

Microsoft 365/Microsoft Defender for Cloud によるゼロトラストの実現

～Modern SOC の活用編～

レベル 200

自己紹介

- 国井 傑 (くにい すぐる)
 - 株式会社エストディアン 所属
 - マイクロソフト認定トレーナー (1997～2023)
 - Microsoft MVP for Enterprise Mobility (2006～2022)
 - <http://AzureAD.net>
- 主な職務・実績
 - ID 関連技術/運用管理を中心としたトレーニング
 - 評価ガイド執筆多数 (Microsoft 365 Defender, MECM 等)
 - テクニカルライター (@IT, ITpro, ZDNet Japan 等)



本セミナーの概要と目標

- Microsoft 365 Enterprise と Microsoft Defender for Cloud を利用した組織内のセキュリティ対策とその運用方法について、概要を紹介します。
本コースでは、セキュリティ対策の構成要素としてゼロトラストと Modern SOC について取り上げ、それぞれの構成要素の概要とその必要性について解説します。
- 以上のトピックを通じて、次の内容の理解を目指す
 - Microsoft Azure リソースを保護するために利用可能な Microsoft Defender for Cloud の機能について説明できる
 - セキュリティ対策に活用できる Microsoft 365 Enterprise の機能について説明できる

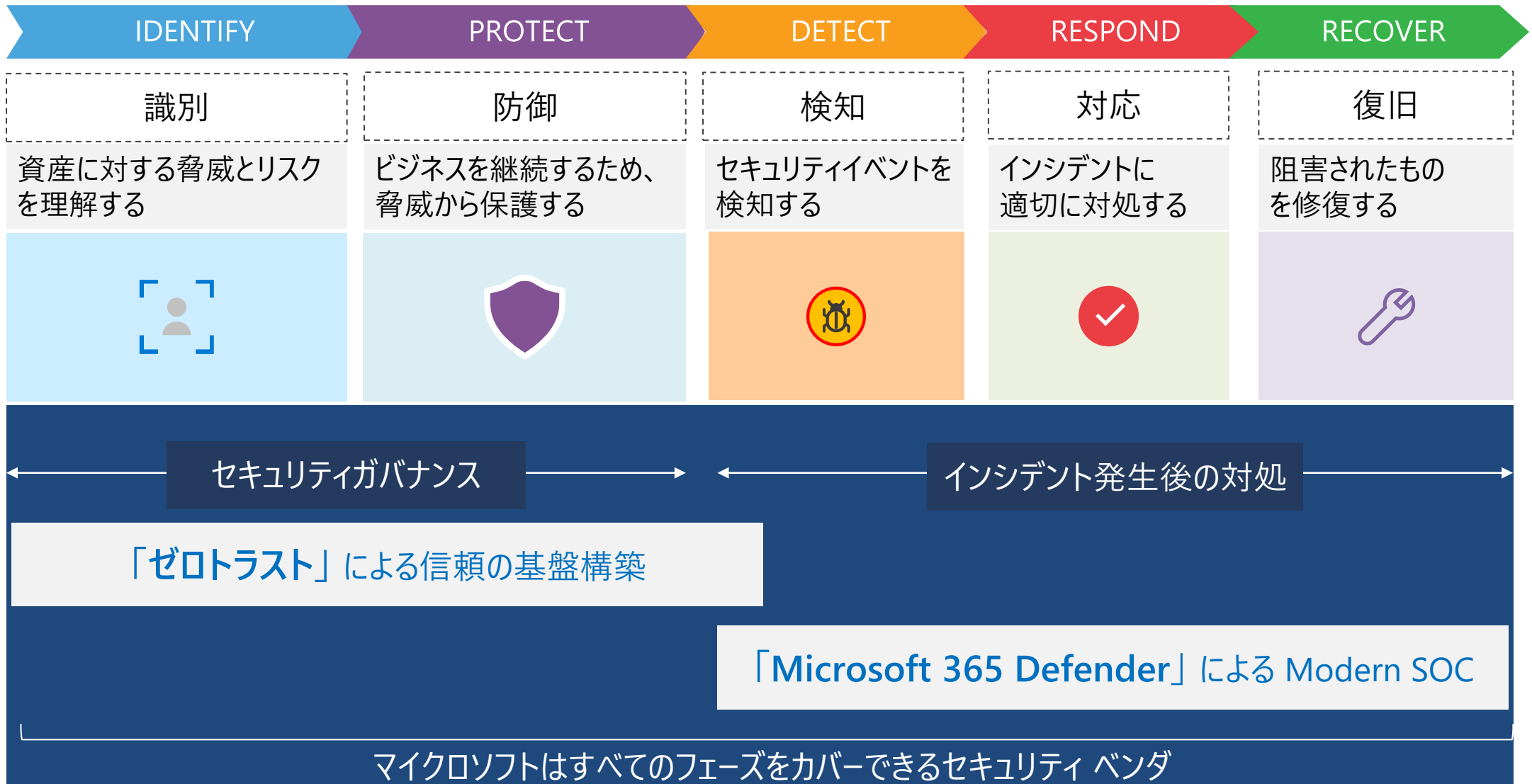
本セミナーの対象者、レベル、前提知識

- 対象者：Microsoft 365/Microsoft Azure を中心としたセキュアなインフラストラクチャの提案を検討している営業 / プリセールス SE
- レベル：200
- 前提知識：以下の知識をお持ちであること
 - Microsoft 365/Microsoft Azure に関する基本的な知識
 - Windows 11/10 に関する基本的な知識

本セミナー シリーズの内容

- ゼロトラスト アーキテクチャ編
- ID 分野のゼロトラストの実現編
- デバイス分野のゼロトラストの実現編
- アプリケーション/データ分野のゼロトラストの実現編
- インフラ/ネットワーク分野のゼロトラストの実現編
- Modern SOC の活用編

NIST CSF とマイクロソフトのアプローチ



Modern SOC によるインシデント対応

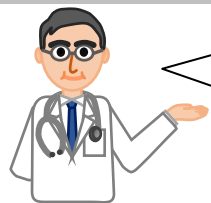
ゼロトラストによるセキュリティ対策ができれば、検知・対応・復旧のステップは必要なさそうですね



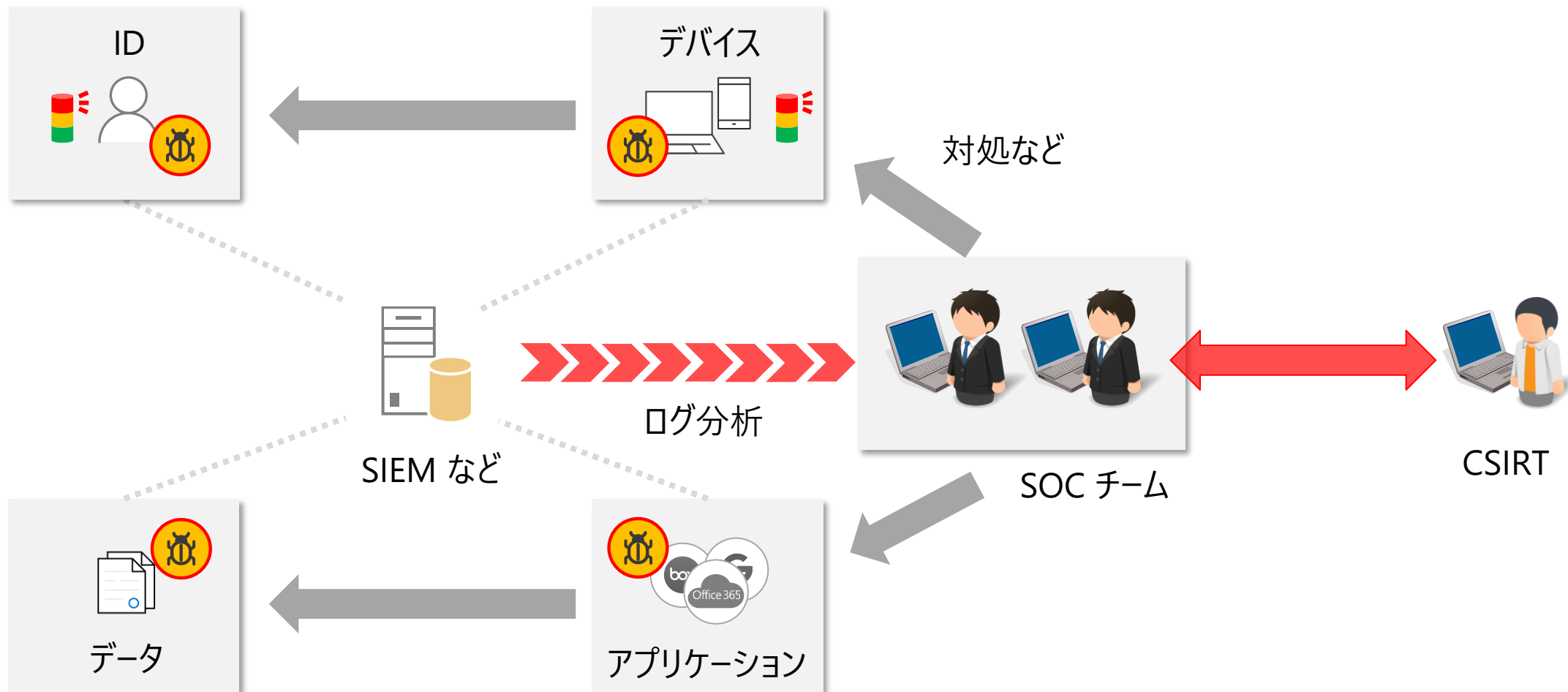
そんなことはありません！

火のもとを用心していても火災は起こるように、セキュリティ対策を行っていても残念ながらセキュリティ インシデントは起こります。SOC によるインシデント対応の体制を整えておきましょう！

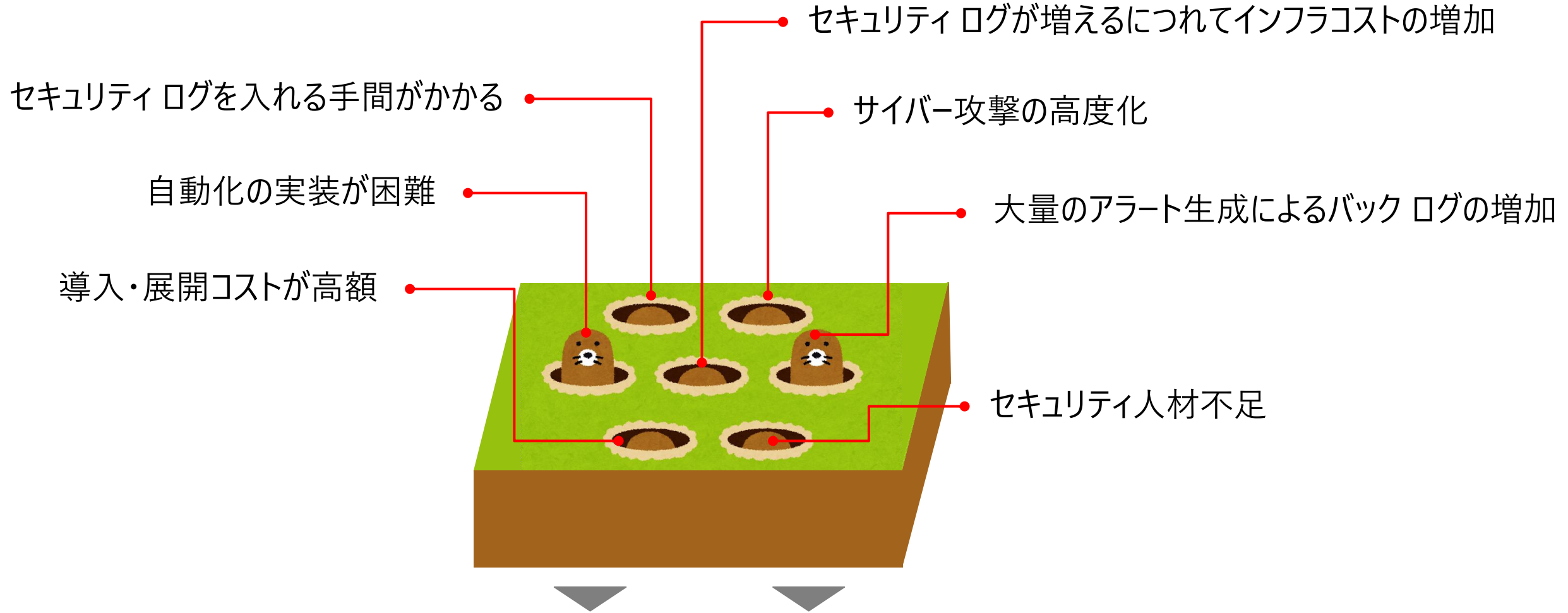
SOC とは



Security Operation Center (SOC) は攻撃の検出や分析を行い、脅威の発生時には事象の通知や対処方法のアドバイス等を行います

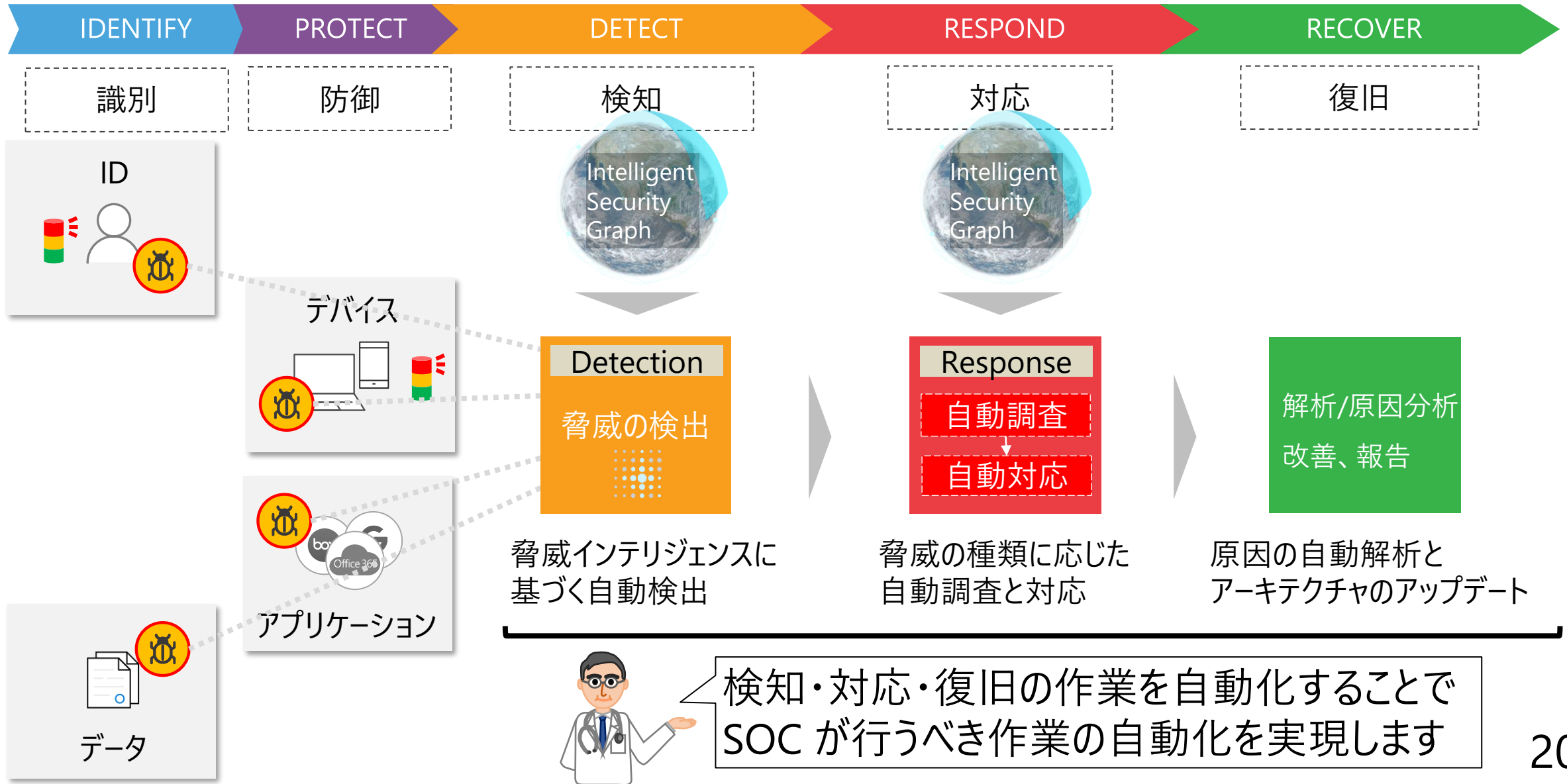


SOC の課題



Modern SOC の導入によって、これらの課題を解決

SOC から Modern SOC へ



- Microsoft 365 で提供するサービスのうち、攻撃の防止・検知・対応に活用できるソリューション群

Microsoft Defender for Identity



- Active Directory をはじめとする オンプレミスの不正アクセスをクラウドベースで分析・検知

Microsoft Defender for Endpoint



- デバイス上の アクティビティを収集・分析し、不正アクセスを検知

Microsoft Defender for Office 365



- Exchange Online をはじめとする Office 365 のトラフィックを分析し、マルウェアやフィッシング詐欺行為を検出

Microsoft Defender for Cloud Apps



- クラウド サービスへのアクセスを分析し、あらかじめ企業で定めた範囲外のアクティビティを検出

Microsoft Defender for Endpoint で実現するインシデント対応の自動化

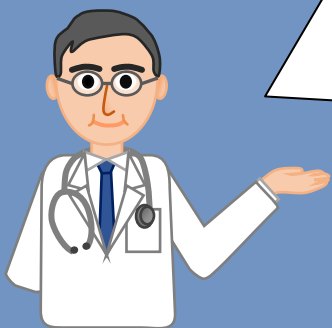
そもそも EDR ってなに？

Microsoft Defender for Endpoint は EDR としてのサービスを提供すると聞きましたが、そもそも EDR ってなんですか？

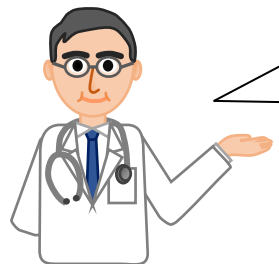


EDR とは Endpoint Detection & Response の略で、オンボーディングされたデバイスの動きを監視し、

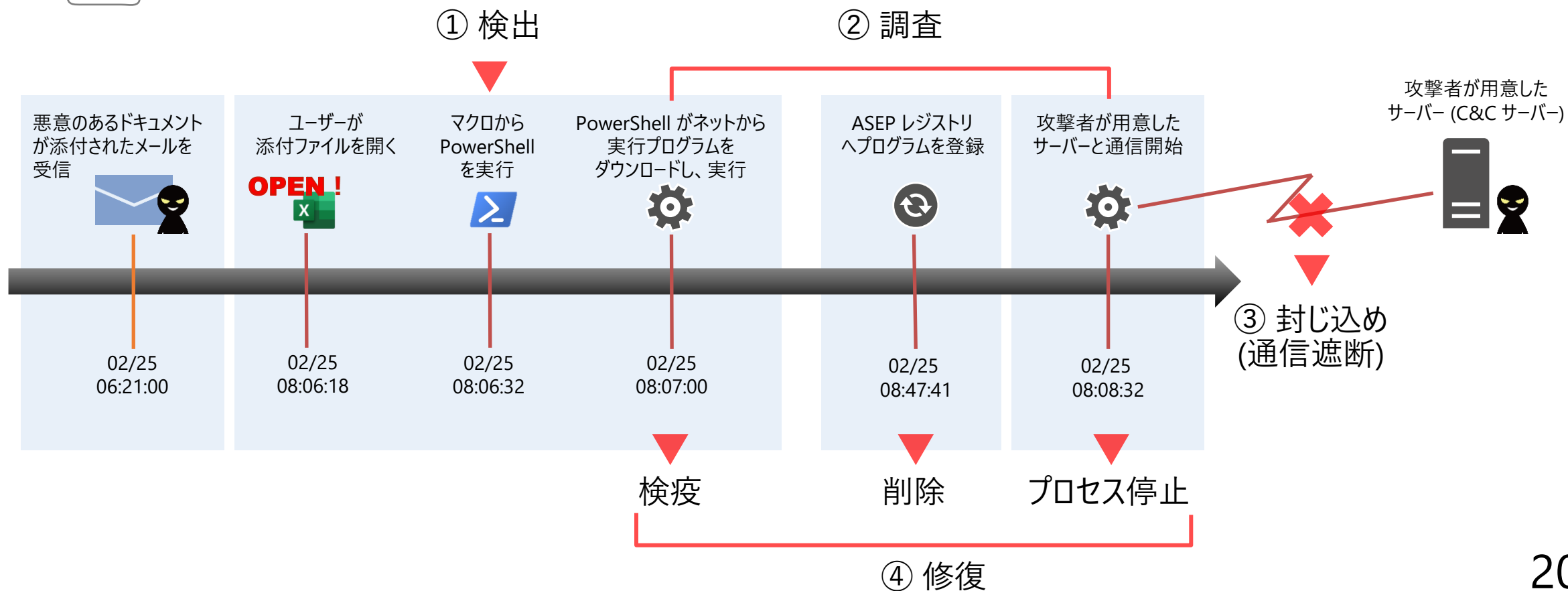
- ① セキュリティ インシデントの検出
 - ② セキュリティ インシデントの調査
 - ③ インシデントを封じ込め
 - ④ エンドポイントを修復
- を実施します。



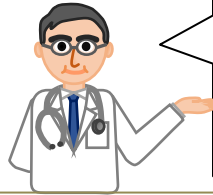
Microsoft Defender for Endpoint による インシデント対応



Microsoft Defender for Endpoint では攻撃を検出すると、
調査・封じ込め・修復までの処理を自動的に実施します

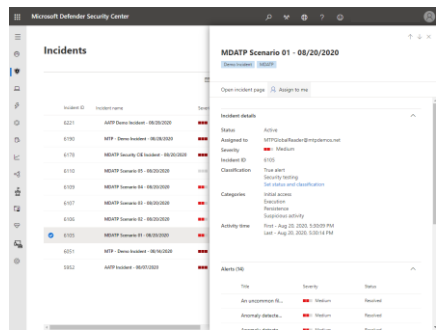


インシデント対応の流れ



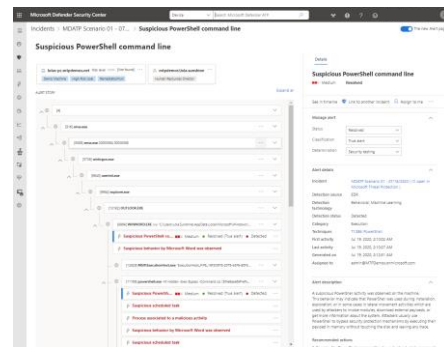
自動調査が有効な場合、アラートを自動的に調査し、脅威の修正を行います。
これによりアラート / インシデント発生からクローズまでの操作をすべて自動化できます。




① インシデントページでアラート確認



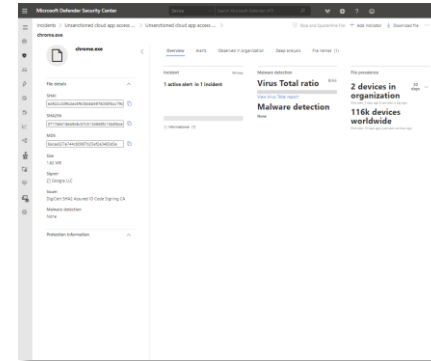
Multi-Stage incident Execution & Defense evasion on one endpoint インシデント




② アラートをドリルダウンして詳細確認



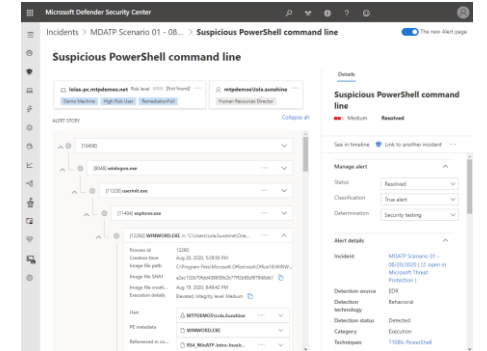
-  WORD ファイルから EXE ファイルの生成と実行
decode-backdoor.exe
-  攻撃者サーバーから EXE ファイルをダウンロード & 実行
mcujpRy.exe
-  ASEP レジストリへの登録
HKLM\Software\Microsoft\Windows\CurrentVersion\Run




③ デバイスやファイルにアクションを実施



-  ファイルの削除
-  ファイルの削除
-  レジストリの削除

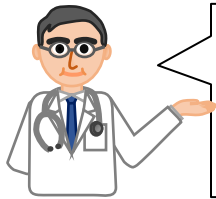
④ インシデント/アラートのクローズ



-  アラートのクローズ
-  インシデントのクローズ
-  インシデントのクローズ

Microsoft Defender for Office 365 で実現するインシデント対応の自動化

Microsoft Defender for Office 365 (MDO)



Microsoft 365 プラットフォームを高度な脅威から保護し、侵入した脅威を自動的に調査して対応することで、安全なコラボレーション基盤をひとつのサービスで実現します



基本的対策

スプーフィング対策

DMARK, DKIM, SPF
ドメイン/ブランド偽装検出
アンチウイルス/スパム対策
メールボックス インテリジェンス

Exchange Online Protection
ゼロアワー自動消去(ZAP)



高度な脅威への対策

コンテンツ分析

添付ファイルの詳細解析
悪意のある URL の検査
BEC/なりすましメール対策
不審なパスワード付ZIP対策

Safe Attachments
Safe Links, フィッシング対策
Safe Documents*



調査の自動化

プレイブック

脅威の詳細調査
調査時間の短縮(自動化)
デバイス(MDE)とのシグナル共有

脅威エクスプローラー
自動調査と応答 (AIR)
キャンペーンビュー



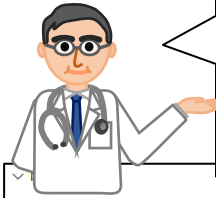
人的対策

ユーザートレーニングとリテラシー向上

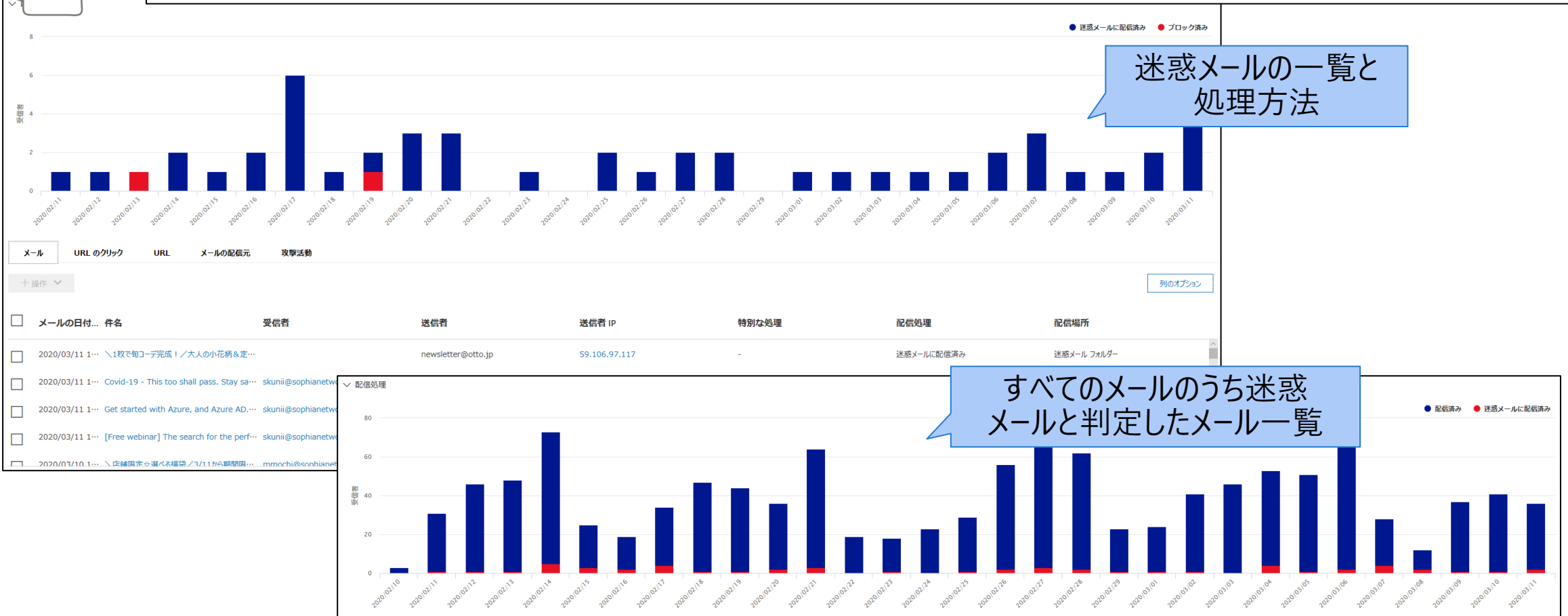
標的型メール攻撃訓練
パスワード スプレー攻撃テスト
ブルートフォース パスワード攻撃テスト

攻撃シミュレーター

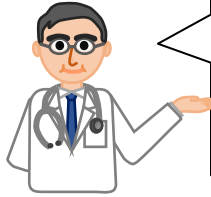
익스プローラー 뷰による攻撃の検知と検知内容の参照



익스プローラー 뷰ではマルウェア入りメール、フィッシング詐欺メール、すべてのメールの単位で組織・個人で受信したメールの一覧を参照できます。



自動調査と応答 (AIR)



特定のメールを対象に詳細な調査を行い、調査結果の報告と行うべき対応を提示 (自動対応) します。調査は管理者によって開始できるほか、ユーザー報告に基づき自動開始することも可能です。

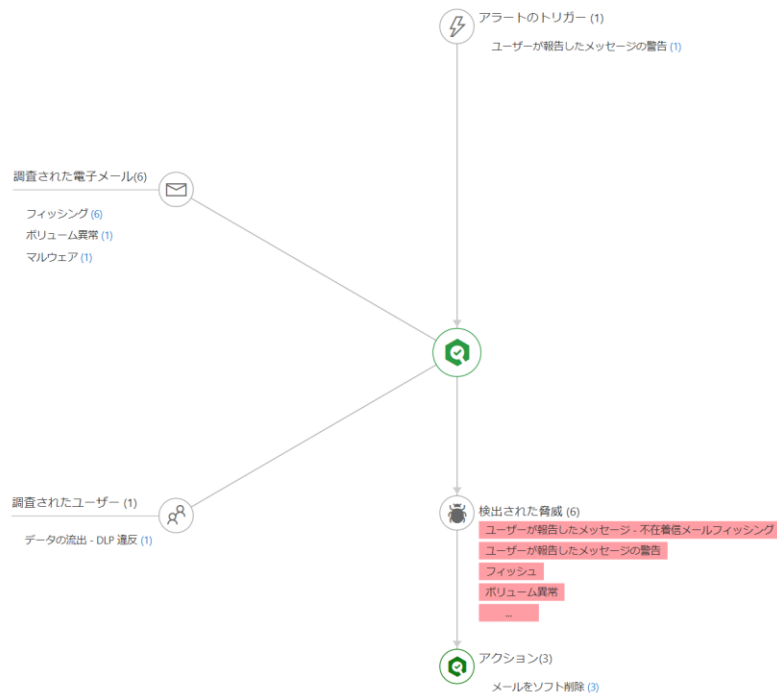
 ユーザーは、悪意のある「重要:MSDI - ワトルズ・ウィ...」
調査#9c2f5bが修復される

User reported message as malicious "IMPORTANT: MSDI - Wattles Withers" for "Phish"

開始時刻
2020年11月17日 13:46:35
終了時刻
2020年11月18日 7:10:25
保留中の合計時間
0日16時間37分

17:23:50
修理

調査グラフ アラート 1 電子メール 6 ユーザー 1 マシン エンティティ ログ アクション 3



・ユーザーがOutlookアドイン「レポート メッセージ(報告)」を実施したことをトリガーとして動作し、当該ユーザー以外のユーザー メールボックスも含めて調査が自動的に実施される。

(その他の自動調査の実行トリガー)

- ・判定変更された悪意のあるURLリンクをユーザーがクリック
- ・メール配信後に、マルウェアを検出 (マルウェアZAP)
- ・メール配信後に、フィッシングメールを検出 (フィッシングZAP)
- ・侵害されたユーザーの検出 (不審なメール送信/メール送信制限)

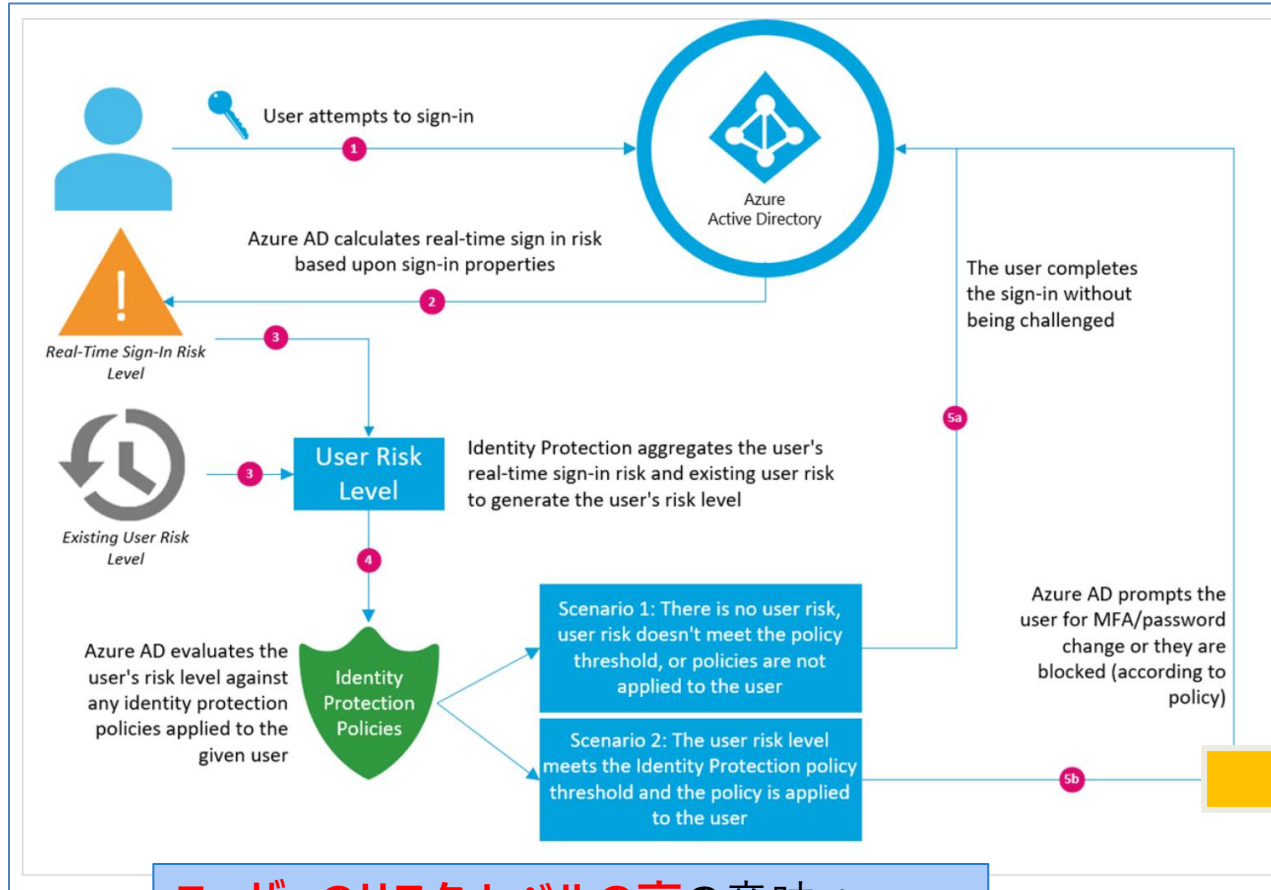
・Microsoft Security Intelligent Graph を通じ、Microsoft Defender for Endpoint (MDE) との検出シグナルの共有が可能のため、連携時にはパスワード付 zip ファイル等のフィルタリングをすり抜けたものをエンドポイントで検出した際、同不審メールをMDO でも検出し調査できるようになる。

・「ユーザーからの報告」以外にも、手動での調査開始や API 経由での調査開始も可能。

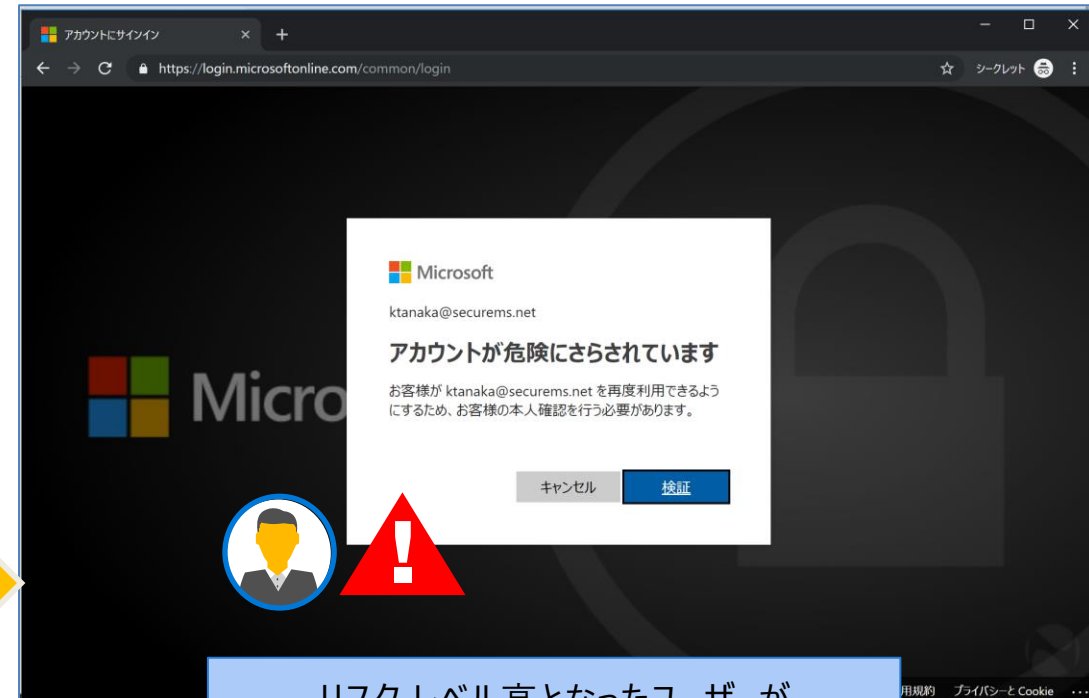
ID 分野の脅威の検出とインシデント対応の自動化

Azure AD Identity Protection によるパスワード漏洩対策

Azure AD Identity Protection のユーザー リスク ポリシーで
ユーザーのリスク(低 / 中 / 高) を監視



ユーザーのリスク レベルが管理者が
定義したユーザー リスク レベルを
超えた場合は動的なアクションを実施

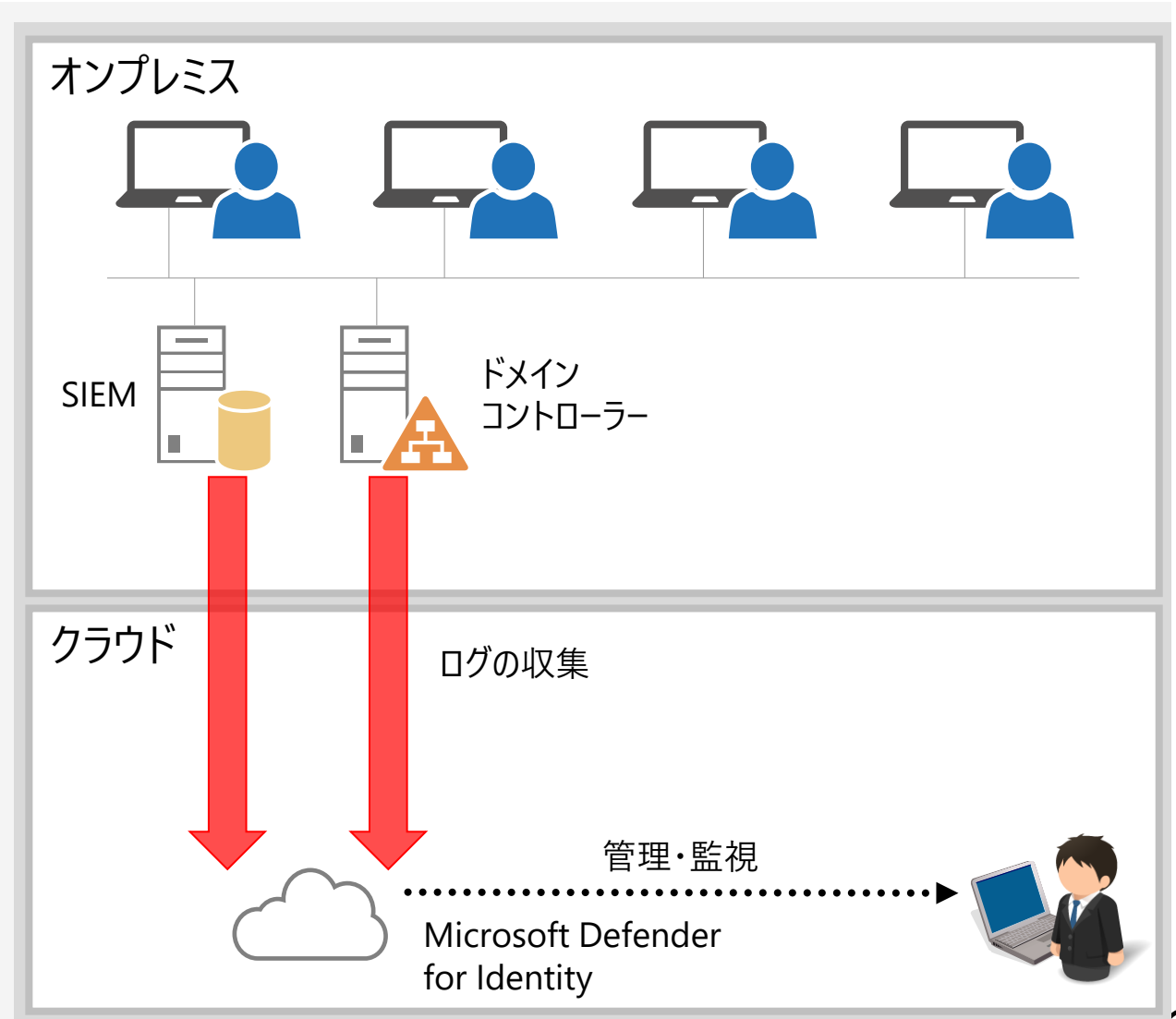


ユーザーのリスクレベルの高の意味：
侵害された可能性が高く該当するユーザー アカウントを
すぐに修復する (パスワードの変更) 必要がある状態

リスクレベル高となったユーザーが
サインインするとアカウントが
危険な状態であることを警告

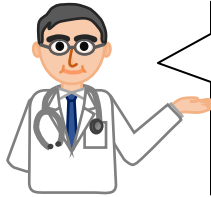
Microsoft Defender for Identity

- Microsoft Defender for Identity とは Active Directory やオンプレミスのトラフィックを収集・分析し、不正アクセスを検出した際にはアラートを出力
- オンプレミスのサーバーにセンサーを設置し、主に次の攻撃を検出
 - ・ 偵察
 - ・ 資格情報の侵害
 - ・ 横方向の活動
 - ・ ドメインの支配
- オンプレミスの攻撃を検出することで、マルウェア感染後に行われる攻撃に対処



Microsoft Sentinel で実現する セキュリティ運用負荷の軽減

Microsoft Sentinel



Microsoft Sentinel は SIEM, SOAR, UEBA の 3 つの性質をあわせ持つ Microsoft Azure のサービスで各種サービスのログ収集、多角的なログ分析と対応を自動化します



Microsoft Sentinel

Cloud Native

SIEM as a Service

Security Information & Event Management

+ SOAR + UEBA

Security Orchestration Automation & Response

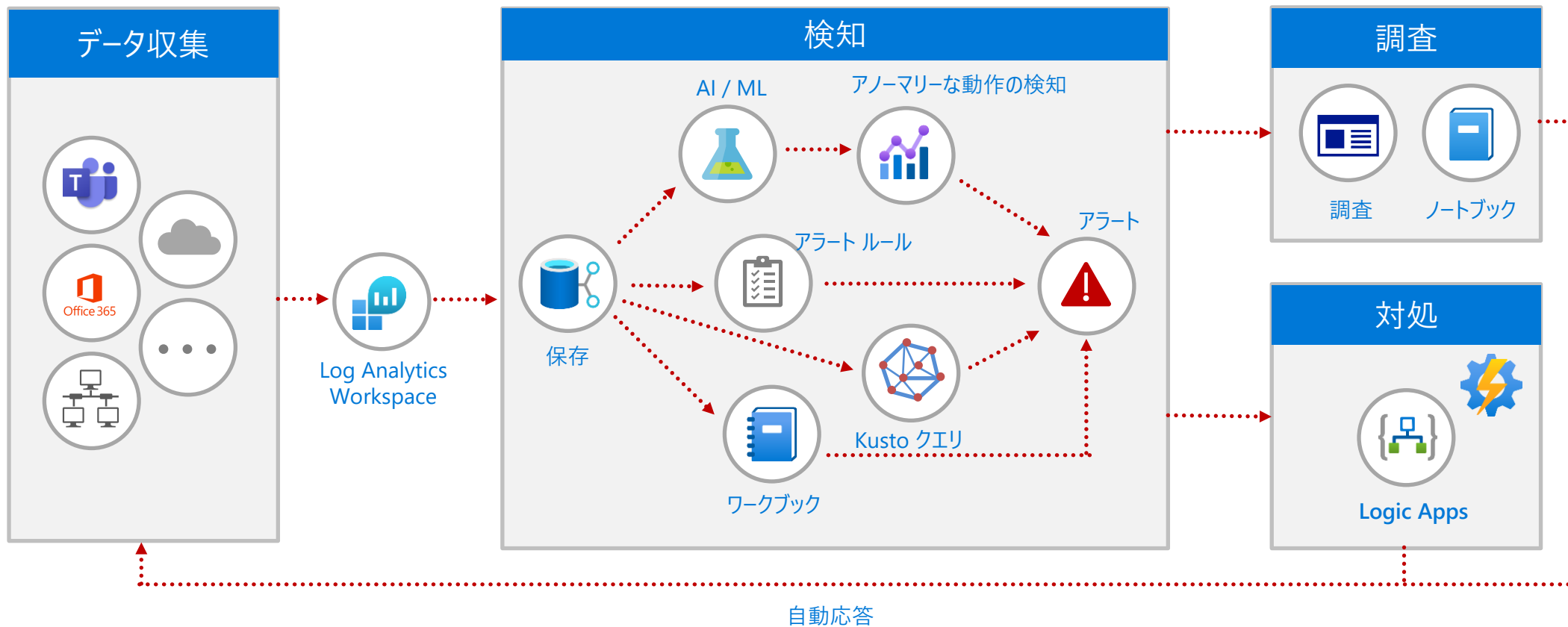
User Entity Behavior Analytics



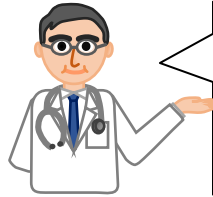
Microsoft Sentinel によるセキュリティ運用



Microsoft Sentinel を利用したセキュリティ運用を行う場合、データの収集、検知、調査、対処の4つのフェーズでの作業が発生します。ここからはそれぞれのフェーズで提供するサービスを確認します。

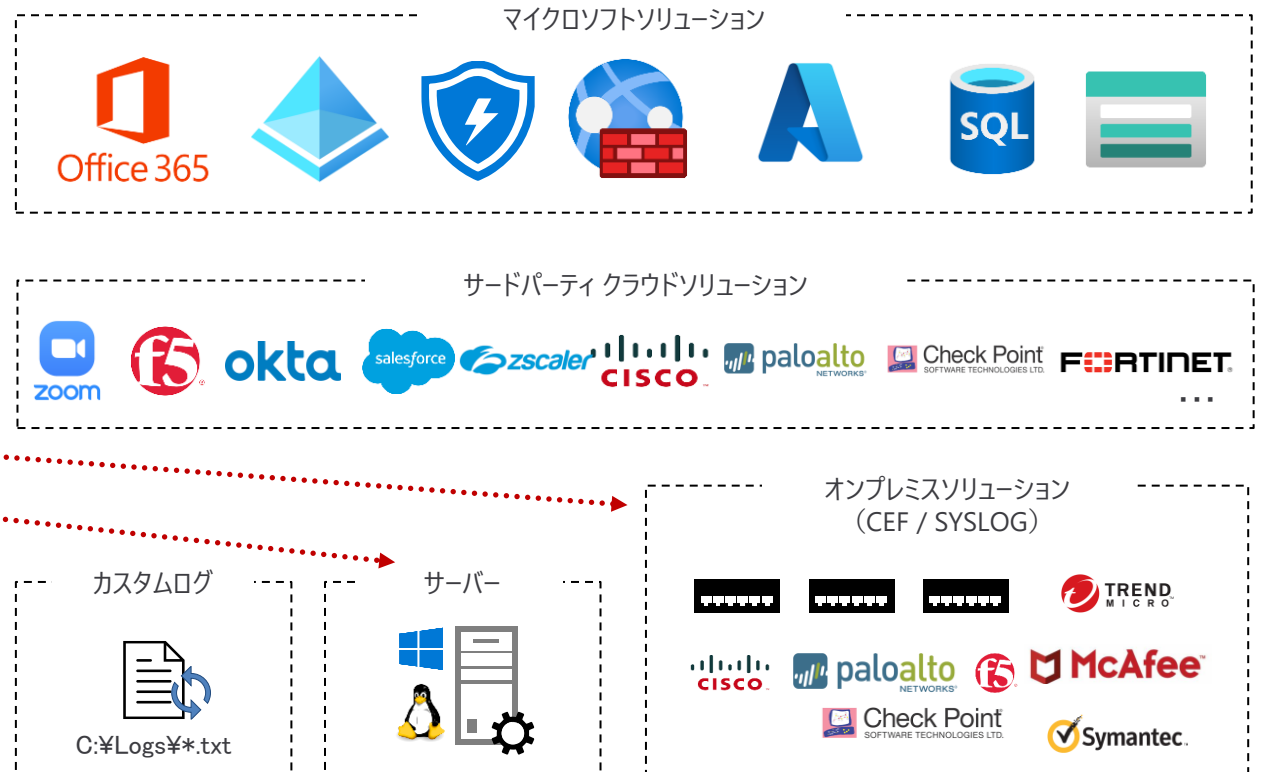


Microsoft Sentinel によるデータの収集



データ コネクタを利用して様々なクラウドサービス、オンプレミスのサーバー、ネットワーク機器に簡単に接続し、ログを収集開始できます。

Microsoft Sentinel データ コネクタ



※ SIEM とはネットワーク機器やサーバーなどの様々なソースからセキュリティ情報を収集し、横断的に分析する統合ログ管理サービスです

収集したデータの活用



データ コネクタを利用して収集したデータは単純に Log Analytics ワークスペースに保存されるだけでなく、一元管理、可視化、検索等に活用できます。

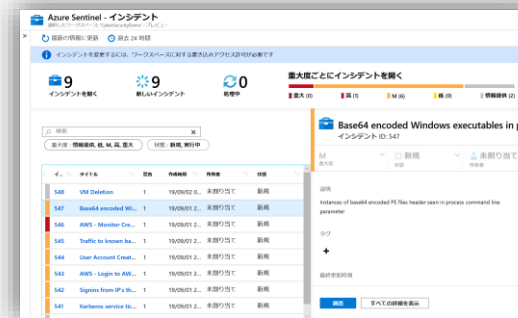


Microsoft Sentinel
データ コネクタ

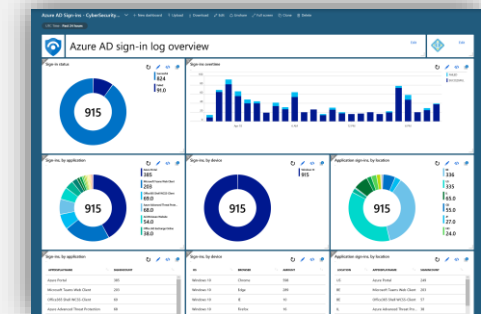


Log Analytics
Workspace

イベントの一元的な管理



ダッシュボードによる可視化



最長2年間の保存

データ保有期間

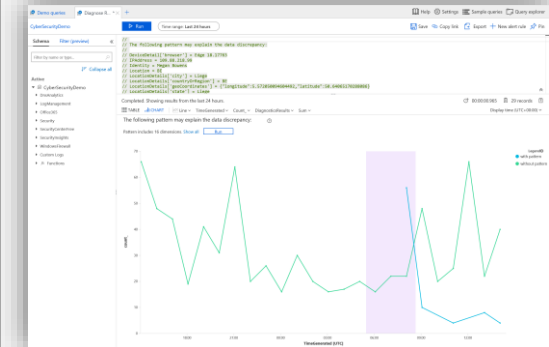
お客様の料金プランには、31日間の保有期間が含まれます。保有期間をもっと長くするには、追加料金がかかります。

データの保存期間 (日)

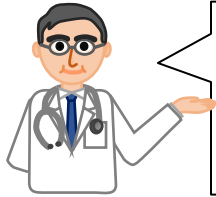


OK

必要なデータの検索



インシデント/アラート



収集したログはアラート ルール、各種機械学習 (ML) モデル、Kusto クエリなどの脅威検知の手法を利用してアラートを出力します

ホーム > Microsoft Sentinel

Microsoft Sentinel | インシデント

選択したワークスペース: 'sophia-azuresentinel'

検索 (Ctrl+/) << 最新の情報に更新 過去 30 日間 操作 セキュリティ効率ブック 列 ガイドとフィードバック

全般

- 概要
- ログ
- News & guides
- 検索 (プレビュー)

脅威管理

- インシデント
- ブック
- ハンティング
- ノートブック
- エンティティの動作
- 脅威インテリジェンス
- MITRE

5 インシデントを開く

5 新しいインシデント

0 アクティブなインシデント

重大度ごとにインシデントを開く

■ 高 (0) ■ 中 (0) ■ 低 (3) ■ 情報提供 (2)

ID, タイトル, タグ, 所有者 または 製品 で検索

重大度: すべて 状態: 2 件選択済み 製品名: すべて 所有者: すべて

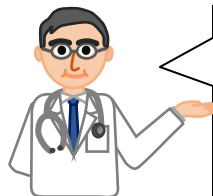
自動更新: インシデント

<input type="checkbox"/> 重大度 ↑↓	インシデント ID ↑↓	タイトル ↑↓	警告	製品名	作成時刻 ↑↓	最終更新時間 ↑↓
<input type="checkbox"/> 情報提供	302	Multi-stage incident on multiple endpoints	81	Microsoft 365 Defe...	21/10/28 19:17	22/03/29 17:51
<input type="checkbox"/> 低	331	外部共有ファイルの失効 involving one user	5	Microsoft 365 Defe...	22/03/21 18:45	22/03/21 19:00
<input type="checkbox"/> 低	329	外部共有ファイルの失効 involving one user	5	Microsoft 365 Defe...	22/03/21 05:02	22/03/21 17:25
<input type="checkbox"/> 情報提供	330	Device tried to access a phishing site on one ...	1	Microsoft 365 Defe...	22/03/21 13:11	22/03/21 13:11
<input type="checkbox"/> 低	325	外部共有ファイルの失効 involving one user	1	Microsoft 365 Defe...	22/03/01 09:37	22/03/01 09:37

Security Orchestration Automation Response

調査

対処



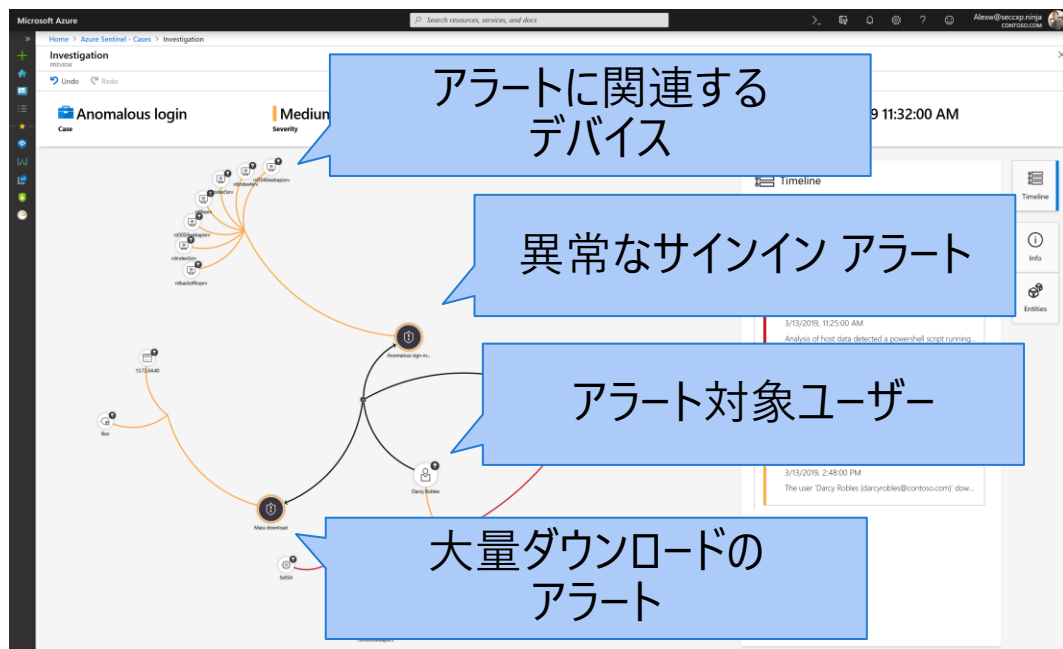
アラートが出力されたら調査を開始します。調査では SOAR としての特徴である、セキュリティ情報間での連携 (Security Orchestration) を行い、調査結果に基づくインシデント対応の自動化 (Automation) を行い、さらに自動的に調査と対処 (Response) を行います。

脅威の可視化

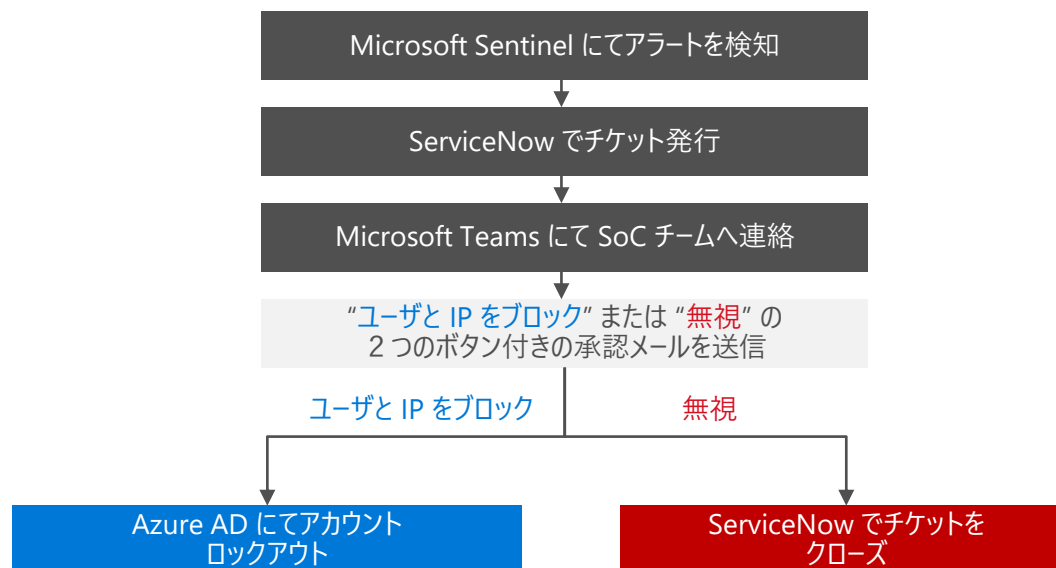
アラートの
相関分析
インシデント
マッピング

インシデントの
優先順位

対処



プレイブックによる対処の例

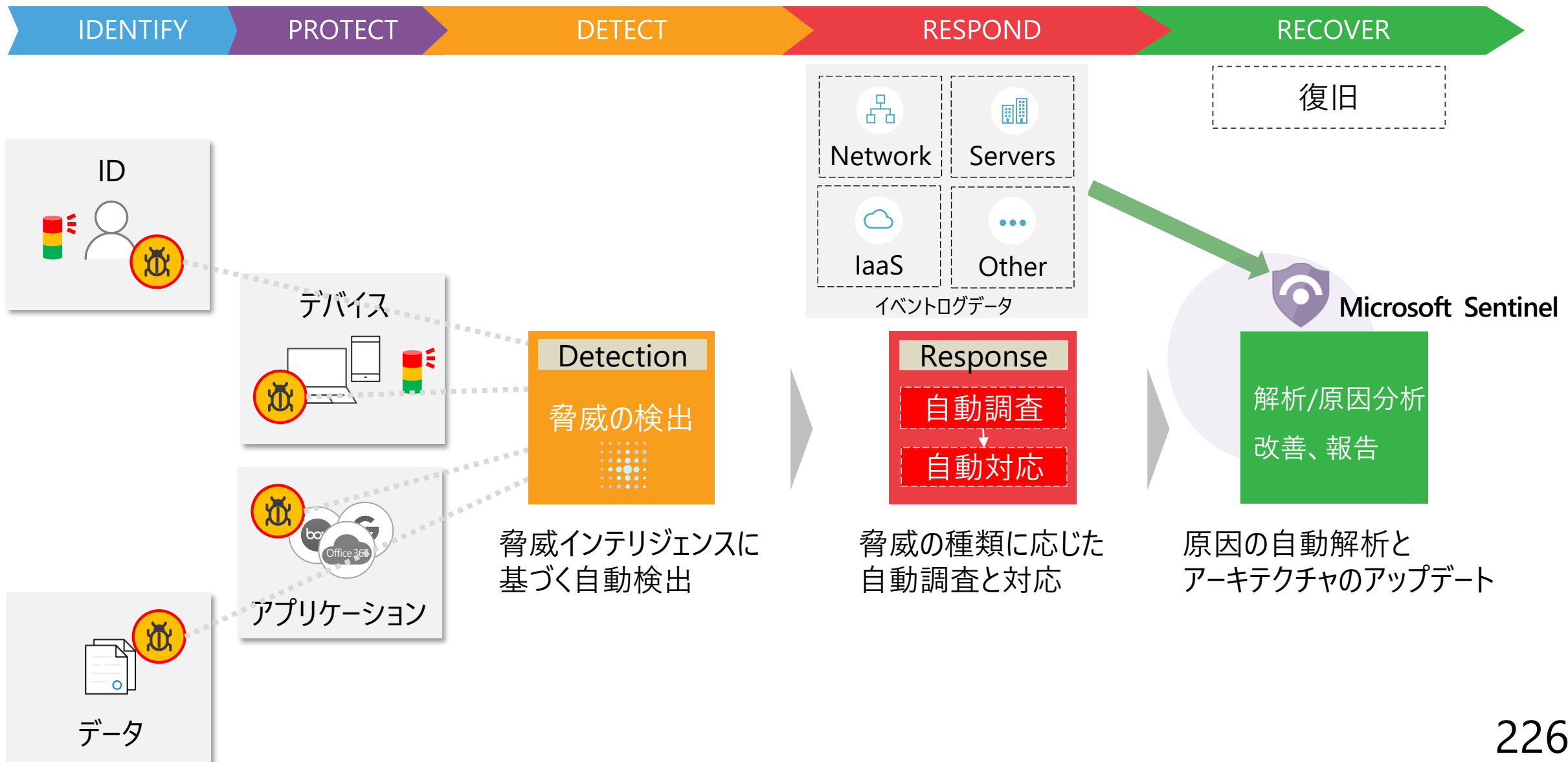


User Entity Behavior Analytics

アラートに基づく調査の段階ではさまざまな調査をおこなうことができますが、その手法のひとつにユーザーをキーにした分析 (UEBA) が利用できます。組織内で最もリスクの高いユーザーとその潜在的な影響を特定することで、インシデントの解析や原因の特定につなげることができます。



Microsoft Sentinel を利用してインシデントの解析を実施



Cyber Security Framework とマイクロソフトのアプローチ

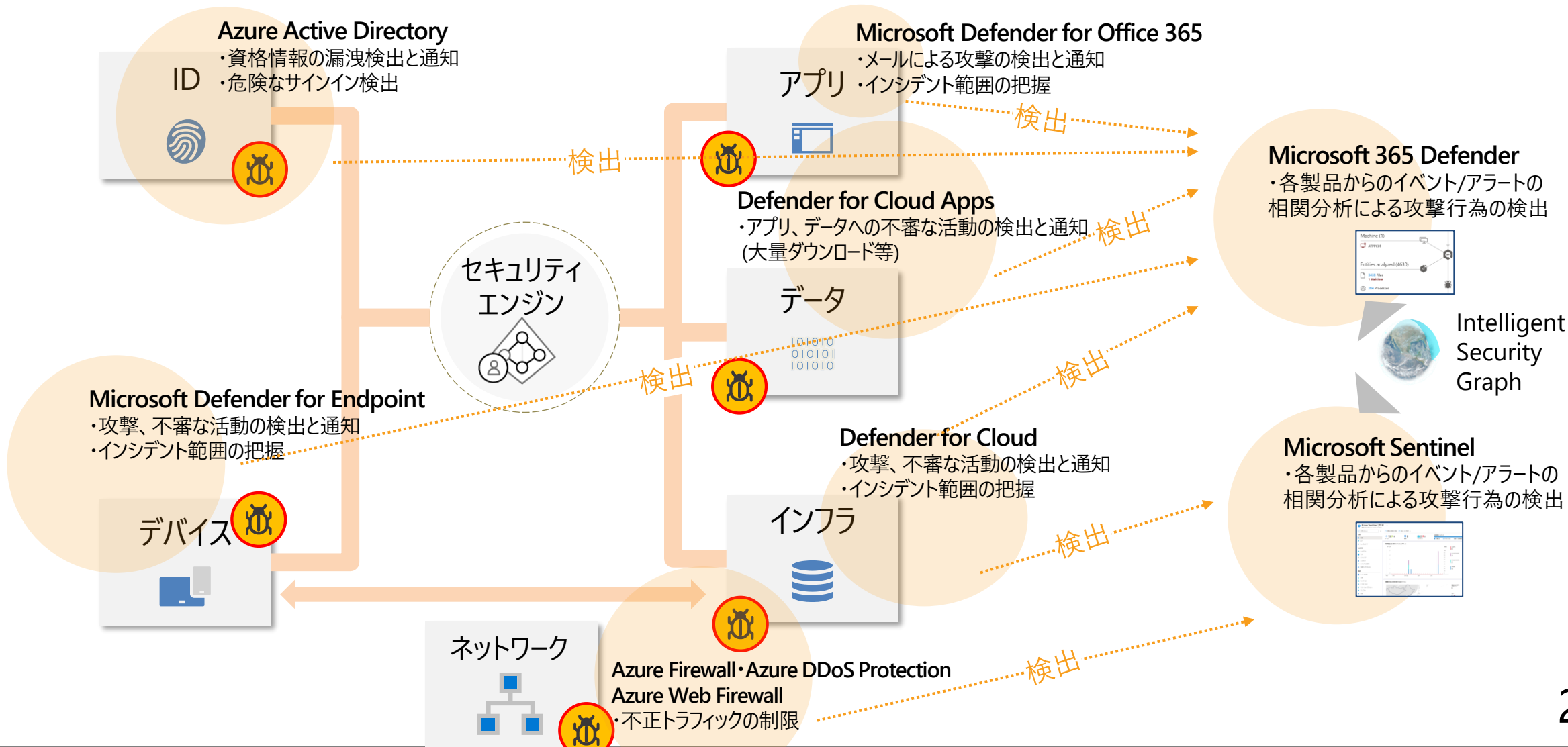
IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER



Cyber Security Framework とマイクロソフトのアプローチ

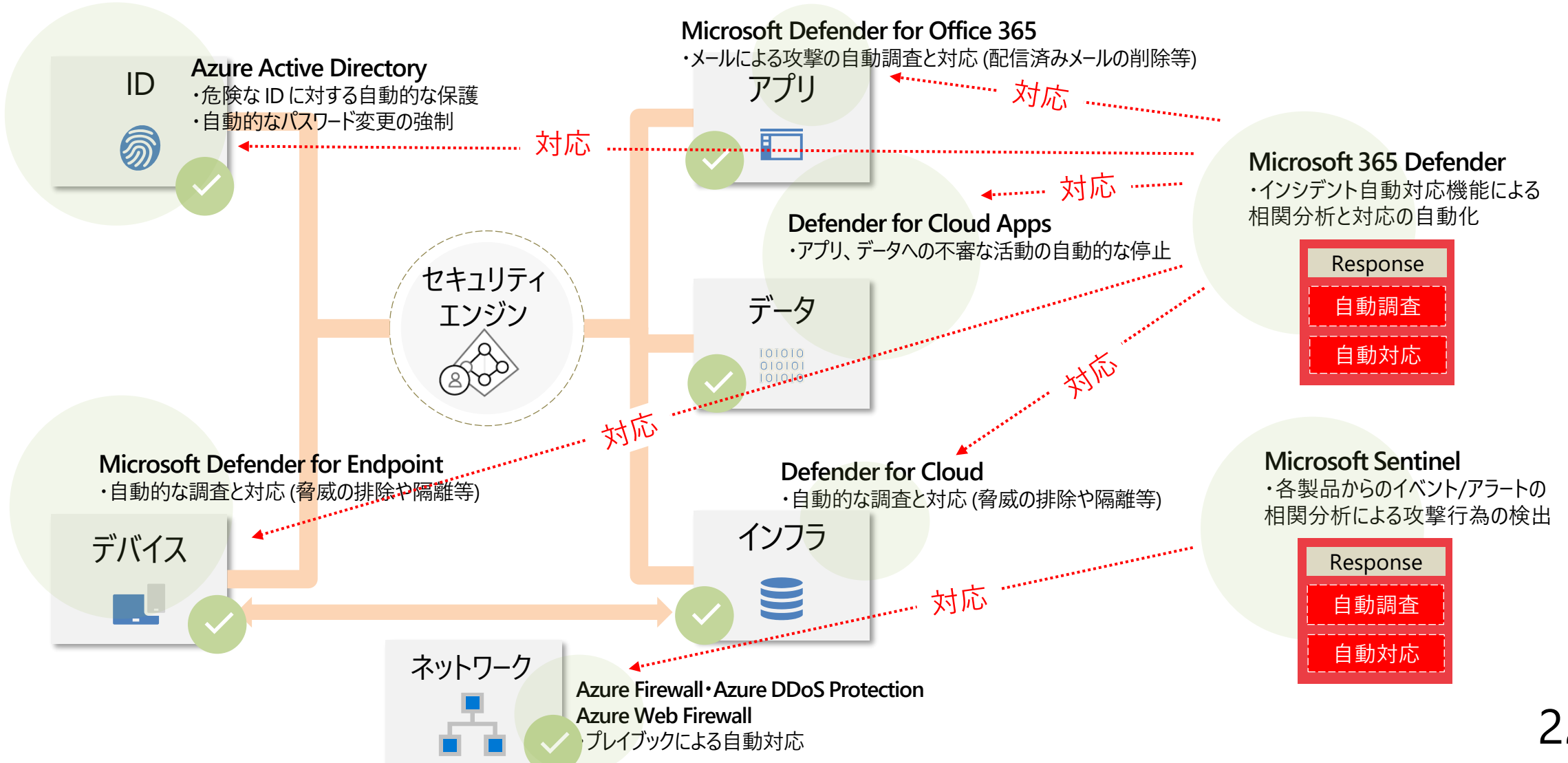
IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER



Cyber Security Framework とマイクロソフトのアプローチ

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

ID

Azure Active Directory
・セキュリティレベルのスコアリング
・ID 保護ポリシーの見直し



Defender for Cloud Apps

・アプリの保護ポリシー見直し
・データの保護ポリシー見直し

アプリ



セキュリティ
エンジン



Microsoft Purview Information Protection

・ラベルポリシーの見直し

データ



Network

Servers

IaaS

Other

イベントログデータ

Microsoft 365 Defender

・ログの連携

Microsoft Sentinel

解析/原因分析
改善、報告

Microsoft Defender for Endpoint

・フォレンジック情報の提供
・セキュリティレベルのスコアリング

デバイス



Defender for Cloud

・ポリシーの見直し
・セキュリティレベルのスコアリング
・フォレンジック情報の提供
・セキュリティレベルのスコアリング



Microsoft Endpoint Management

・デバイス / アプリ管理ポリシーの見直し

ネットワーク

Azure Firewall・Azure DDoS Protection

Azure Web Firewall

・ルール・ポリシーの見直し



アップデート

セキュリティ
アーキテクチャ

コンプライアンス
マネジメント

Modern SOC の活用編のまとめ

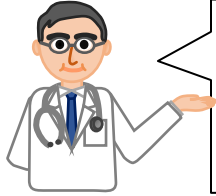
SOC チームの負荷増大

Microsoft 365 Defender の各サービスを実装し、
Modern SOC 化を実現 

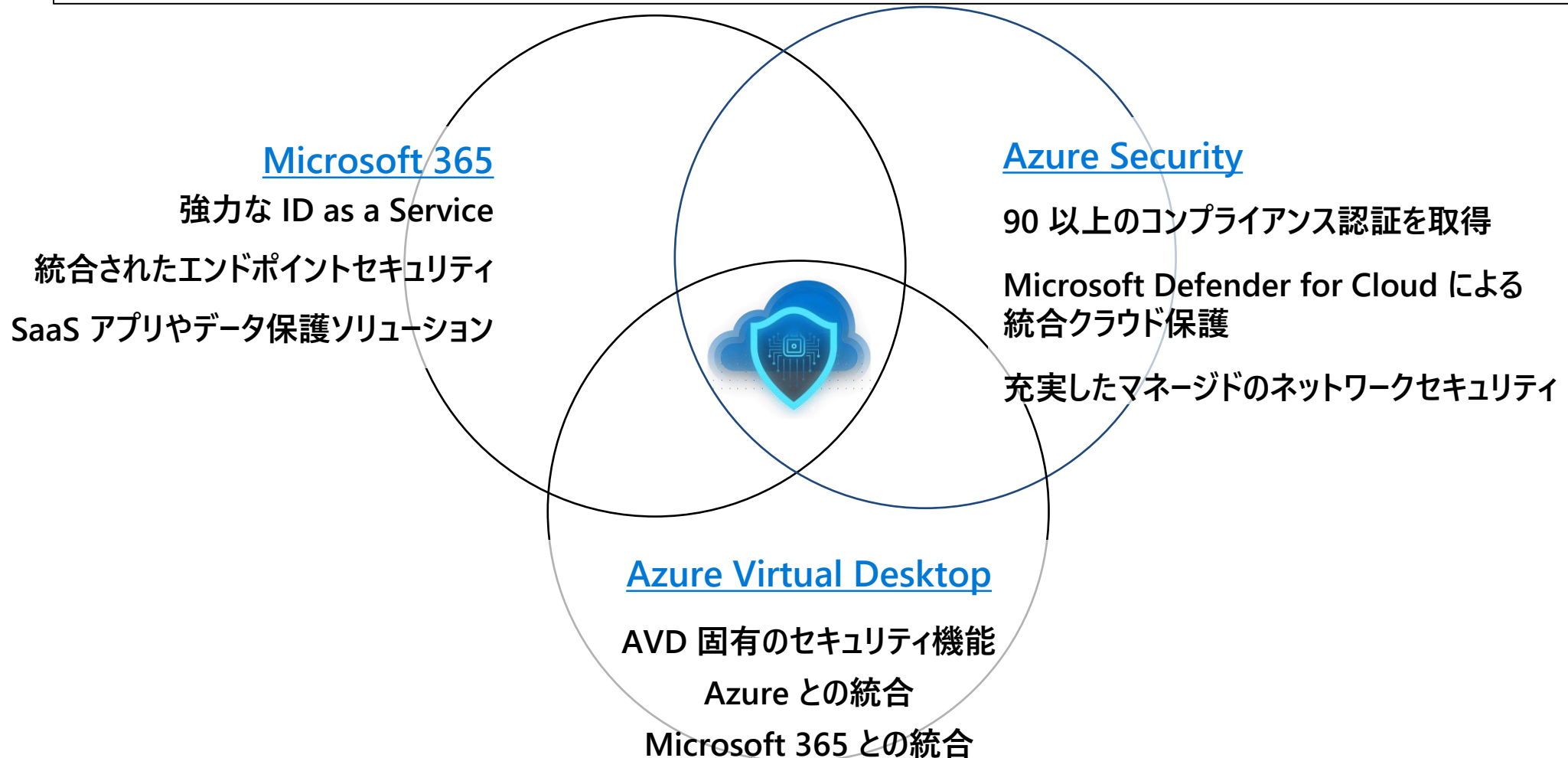
各サービスで個別に生成される
ログ/アラートの管理

Microsoft Sentinel にログを集約し、
一元的な管理体制を実現 

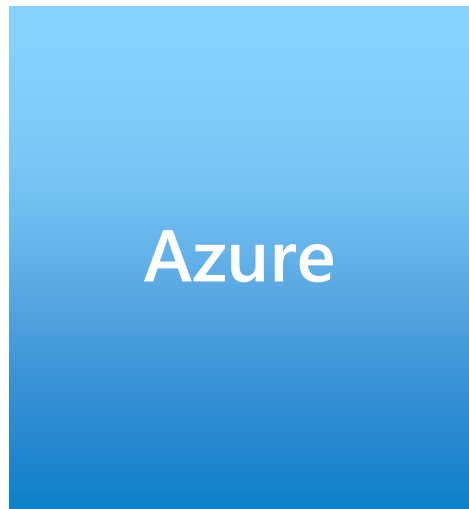
Azure Virtual Desktop × セキュリティ



Azure Virtual Desktop (AVD) のようなサービスは Microsoft 365 と Microsoft Azure の双方からのアプローチによるセキュリティ対策の必要性を理解しやすいケースと言えます。



Azure Virtual Desktop に対するゼロトラスト型アプローチ



ゼロトラスト型のアプローチ
によるセキュリティ対策



評価に必要なライセンスの取得

• Microsoft 365 E5 無料試用版の取得方法

① Office 365 E5 の無料試用版を取得
(既にグローバル管理者の Azure AD ユーザー
を保有している場合は割愛可)



<https://products.office.com/ja-jp/business/office-365-enterprise-e5-business-software>

① Microsoft 365 管理センターから 課金情報
> サービスを購入する > Microsoft 365 E5 の
順にアクセスし、無料試用版を取得

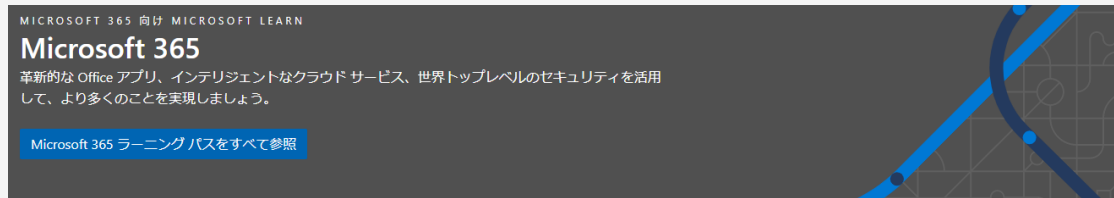


<https://admin.microsoft.com/>

動画学習リソース

- Microsoft 365 および Microsoft Defender for Cloud の概念について動画でも学習していただけます。

Microsoft Learn - Microsoft 365
<https://docs.microsoft.com/ja-jp/learn/m365/>



コミュニティ
Microsoft Tech Community
最新のニュース、製品の更新情報、ベストプラクティスについて、Microsoft の専門家や仲間とつながって議論することができます。
[コミュニティに参加する](#)

EVENTS
Virtual Training Days
これらの1日と2日の仮想イベントでは、あなたのスキルセットを広げ、Microsoft の専門家とつながる機会が提供されます。
[トレーニングイベントの参照](#)

ラーニングパス
Microsoft 365 と Teams の開発者
オンライン ラーニングパスをご覧になり、Microsoft Graph、ID、SharePoint、Office アドインなど、Microsoft 365 と Teams の開発に関するトピックの詳細をご確認ください。
[ラーニングパスを参照](#)

mstep オンライン
<https://partner.microsoft.com/ja-jp/training/mstep-productivity>

セキュリティ 関連トレーニングコース

コース名	レベル	対象	セッション
Microsoft 365 Enterpriseで実現するサイバーセキュリティ対策(2019年10月)	200	営業/技術	テキスト(2019年10月更新) 視聴する (約130分)
Azure Sentinelを利用したセキュリティ分析(2020年11月)	200	営業/技術	テキスト(2020年11月更新) 視聴する (約130分)
Microsoft 365 Enterprise セキュリティ基礎と応用 (EMS - Azure Active Directory/Microsoft Defender for Identity 編) (2021年3月)	300	技術	テキスト(2021年3月更新) 視聴する (約280分)
Microsoft 365 Enterprise セキュリティ基礎と応用 (EMS - Microsoft Intune, Azure Information Protection, Microsoft Cloud App Security) (2021年4月)	300	技術	テキスト(2021年4月更新) 視聴する (約270分)
Microsoft 365 Enterprise セキュリティ基礎と応用 (Office 365 編) (2019年2月)	300	技術	テキスト(2020年1月更新) 視聴する (約160分)
Microsoft 365 Enterprise セキュリティ基礎と応用 (Windows 10 編) (2020年7月)	300	技術	テキスト(2020年7月更新) 視聴する (約80分)
Microsoft 365 によるサイバーセキュリティ&コンプライアンス対策実践編 (2020年12月)	300	技術	テキスト(2020年12更新) 視聴する (約230分)
組織のブランドと信用を守る Microsoft 365 Compliance (2020年8月)	300	技術	テキスト(2020年8月更新) 視聴する (約330分)



© 2022 Microsoft Corporation. All rights reserved.

本情報の内容 (添付文書、リンク先などを含む) は、2022 年 3 月 25 日時点のものとあり、予告なく変更される場合があります。

本コンテンツの著作権、および本コンテンツ中に出てくる商標権、団体名、ロゴ、製品、サービスなどはそれぞれ、各権利保有者に帰属します。