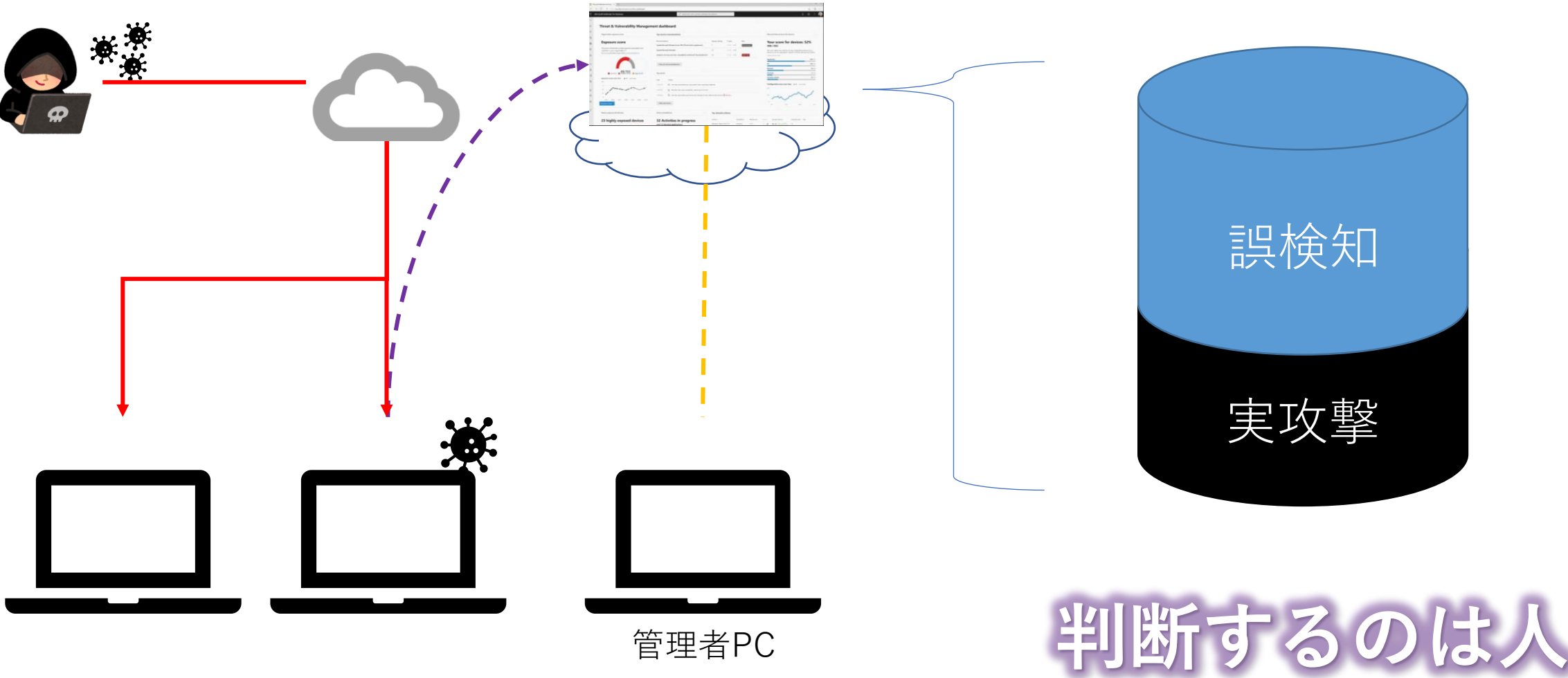


Microsoft Defender for Endpoint／Businessに監視サービスは必要か？

株式会社ソフトクリエイト
セキュリティサービス事業部

なぜEDRに運用が必要か？



なぜEDRに運用が必要か？

アラート通知メールに記載されているURLから管理画面にログインし、アラート調査します。

Low severity alert: Fancy Bear(Russia)_2201 on [redacted]

Microsoft 365 Defender <defender-noreply@microsoft.com>
宛先 [redacted] 2022/ [redacted]

このメッセージの表示に問題がある場合は、ここをクリックして Web ブラウザーで表示してください。

メッセージを日本語に翻訳する 翻訳しない: 英語 翻訳に関する設定

Microsoft 365

Fancy Bear(Russia)_2201 was detected by Microsoft Defender for Endpoint on nichikaw-n7

Alert details

Title	Fancy Bear(Russia)_2201
Severity	Low
Category	SuspiciousActivity
Source	Custom TI
Detection time	2022 5:52 UTC
Device name	[redacted]

Alert page

[View in Microsoft 365 Security Center >](#)

[View in Microsoft Defender for Endpoint >](#)

Incident page

[View in Microsoft 365 Security Center >](#)

[View in Microsoft Defender for Endpoint >](#)

Fancy Bear(Russia)_2201

今年初めに発表された MDE SIEM API の非推奨化は、現時点では延期されています。詳細については、2022 年第 3 四半期に予定されています。

アラートの詳細を表示

[redacted] Risk level Low
データの機密性: 公開ラベル +1
AzureAD [redacted] (softcreate) 部長

アラートのストーリー

すべて展開

2022/ [redacted] 10:08:30	[580] smss.exe	...
10:08:31	[1392] winlogon.exe	...
22:19:43	[22936] explorer.exe	...

インシデント > Fancy Bear(Russia)_2201 on one endpoint

Fancy Bear(Russia)_22...

インシデントの管理 脅威エキスパートに相談

概要 アラート (1) デバイス (1) ユーザー (0) メールボックス (0) アプリ (0) ...

アラートとカテゴリ

1/1 件のアクティブなアラート

MITRE ATT&CK の戦術なし

範囲

デバイス 1 件が影響を受けました

影響を受けた主なエンティティ

エンティティの種類 [redacted] リスクのレベル/調査の優先 [redacted] 低

インシデントの情報

- ノートシールの概要
- インシデントのタグ
- データの機密性: 公開ラベル
- インシデント 詳細

なぜEDRに運用が必要か？

【アラートサンプル／管理画面】

Microsoft 365

Suspicious LDAP query was detected by Microsoft Defender for Endpoint on [redacted]

Alert details

Title	Suspicious LDAP query
Severity	Medium
Category	Collection
Source	EDR
Detection time	March 31, 2022 2:41 UTC
Device name	[redacted]

Alert page

View in Microsoft 365 Security Center >

View in Microsoft Defender for Endpoint >

Incident page

View in Microsoft 365 Security Center >

Microsoft 365 Defender | 検索

インシデントとアラート

Multi-stage incident involving Execution & Collection...

アラートとカテゴリ

0/2 件のアクティブなアラート

2 MITRE ATT&CK の戦術

範囲

デバイス 1 件が影響を受けました

1 人の影響を受けたユーザー

影響を受けた主要なエンティティ

エンティティの種類

リスクのレベル/調査の優先度

タグ

証拠

2 個のエンティティが見つかりました

すべてのエンティティの表示

インシデントの情報

このインシデントは、より多くのインシデントに関連付けられています。

関連付けられているインシデント

インシデント ID

理由

エンティティ

2664

同じデバイス

901491aa5...

2643

コマンドライン...

powershell...

ノートブックの概要

インシデントのタグ

インシデント 詳細



ここからアラートのイベント概要、詳細を読み取るのは、セキュリティの知見がないと困難・・・



Security FREE for

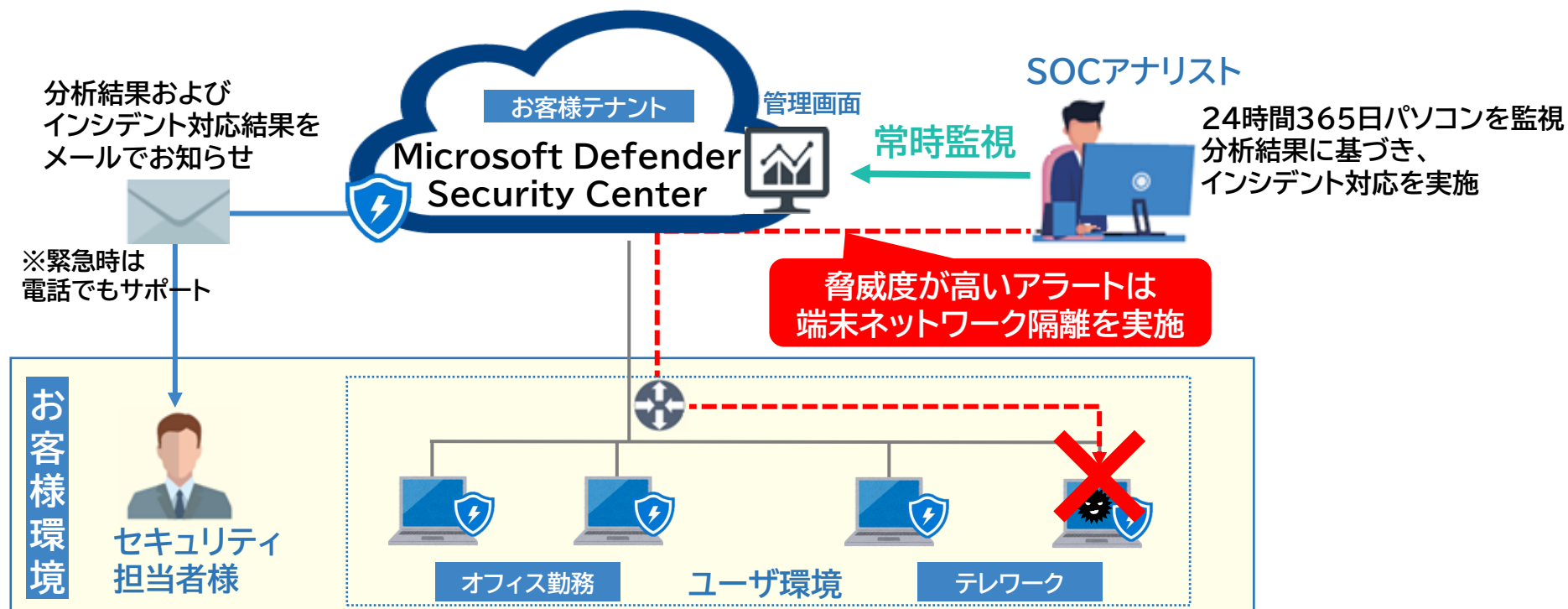
Microsoft Defender for Endpoint／Business

概要

Microsoft Defender for Businessで発生したアラートを**24時間365日**で監視し、当社基準にて脅威判定を行い、お客様にエスカレーションするSOCサービスです。

脅威度が高いアラートについては、サービス側で端末の隔離も実施いたします。

- ✓ 専門家判断でセキュリティ対応の精度を向上
- ✓ セキュリティ担当者の負担を軽減



- Microsoft Defender for Endpoint の機能によりブロックまたは自動調査機能により無害化されていないアラート（下図の赤枠）を対象にSOCで対応いたします。

製品自体の機能でブロック	SOCで対応
不審なファイルの実行 （ファイルがマルウェアと判定されている）	ファイルの実行後に不審なスクリプトの実行 （ファイルはマルウェア判定されていないが、実行したマクロ・スクリプトが危険と判断された場合）
不審なリンク・サイトへのアクセス （サイト自体が不審と判定されている）	サイトへのアクセス後に不審な通信が発生 （サイトは不審なサイトとして判定されていないが、ユーザ操作とは考えにくい通信が発生した場合）
使用しているアプリケーションの脆弱性をついた攻撃 ※ブラウザ、Adobe Flash Player、O365 （脆弱性をついた攻撃と判断されている）	一部のブロックできなかったアプリケーションの脆弱性をついた攻撃 （バッファオーバーフローなどを利用しPCへ侵入、PCの情報を取得する場合）

エンドポイントの安心運用をご提供

「Emotet」への感染を狙ったマクロ付きファイルを開いた際の挙動を、Microsoft Defender for Endpointが検知した際の管理画面です。

製品側の重大度は下から2番目の「Low」でしたが、SOC側では確認が推奨されるアラートであると判断しました。

警告の名前	タグ	重大度	調査の状態	状態	カテゴリ
'Emotet' malware was detected		■■■ 情報	Remediated	● 解決済み	マルウェア
'EncDoc' malware was detected		■■■ 情報		● 解決済み	マルウェア
A malicious file was detected based on indi...		■ ■ ■ 低	Remediated	● 解決済み	マルウェア
'EncDoc' malware was prevented		■■■ 情報	Terminated by system	● 新規	マルウェア
'Emotet' malware was detected		■■■ 情報	Terminated by system	● 新規	マルウェア
A malicious file was detected based on indi...		■ ■ ■ 低	Terminated by system	● 解決済み	マルウェア

製品側の重大度は「Low」

SOC/MSSの実例

このように、製品側の重大度が比較的低めのアラートであっても、SOC側の分析の結果、対処が推奨される場合は、エスカレーション通知を行います。（必要に応じて端末隔離も実施）

分析イメージ

イベント

該当端末のタイムライン

EXCEL.EXE created registry key 'S-1-5-21-...'

excel.exe がレジストリ キー 'HKEY_CURRENT_USER\S-1-5-21-...'

EXCEL.EXE created registry key 'S-1-5-21-...'

excel.exe がレジストリ キー 'HKEY_CURRENT_USER\S-1-5-21-...'

OUTLOOK.EXE がプロセス EXCEL.EXE を作成しました

Alert process tree

プロセスツリーサンプル

userinit.exe

explorer.exe

cmd.exe

powershell.exe

Process cmd.exe has been executed with elevated permissions via svchost.exe

Export データサンプル

ComputerName	Action Type	Process Name
esktop-3fj4ntu	ProcessCreated	RuntimeBroker.exe
esktop-3fj4ntu	ProcessCreated	RuntimeBroker.exe
esktop-3fj4ntu	ConnectionSuccess	
esktop-3fj4ntu	ProcessCreated	RuntimeBroker.exe
esktop-3fj4ntu	ImageLoaded	vaultcli.dll
esktop-3fj4ntu	ImageLoaded	dbghelp.dll
esktop-3fj4ntu	ImageLoaded	hid.dll
esktop-3fj4ntu	FileCreated	__PSScriptPolicyTest_znv0hfl...
esktop-3fj4ntu	FileCreated	__PSScriptPolicyTest_4y3le5c...
esktop-3fj4ntu	ConnectionSuccess	
esktop-3fj4ntu	ProcessPrimaryTokenModified	
esktop-3fj4ntu	ProcessCreated	backgroundTaskHost.exe
esktop-3fj4ntu	ProcessCreated	HxTsr.exe

etc.

対応イメージ

お世話になっております。S&Iアナリストチームです。

MDREにてアラートを検知し分析を行いました。以下の通り、ご連絡いたします。

1. 検知イベント概要

- 検知時間: [redacted]
- 検知件数: 1件
- 検知端末: [redacted]
- 検知項目: マルウェア

2. 脅威判定

(1) 見解

脅威レベルは「3」（不審なファイルによる感染の疑い）となります。不審なファイルを検知しました。

(2) 影響範囲

現時点では1項の「検知端末」のみで発生しております。

3. 分析詳細

(1) 分析結果

不審なファイルは以下となります。

[redacted] xlsxm

[redacted] 作業者がOUTLOOK.EXEを起動。

[redacted] [redacted] .ip) を解凍しました。

SecurityFREEポータルからエスカレーションを実施

ncidents > 1 > [Test Alert] Suspicious Powershel... > desktop-100sj8k

Manage tags Isolate device Restrict app execution ...

desktop-100sj8k

No known risks Active

Overview Alerts Timeline Security recommendations Software inventory Discov

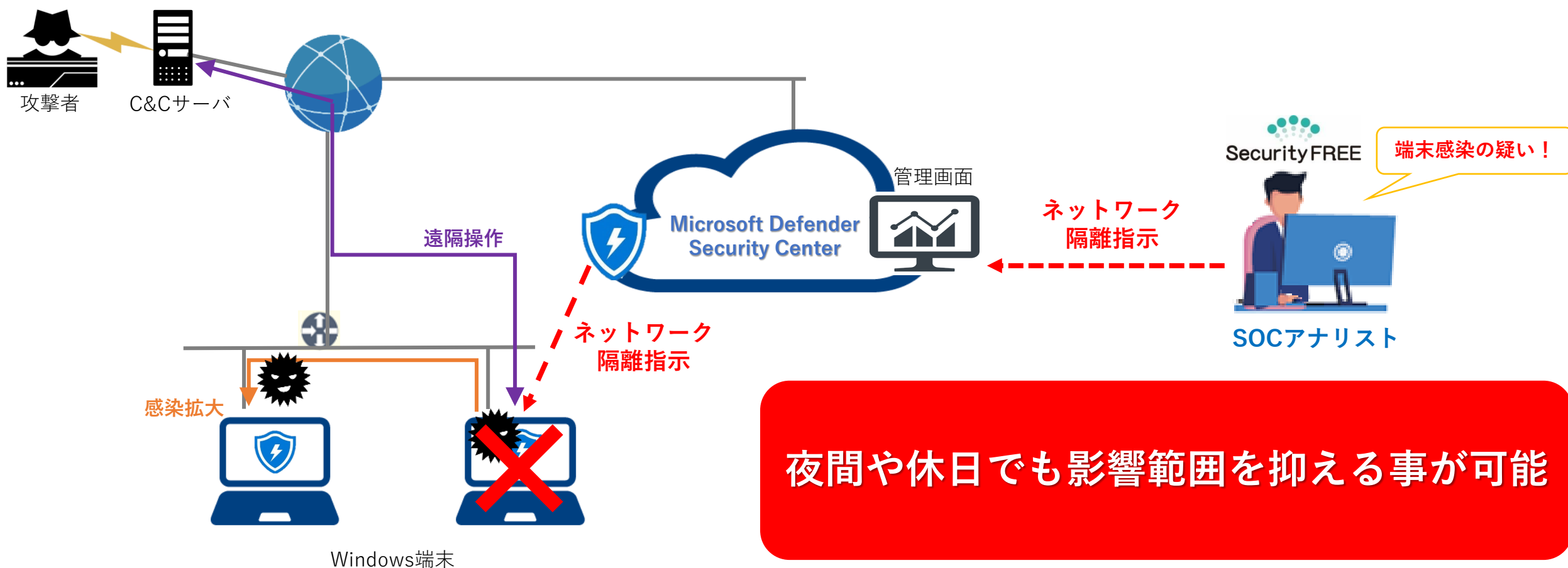
※検証環境のデバイスです

必要に応じて、該当デバイスをNWから分離

セキュリティインシデント発生時の支援

セキュリティインシデント対応

分析の結果、脅威レベル3または4と判断した場合、該当端末をネットワークから隔離します。



エスカレーションサンプル

1. 検知イベント概要

- ・検知時間 : 2020/09/01 14:17
- ・検知件数 : 1件
- ・検知端末 : desktop-1112223¥test_analyst
- ・検知項目 : Suspicious Powershell commandline

2. 脅威判定

(1) 見解

脅威レベルは「3」（1つの端末でマルウェアの感染が強く疑われるイベント）となります。

* 該当の端末は隔離しております。

検知したイベントはコマンドプロンプトからPowerShellを起動したことを検知しております。
PowerShellで不審なファイルをダウンロードした可能性があります。

(2) 影響範囲

現時点では1.項の「検知端末」のみで発生しております。

脅威度が
一目で分かる

3. 分析詳細

(1) 分析結果

PowerShellからファイルのダウンロードとそのファイルの実行する挙動を検知しており、
該当ファイルはレピュテーションサイトではマルウェアと判断されております。

ファイル名 : 1.exe

当該端末のプロセス生成ログを確認しましたが、ダウンロードしたファイルのログは
ございませんでした。

また、PowerShellで暗号化された内容をデコードした結果、通信先は以下と考えられますが、
接続ログにはございませんでした。

- ・hxxp://xxx.yyy.zzz
- ・hxxp://55.66.77.88

4. 対処依頼事項

ファイルをダウンロードした可能性があるため、当該端末の使用者へヒアリングをお願いします。
ファイルの削除および端末のウィルススキャンを実施の上、問題がなければ隔離解除をご依頼くだ
さい。

何が起こったか、
専門家でなくても把握できる

対処方法まで案内されるため
専門家でなくても安心

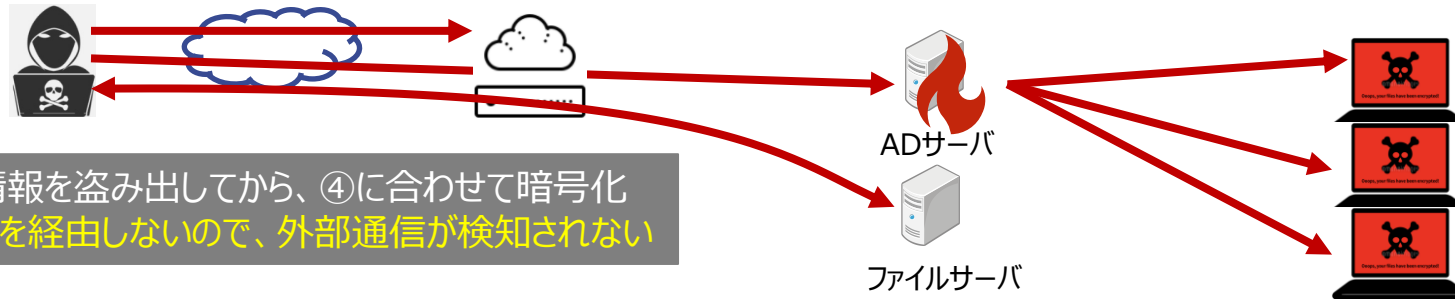
VPNルータの脆弱性／アカウントから侵入され、ADサーバが制圧されユーザPCが暗号化

- A①：VPNルータへ脆弱性を突いて侵入
B②：VPNルータへブルートフォース攻撃でアカウント取得

- ② AD情報を収集し、パスワードプレイ攻撃から管理者アカウントでADへ侵入し、グループポリシー 改竄
ユーザPCのAV,EDRの無効化/ユーザPCへマルウェア配信

- ③ 機密情報を盗み出してから、④に合わせて暗号化
プロキシを経由しないので、外部通信が検知されない

- ④ PC起動時にランサムウェアが起動



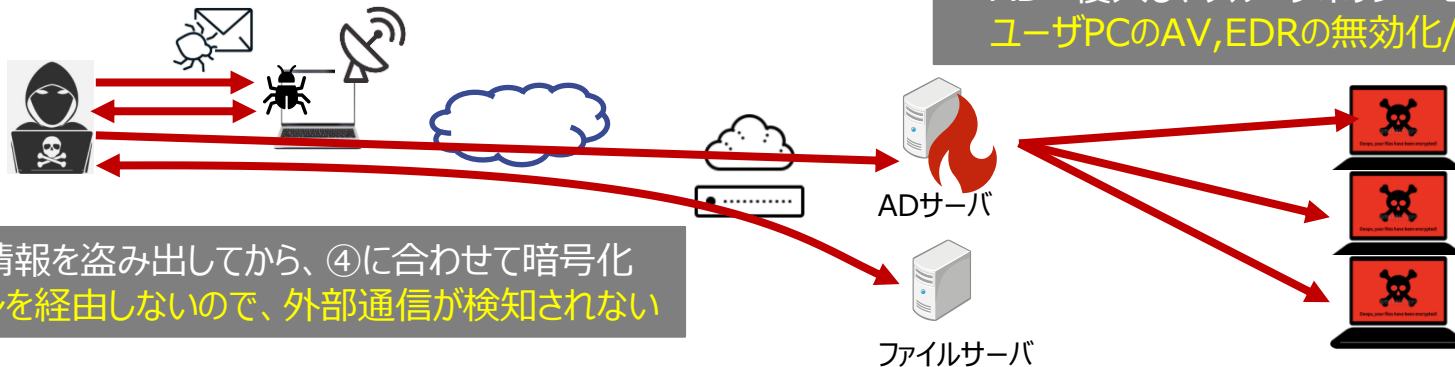
メール添付ファイルから侵入、ADサーバが制圧されユーザPCが暗号化

- ① マルウェア付きメールを送信

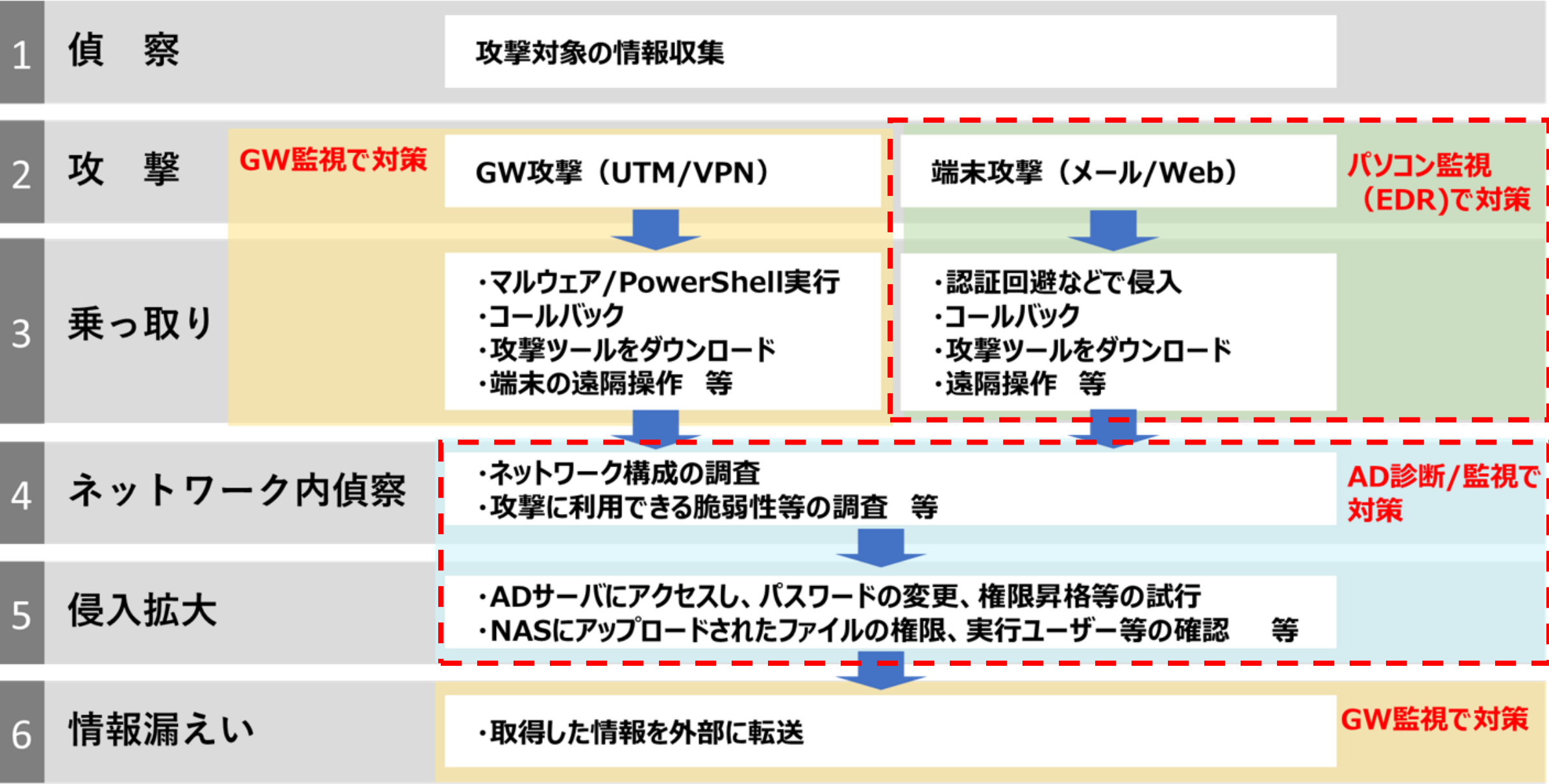
- ② AD情報を収集し、パスワードプレイ攻撃から管理者アカウントでADへ侵入し、グループポリシー 改竄
ユーザPCのAV,EDRの無効化/ユーザPCへマルウェア配信

- ③ 機密情報を盗み出してから、④に合わせて暗号化
プロキシを経由しないので、外部通信が検知されない

- ④ PC起動時にランサムウェアが起動



対策のポイント





① 誤検知か実際の攻撃か判断するのは**人**

② サイバー攻撃対策の第一歩として**PC監視**

③ PC対策と並行して**AD対策**も必須