捉えられることによって、本質的なアプローチができないことが多かった

ゼロトラストと多層防御は相性が悪い

真のサイバーハイジーンを実現するためのアプローチ

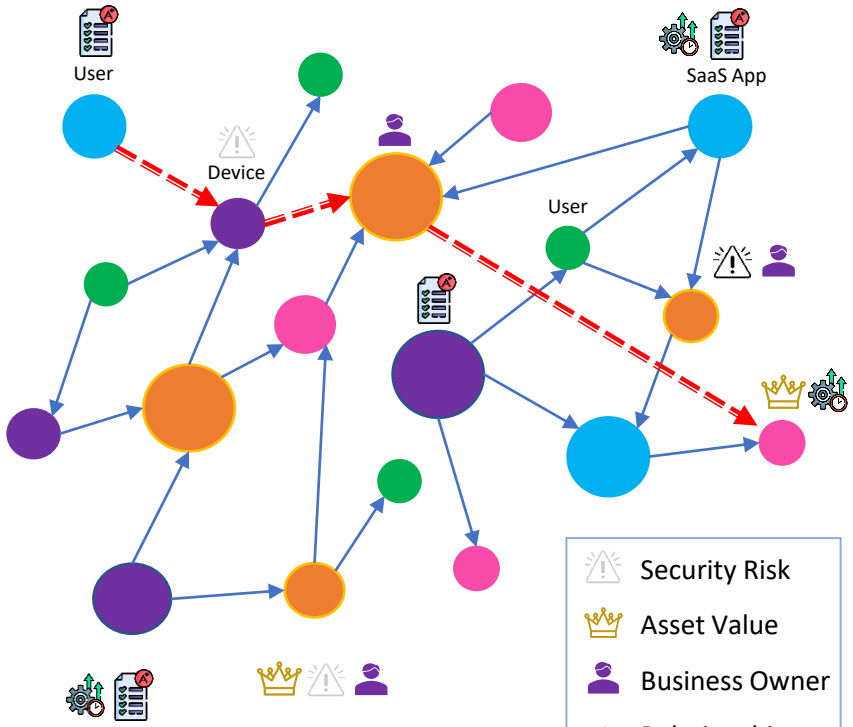


Exposure Managementによるサイバーハイジーン

CMDB
servicenow
Vulnerability Management
tenable.io
Email Security
proofpoint. AVANAN
Identity Security
okta CROWDSTRIKE
Endpoint Security
CROWDSTRIKE
SaaS Security
OBSIDIAN ADAPTIVE SHIELD
Application Security
snyk Checkmarx
Cloud Security
paloalto WIZ
External Attack Surface
paloalto CYCOGNITO
Threat Intelligence
Recorded Future

アセットメタデータ
運用状況
構成データ
ポリシー
セキュリティ調査
サービス状態

エンティティ把握の解像度を向上
整理、正規化、集約、重複排除、コンテキスト

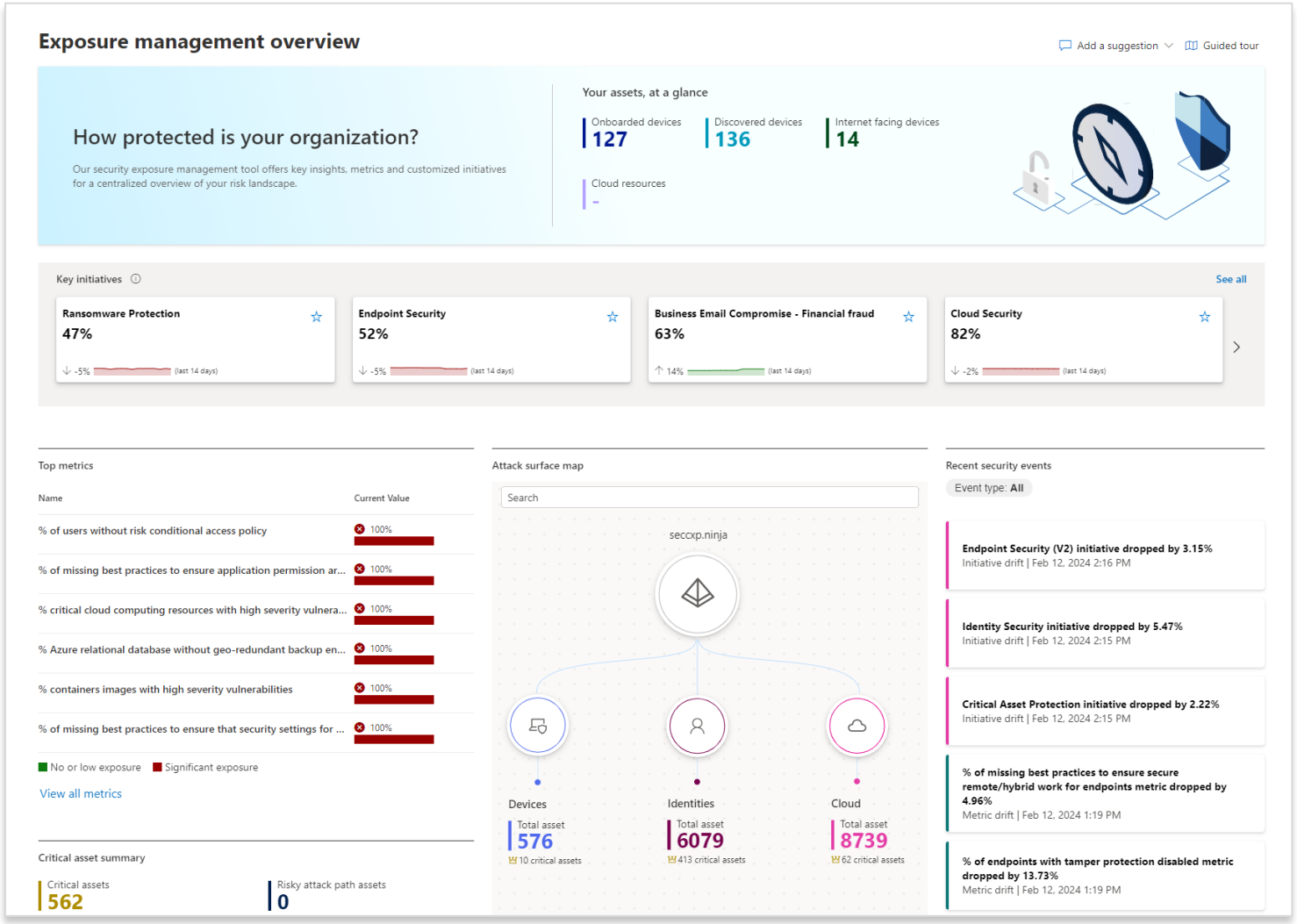


攻撃パス分析
従来のサイロ化されたアプローチからの脱却、攻撃者の視点を考慮して脆弱性対策の優先順位を決定

Attack Surface管理
組織の資産を継続的に判別、コンテキストを整理、管理し、攻撃者の視点を提供

一元管理
セキュリティ状況を把握し、既成概念にとらわれない洞察力で担当者からの問いに積極的に対応

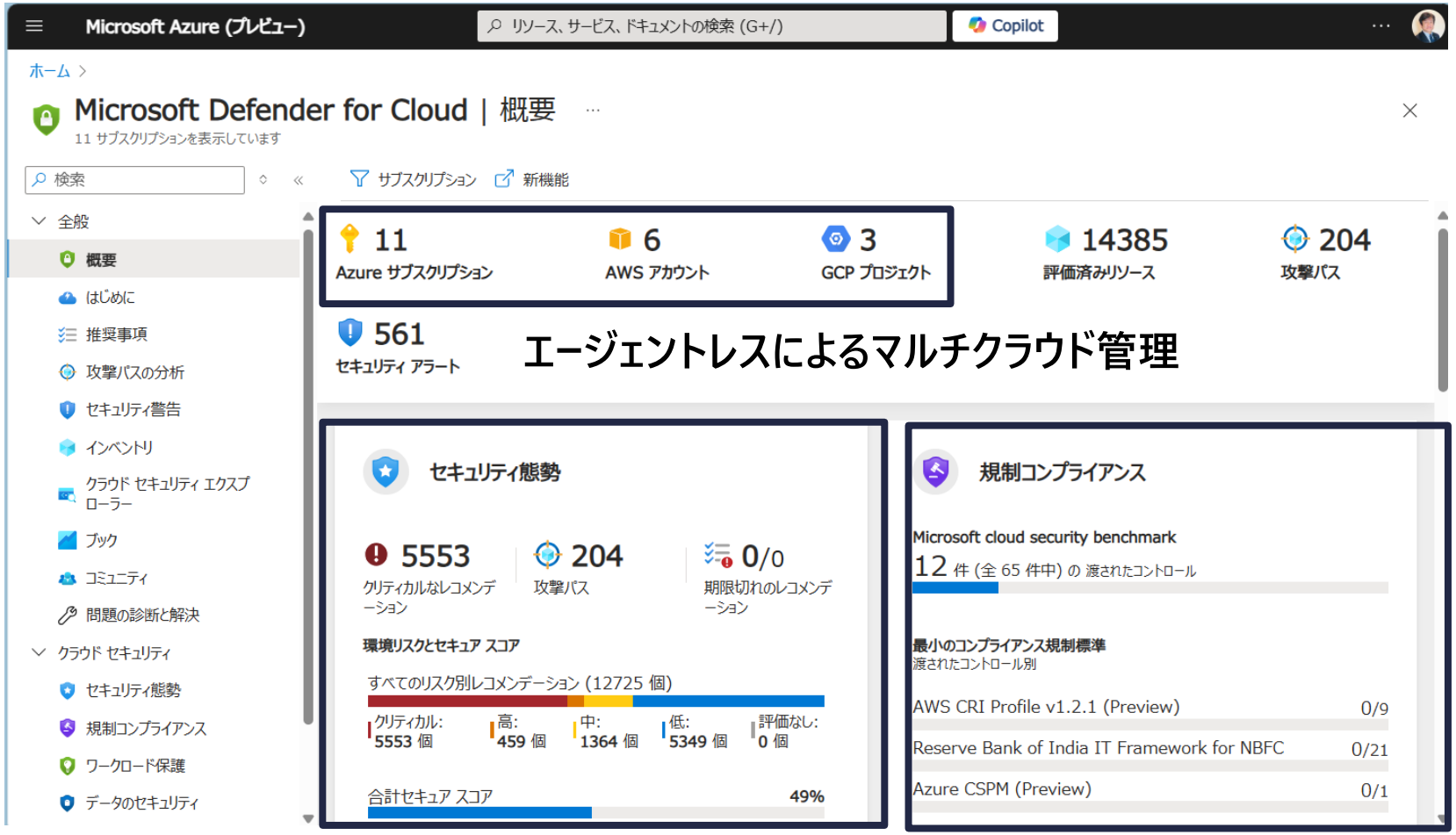
Exposure Managementによる弱点の一元管理



個別のセキュリティ管理の関連づけによる新たな発見と対応

- 脆弱性管理
- Attack Surface管理
- クラウドサービスセキュリティ
- エンドポイントセキュリティ
- アイデンティティセキュリティ
- CASB
- 電子メールセキュリティ
- OT/IoTセキュリティ
- 資産管理
- 構成管理

マルチクラウド・オンプレミス統合管理



マルチクラウドポスチャー管理

ISOやNISTなどの標準対応状況

規制・コンプライアンス管理

各国・業界の規制を分析

↓

Microsoft Cloud Security Benchmark

↓

それぞれの規制に再マッピング

↓

各サービスでのリアルタイム監査

↓

必要に応じて修正

セキュリティ対策の一元化によるガバナンス

予防的対策による
サイバーハイジーンの実現

インシデント対応の自動化と
深い洞察の実現

SIEMとかUEBAとか・・・ではない基盤構築

SIEM	XDR	UEBA
セキュリティログから 何がわかるの？	複数のサービスの セキュリティ基準をどうする？	行動を管理するための 基準は？
侵入検知主体の記録	いつもと違う状態の記録	アクセス管理の記録

ゼロトラストの目的　＝　サイバーハイジーン（脆弱性のない状態）

グラフデータベースによるリアルタイムガバナンス、マイクロサービスによるレジリエンス


Microsoft Security
Microsoft