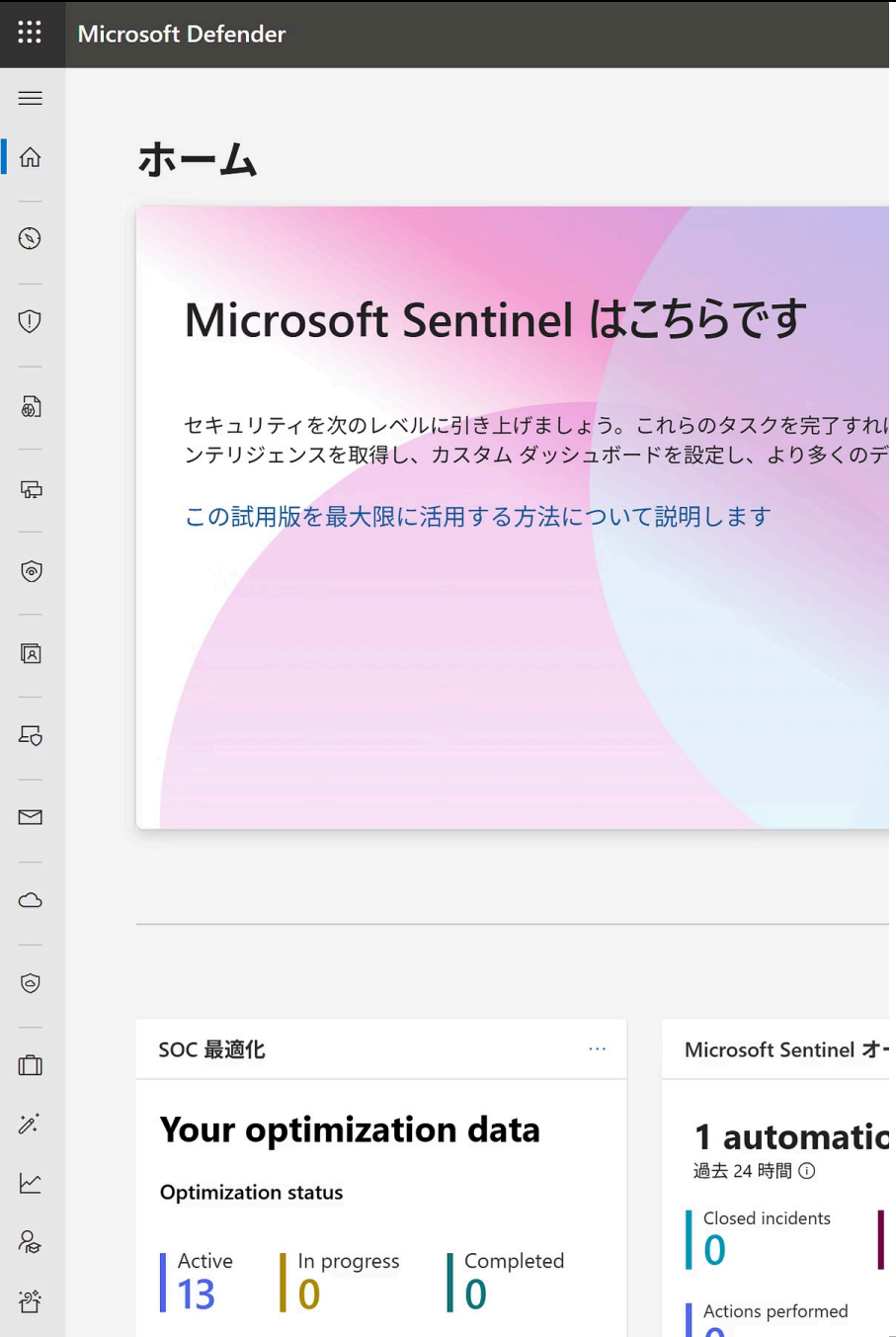


見張ってまっか？
Azure の世界をまるごと守る Sentinel 入門

銀行CSIRTで学んだ"攻撃の初動"をクラウドで自動化する

～Microsoft Sentinel × SOAR × Microsoft Security Copilot～

自己紹介

高瀬みこと

Azure PaaSインフラ構築 / 銀行CSIRT / エンドポイント管理のSIer（IntuneなどM365周り）

CSIRT

内部で発生したインシデント対応
配属チームはほんまにエンジニアかなってくらい定時上がり

今日のゴール

「攻撃の初動 → 自動防御」の仕組みを理解し、クラウドでのセキュリティ自動化を明日から使いたくなる

CSIRTとは？

Computer Security Incident Response Team

企業を攻撃から守る"セキュリティ専門部隊"です。サイバー攻撃が発生した際、迅速に対応し、被害を最小限に抑える役割を担っています。

CSIRTの主な役割

不審ログの監視

24時間365日、システムログを監視し、異常な振る舞いを検知します。

インシデント初動対応

攻撃を検知した瞬間、迅速に初動対応を開始し、被害拡大を防ぎます。

端末隔離・アカウント停止

感染端末やアカウントを即座に隔離し、ネットワークへの影響を遮断します。

攻撃経路調査

攻撃者がどこから侵入し、何を狙ったのかを詳細に分析します。

事後対策の提案

同様の攻撃を防ぐため、システム改善や運用ルールの見直しを提案します。

従業員30,000人規模のCSIRT運用は"ログとの戦い"

① ログ量は"人の許容量"を大きく超える

- 3万人規模 → 端末が3万台
- 毎日発生するログ：数千万〜億レベル
- 1つの不審動作を、人が手作業で探すのは現実的ではない

②"見落とし"が即インシデントにつながる世界

- 攻撃者は深夜・休日も関係なく動く
- 不審な通信やスキャンは数秒〜数分で次の攻撃フェーズへ移行
- 1つのログを見逃すと、横展開 → 社内ラテラルムーブ → データ盗難まで一気に進む危険性

③ CSIRTだけで対応しきれない理由

- ログ量増大に比例して担当者は増やせない
- 手動だと「通知 → 調査 → 判断 → 対応」ひとつひとつに時間がかかる
- 早期発見・早期隔離が必須だが、人の速度では追いつかない

なぜ自動化が必要なのか

手動対応だと遅い

気づいてから対応するまでに数分〜数時間。その間に攻撃は進行します。

誤検知対応で疲弊

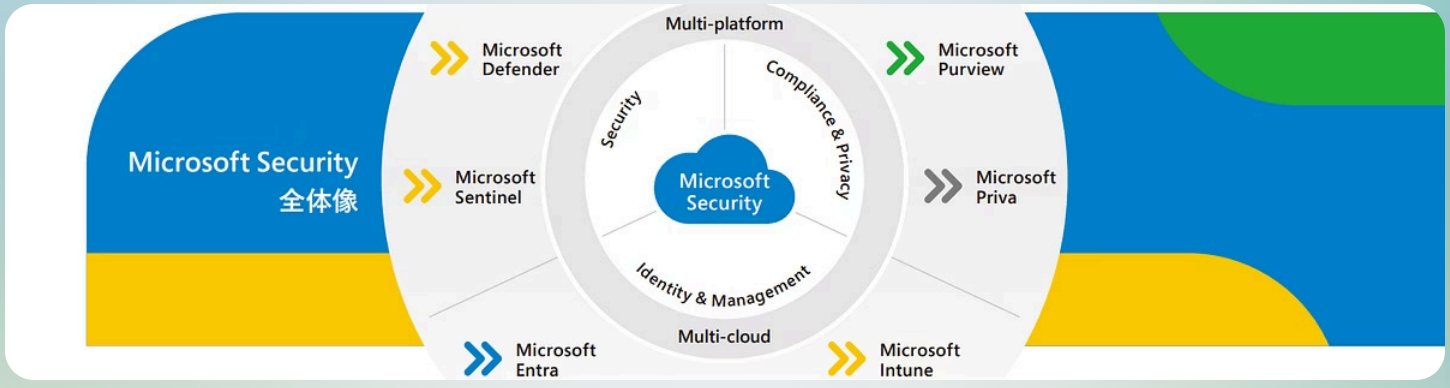
大量のアラートの中から真の脅威を見つけるのは困難です。※上がるアラートのほとんどすべてが誤検知

攻撃は24時間止まらない

攻撃者に休日はありません。常時監視と即座の対応が必要です。

"気づく"と"防ぐ"のスピード

検知から対応までの時間を秒単位に短縮することが重要です。



Microsoft Securityの全体像

ID & アクセス管理

- Microsoft Entra ID: クラウドベースのID・アクセス管理。多要素認証、条件付きアクセス、パスワードレス認証を提供
- Entra ID Protection: 侵害されたアカウントをAIで検出・対応
- Permissions Management: マルチクラウドの権限管理を一元化

エンドポイント保護

- Microsoft Defender for Endpoint: ランサムウェアやマルウェアからデバイスを保護。Windows/Mac/Linux/モバイル対応
- Microsoft Intune: デバイス管理(MDM)とアプリ管理(MAM)。BYOD対応
- Defender Vulnerability Management: 脆弱性を検出し優先順位付けして修復

メール・アプリ・クラウド防御

- Defender for Office 365: フィッシング、マルウェア添付ファイル、悪意あるリンクから保護
- Defender for Cloud Apps: SaaSアプリの可視化・制御。シャドウIT検出とセッション制御

クラウドインフラ保護

- Defender for Cloud: Azure/AWS/GCPのセキュリティ態勢管理(CSPM)とワークロード保護(CWPP)

データ保護・コンプライアンス

- Microsoft Purview: 情報保護、DLP、データ分類、eDiscovery、コンプライアンス管理を統合
- Microsoft Priva: プライバシーリスク管理とデータ主体権利要求(DSAR)対応

セキュリティ運用(SecOps)

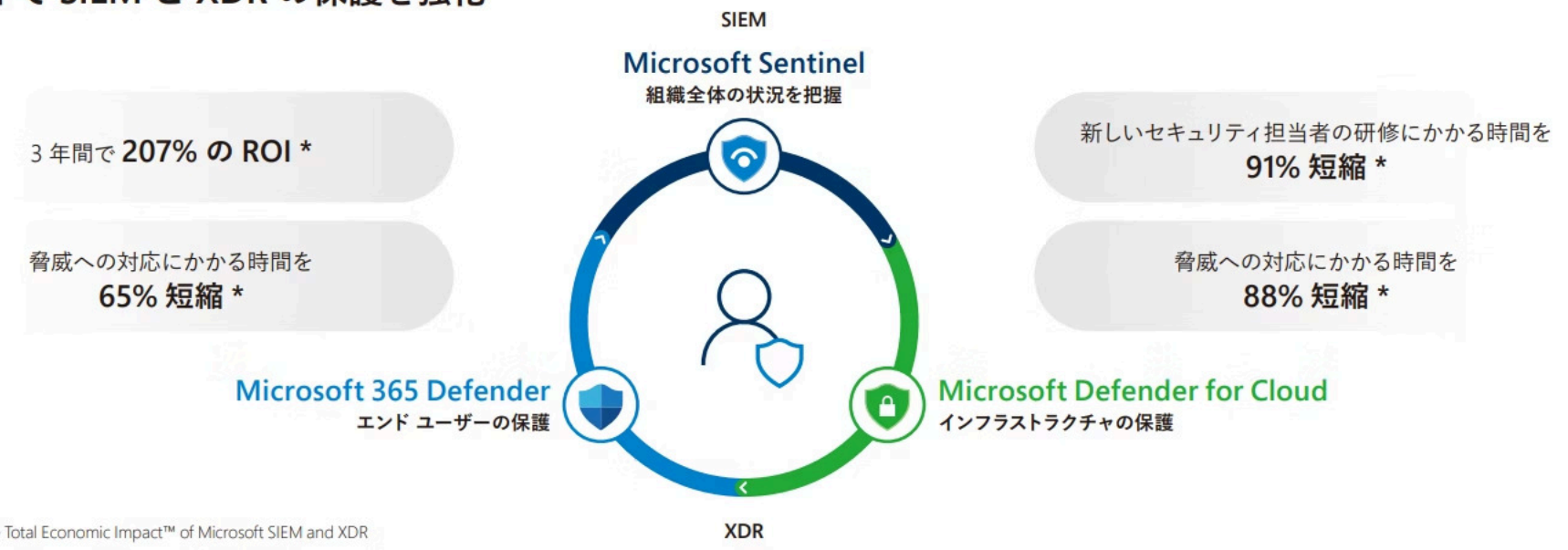
- Microsoft Sentinel: クラウドネイティブSIEM + SOAR。AI活用で脅威検出・自動対応
- Copilot for Security: AIアシスタントがインシデント分析と対応を支援

Microsoftのドキュメントより引用

クラウドと AI を活用した次世代型セキュリティ運用

Microsoft Sentinel は、スケーラブルでクラウド ネイティブのソリューションで、セキュリティ情報とイベント管理 (SIEM) とセキュリティ オーケストレーション、オートメーション、応答 (SOAR) によって、インテリジェントなセキュリティ分析と脅威インテリジェンスを組織全体に提供します。

低コストで SIEM と XDR の保護を強化



* The Total Economic Impact™ of Microsoft SIEM and XDR

Microsoft Sentinelとは

クラウドネイティブな統合セキュリティ基盤

Microsoft Sentinelは、SIEM（セキュリティ情報イベント管理）、SOAR（セキュリティオーケストレーション自動対応）、インシデント管理を統合したクラウドネイティブなセキュリティプラットフォームです。

SIEM機能

ログ収集・統合・分析

SOAR機能

自動対応・オーケストレーション

統合管理

インシデント一元管理

SIEMの役割

ログ収集・統合

Azure、オンプレミス、他社クラウドなど、あらゆる環境からログを一元収集します。

不審動作の検知

機械学習とルールベースで、通常と異なる振る舞いを自動検知します。

横断分析

コマンド実行、ログオン失敗など、複数の兆候を関連付けて分析します。

SOARの役割

SOAR（Security Orchestration, Automation and Response）は、人の代わりに"即行動"してくれる自動対応の仕組みです。

01

アラート受信

SIEMから不審な動作の通知を自動で受け取ります。

02

条件判定

事前に定義したルールに基づいて、対応の要否を自動判断します。

03

自動対応

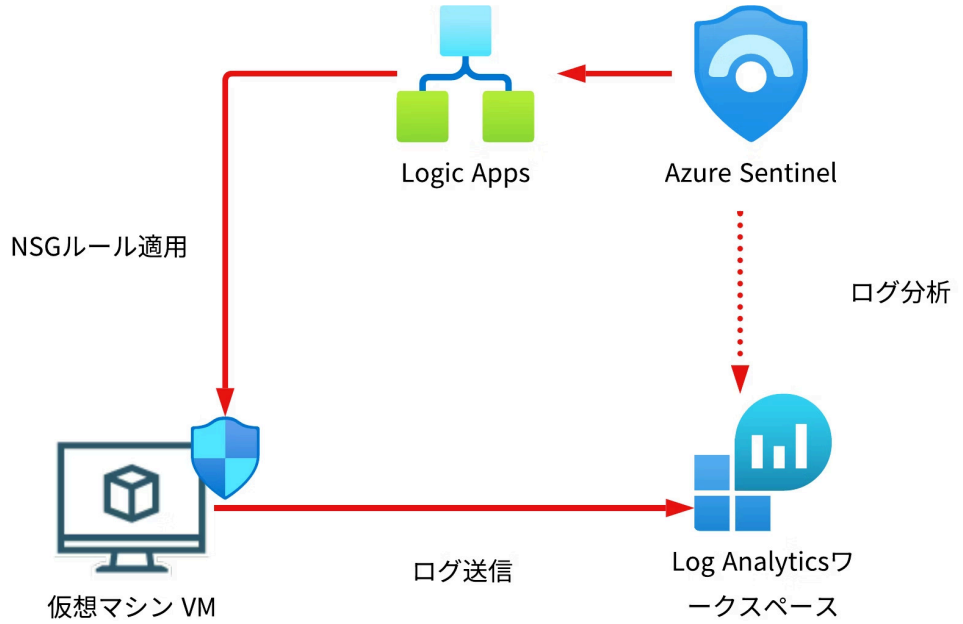
通知送信、アカウントブロック、端末隔離などを自動実行します。

今回の実践シナリオ

curl 実行 → Sentinel が検知 → 自動で NSG を書き換え → VM隔離

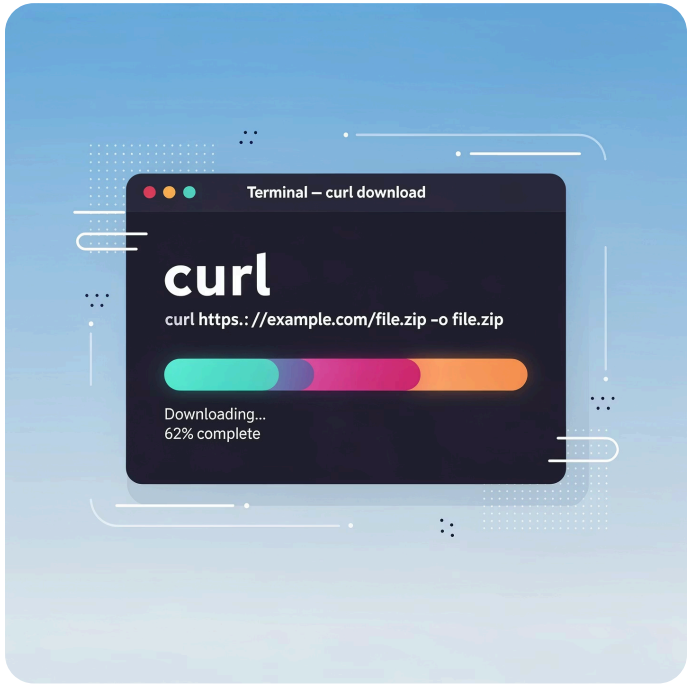
> ある日、Azure VM 上で誰かが curl コマンドを実行しました。外部の不審なサイトへアクセスを試みています。

このシナリオでは、Sentinelが自動的に脅威を検知し、Logic Appsを通じてNSG（ネットワークセキュリティグループ）を書き換え、VMを即座にネットワークから隔離する様子を実演します。



curl・nmapが危険とされる理由

curl の危険性



- **ペイロードのダウンロード**：攻撃者がマルウェアを外部から取得する際に使用
- **C2通信**：Command & Control サーバーとの通信に利用される
- **データ窃取**：機密情報を外部に送信する手段として悪用

nmap の危険性

- **偵察活動**：攻撃者が標的ネットワークの構成を調査
- **脆弱性探索**：開いているポートやサービスを特定
- **攻撃準備**：本格的な侵入の前段階として必ず実行される

重要：これらのコマンドが勝手に実行されることは、攻撃の初動サインです。早期検知と即座の対応が被害を最小化します。

実践フロー全体図

curl実行

VM上で不審なコマンドが実行される

Log Analytics

プロセス実行ログが送信される

Sentinel検知

Analytics Ruleで異常を検知しインシデントを作成

Playbook実行

Automation Rule経由でLogic Apps起動

NSG更新

アウトバウンド拒否ルール自動追加

VM隔離完了

外部通信が遮断される

デモ① – VM で curl 実行

実行内容

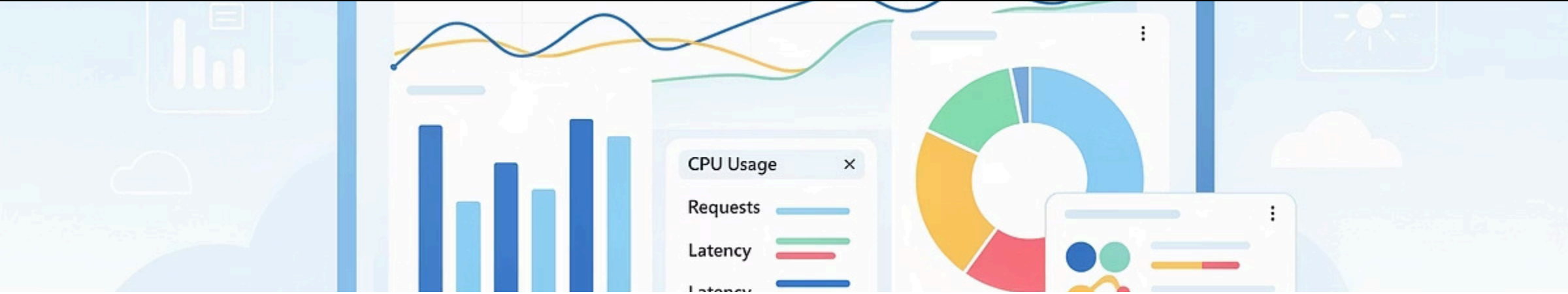
```
curl google.com
```

Azure VM上で、外部の不審なURLに対してcurlコマンドを実行します。
通常の業務では使用されないコマンドです。

※curlコマンドは開発チームで業務利用することもあるので、実際の運用では考慮が必要

本環境では、Symonを利用してcmd上の「curl」実行を監視しています。

※本当はMDEでしたい

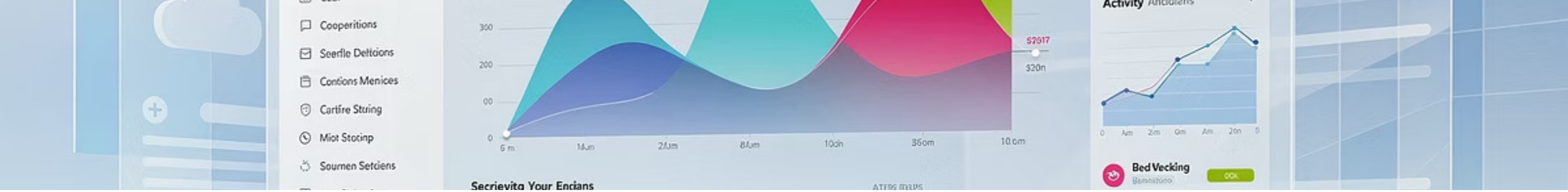


デモ② – Log Analytics でログ確認

プロセス生成ログが大体1分〜10分ほどでLog Analytics ワークスペースに届きます。KQLクエリで確認できます。

```
Event
| where Computer == "vm-test-sukiyan"
| where ParameterXml has "curl"
```

このクエリ結果により、curlコマンドの実行履歴、実行ユーザー、実行時刻が明確に確認できます。



デモ③ – Sentinel アラート→インシデント

分析ルール

事前に定義したルールがログを監視

1

条件一致

curlコマンド検知でアラート生成

2

インシデント作成

自動的にインシデント管理画面に表示

3

※分析ルールがログを分析する頻度の設定が可能です。検知したい内容に合わせて頻度の設計をしてください。
　分析ルールの詳細については以下参照
https://learn.microsoft.com/ja-jp/azure/sentinel/threat-detection

Sentinelのインシデント画面には、重要度、影響範囲、関連エンティティが自動的に整理されて表示されます。

デモ④ – Playbook 動作（Logic Apps）

Automation Ruleにより、Playbook（Logic Apps）が自動的にトリガーされます。

トリガー受信

Sentinelからインシデント情報を受け取る

情報抽出

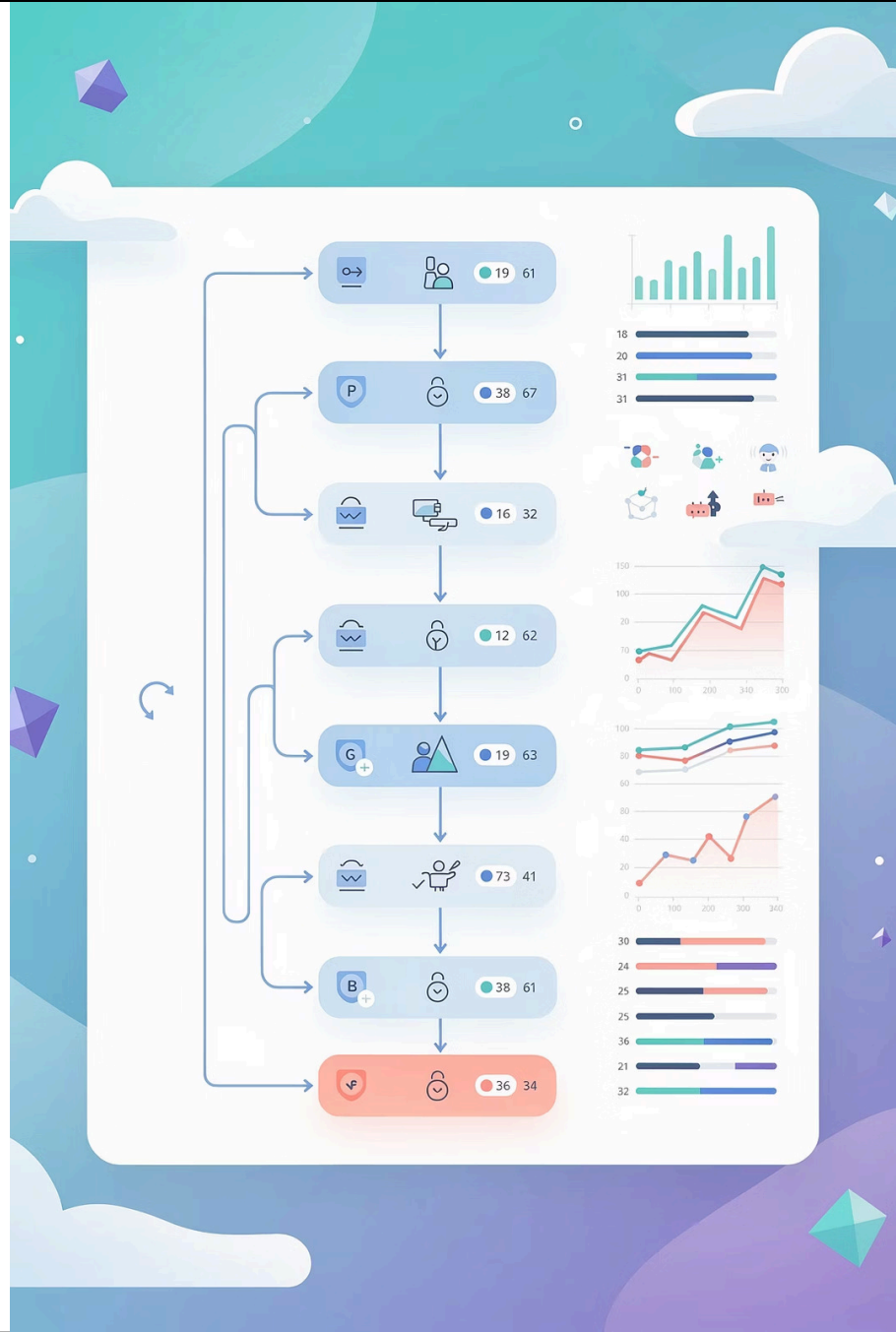
VMのリソースID、IPアドレスを特定

NSG更新実行

Azure APIを呼び出してルール追加

Logic AppsのRun historyで、各ステップの実行状況と結果をリアルタイムで確認できます。

SentinelでのPlaybook実行方法詳細については以下を参照
https://learn.microsoft.com/ja-jp/azure/sentinel/automation/run-playbooks?tabs=after-onboarding%2Cincidents%2Cazure%2Cincident-details-new



デモ⑤ – NSG 自動更新（Before / After）

Before：通常状態

名前でフィルター処理

ポート == すべて　プロトコル == すべて　ソース == すべて　宛先 == すべて　アクション == すべて

優先度	名前	ポート	プロトコル	ソース	宛先
受信セキュリティ規則					
300	⚠ RDP	3389	TCP	任意	任意
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBal…	任意	任意	AzureLoadBalancer	任意
65500	DenyAllInBound	任意	任意	任意	任意
送信セキュリティ規則					
65000	AllowVnetOutBound	任意	任意	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBo…	任意	任意	任意	Internet
65500	DenyAllOutBound	任意	任意	任意	任意

- アウトバウンド通信は許可
- インターネットへの接続が可能

After：自動隔離

名前でフィルター処理

ポート == すべて　プロトコル == すべて　ソース == すべて　宛先 == すべて　アクション == すべて

優先度	名前	ポート	プロトコル	ソース	宛先
受信セキュリティ規則					
300	⚠ RDP	3389	TCP	任意	任意
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBal…	任意	任意	AzureLoadBalancer	任意
65500	DenyAllInBound	任意	任意	任意	任意
送信セキュリティ規則					
500	deny-all-outbound	任意	任意	任意	任意
65000	AllowVnetOutBound	任意	任意	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBo…	任意	任意	任意	Internet
65500	DenyAllOutBound	任意	任意	任意	任意

- **新規ルール自動追加**
- 優先度500で全アウトバウンド拒否　※RDPできなくなるので送信のみ
- VMがネットワークから隔離

検知から隔離完了まで約300秒。攻撃者が次の行動を取る前に自動防御が完了します。

運用チームの課題とSecurity Copilotの必要性

セキュリティアラートの詳細調査は、特に運用チームに新しく加わったメンバーにとって大きな壁となります。

適切なログの特定に難航

膨大なログの中から、アラートに関連する適切な情報を見つけ出すのは至難の業です。経験の浅いメンバーは特に時間がかかります。

KQL作成のハードルが高い

複雑なKQLクエリを作成するには専門知識が必要で、
迅速な調査のためにクエリを組むのは容易ではありません。

これらの課題を解決し、迅速かつ効率的なインシデント対応を実現するために、Security Copilotが欲しかった。
※個人の感想です

Microsoft Security Copilot とは？

セキュリティ特化 AI アシスタント

Copilot for Securityは、Sentinel、Defender、各種ログを横断的に理解し、セキュリティアナリストの作業を支援する生成AIです。

自然言語で質問

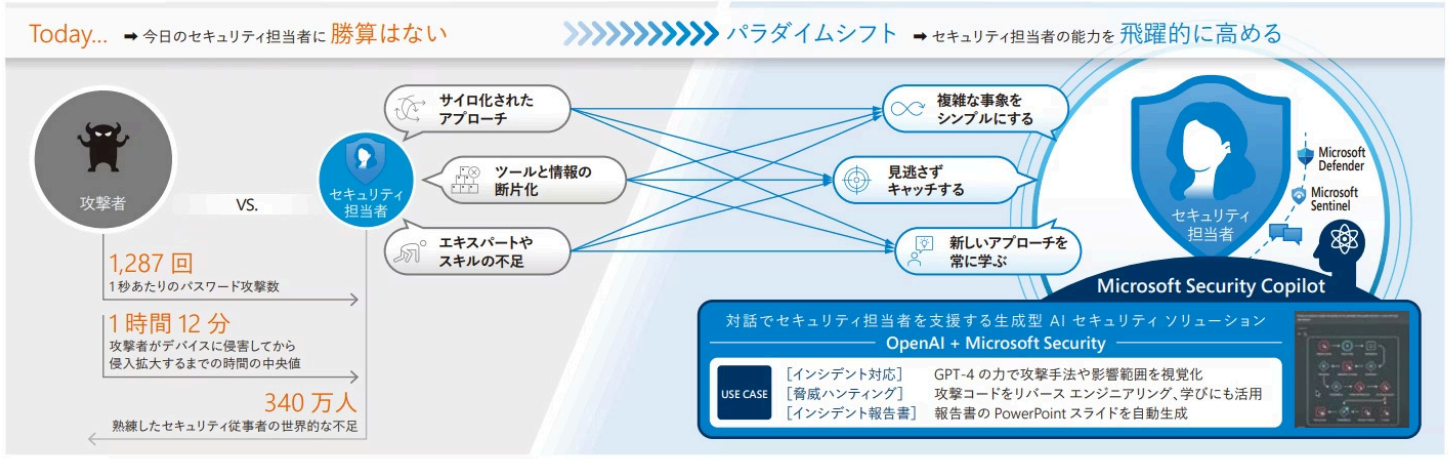
「このIPアドレスは危険ですか？」と聞くだけ

インシデント分析

攻撃の流れを自動で整理・要約

対応支援

推奨アクションを具体的に提示



Copilot for Security で"できること"一覧

～セキュリティ業務をAIが強力サポート～

1. インシデント調査の要約・可視化

- 大量ログを読みやすく"要点"にしてくれる
- 不審な動きの流れ(攻撃チェーン)を整理
- 「このアラートはなに?」「何が起きたの?」に即答

2. 不審スクリプト・コマンドの解析

- PowerShell、curl、nmap、マルウェアっぽいコードの目的とリスクを説明
- 初見のスクリプトでも「危険かどうか」を判断しやすくなる

3. KQLクエリの自動生成・改善

- 自然言語から検索クエリを作成
- 調査したい内容を言うだけで、それに必要なKQLを提案
- クエリ作成の敷居が大幅に低下

4. 推奨アクションの案内

- どのアラートを優先すべき?
- 次に何をすればいい?
- 自動で対応案・判断軸を出してくれる

5. マルチ製品の横断調査

- Defender、Sentinel、Entra ID、Intune、Purviewのログ・アラートを横断して状況をまとめる
- 人間では難しい"製品間のつながり"をAIが整理

6. レポート作成・説明資料の生成

- インシデント報告書、対応まとめ、改善案を自然言語で自動生成

7. 一般的な脅威情報の照合

- AIのセキュリティ知識 + Microsoft Threat Intelligence
- 脅威の背景や攻撃者の手口も説明

Copilot for Security のメリット / デメリット

～AIを使ううえで知っておくべきこと～

メリット(利点)

- **分析スピードが圧倒的に早い**
  - 人が10～30分かける調査を数秒で整理
  - 初動対応のスピードUpにつながる
- **初心者でも"強い分析"ができる**
  - 分析経験が少なくてもAIが要点・背景・次の行動を示す
  - SOC全体のスキル底上げに役立つ
- **KQL・ログ知識が浅くても調査可能**
  - 「これ調べたい」→ クエリ生成
  - 「この動作は危険?」→ 意味を説明
- **複雑なインシデントの"全体像"がわかる**
  - Defender / Sentinel / Entra などを横断して攻撃の流れ(Kill Chain)をまとめてくれる
- **報告資料の作成が爆速**
  - 対応報告書や説明文の下書きを自動生成
  - マネージャー・他部署への説明が超ラク

デメリット(注意点)

- **AIの提案なので"鵜呑み"NG**
  - 誤った解釈がゼロではない
  - 最終判断はアナリストが行う必要あり
- **データ権限設計が重要**
  - ログ閲覧・参照権限が弱いと答えが出ない
  - 組織側の準備も必要
- **すべて自動化はできない**
  - 人間の判断が必要な場面は残る
  - 完全な置き換えではなく"AI補助"が本質
- **コスト管理が必要(SCU課金)**
  - 使うほど費用が増える
  - 必要な時にだけ活用する運用が現実的
- **英語中心(改善中)**
  - 日本語でも使えるが、英語ほど精度は高くない場面がある

ご清聴
ありがとうございました

Microsoft Sentinel と Copilot for Security を活用した、次世代のセキュリティ運用を、ぜひあなたの環境でも実現してください。

今日から始められること：

Azure とE5ライセンスの無料試用版でSentinelを試してみる

見張ってまっか？