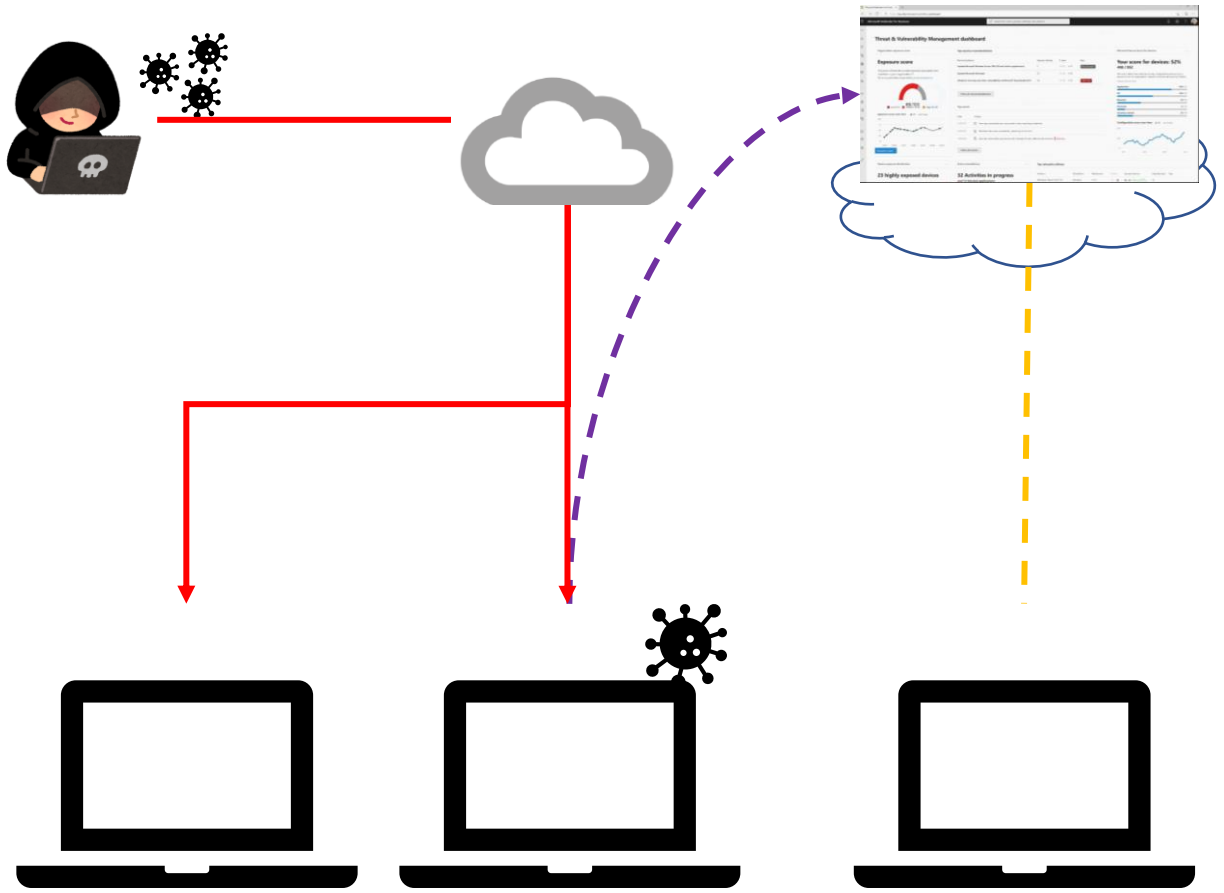
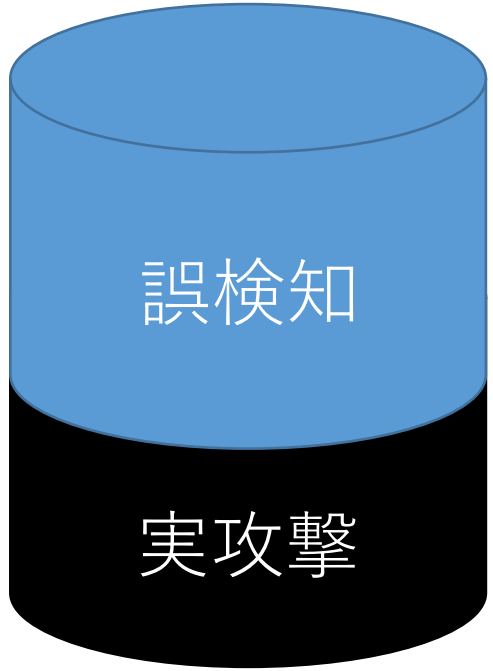
Microsoft Defender for Endpoint／Businessに監視サービスは必要か？

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？



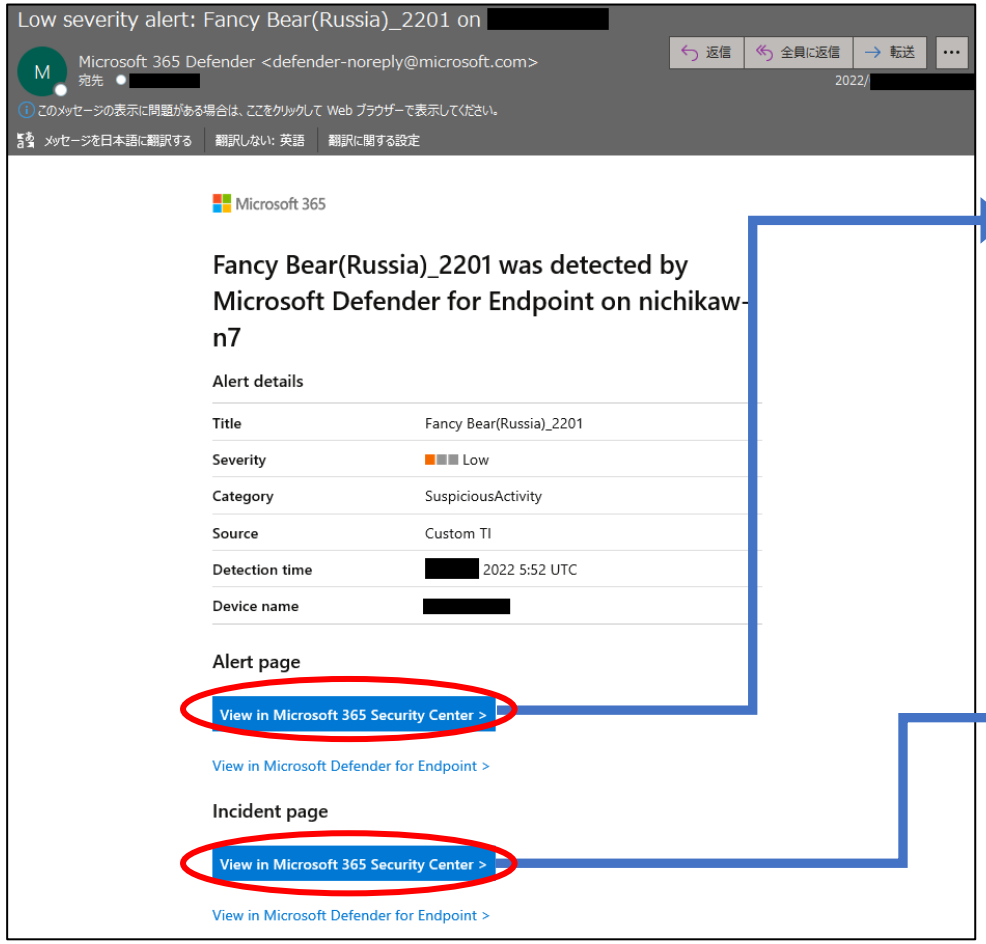
管理者PC

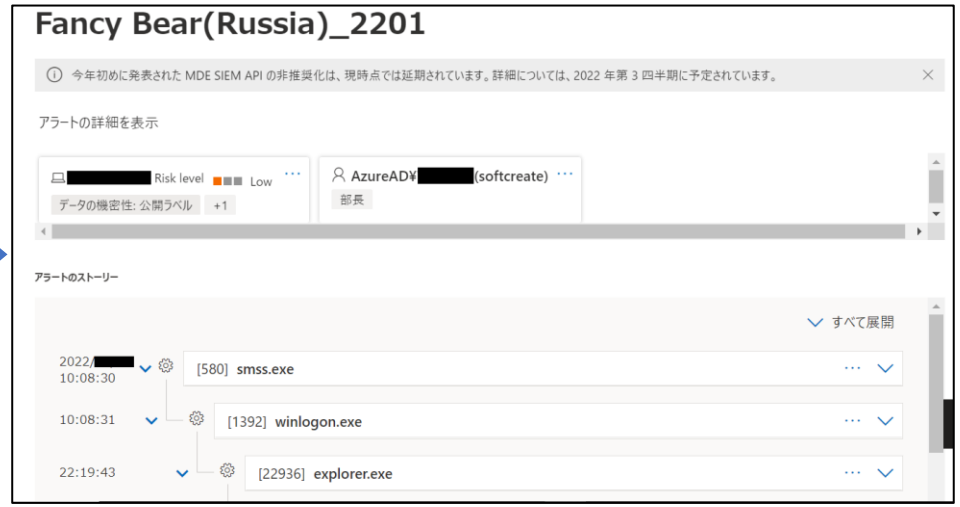


判断するのは人

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。





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]

[redacted]

Alert details

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

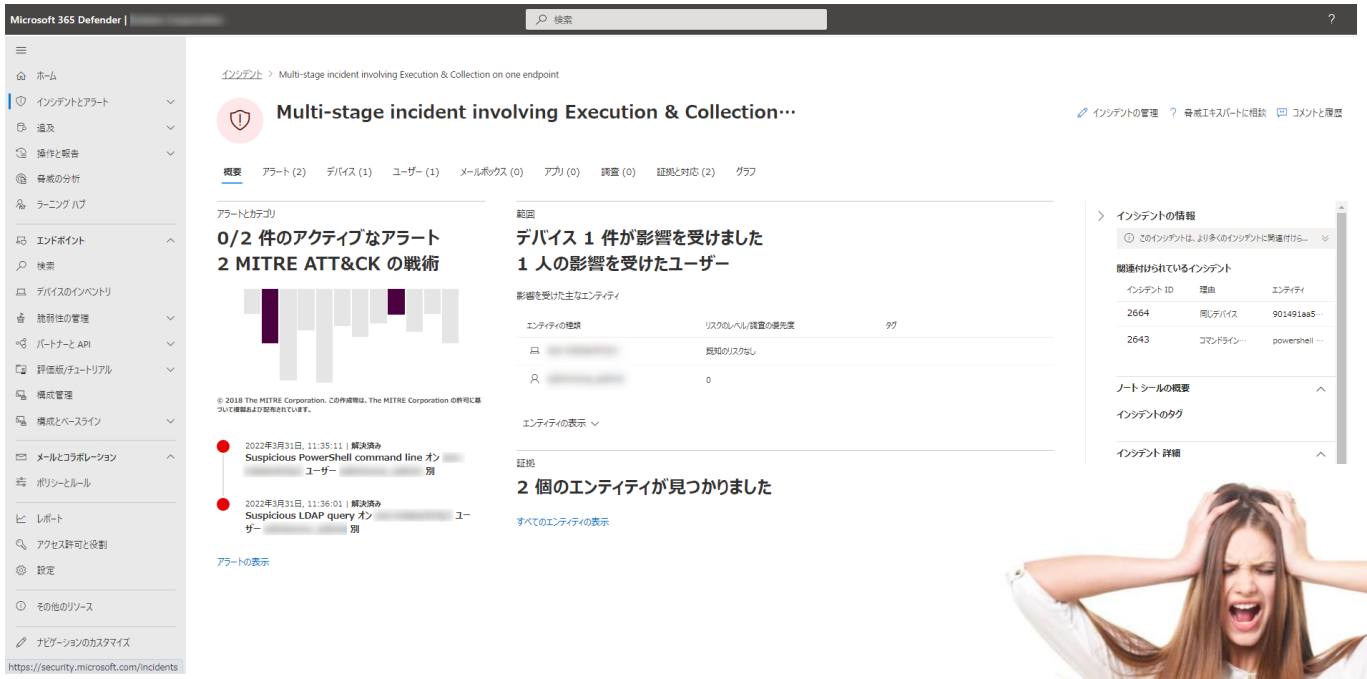
Alert page

View in Microsoft 365 Security Center >

View in Microsoft Defender for Endpoint >

Incident page

View in Microsoft 365 Security Center >



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・・・

Microsoft DIGITAL TRUST SECURITY Alliance

Security FREE for

Microsoft Defender for Endpoint／Business

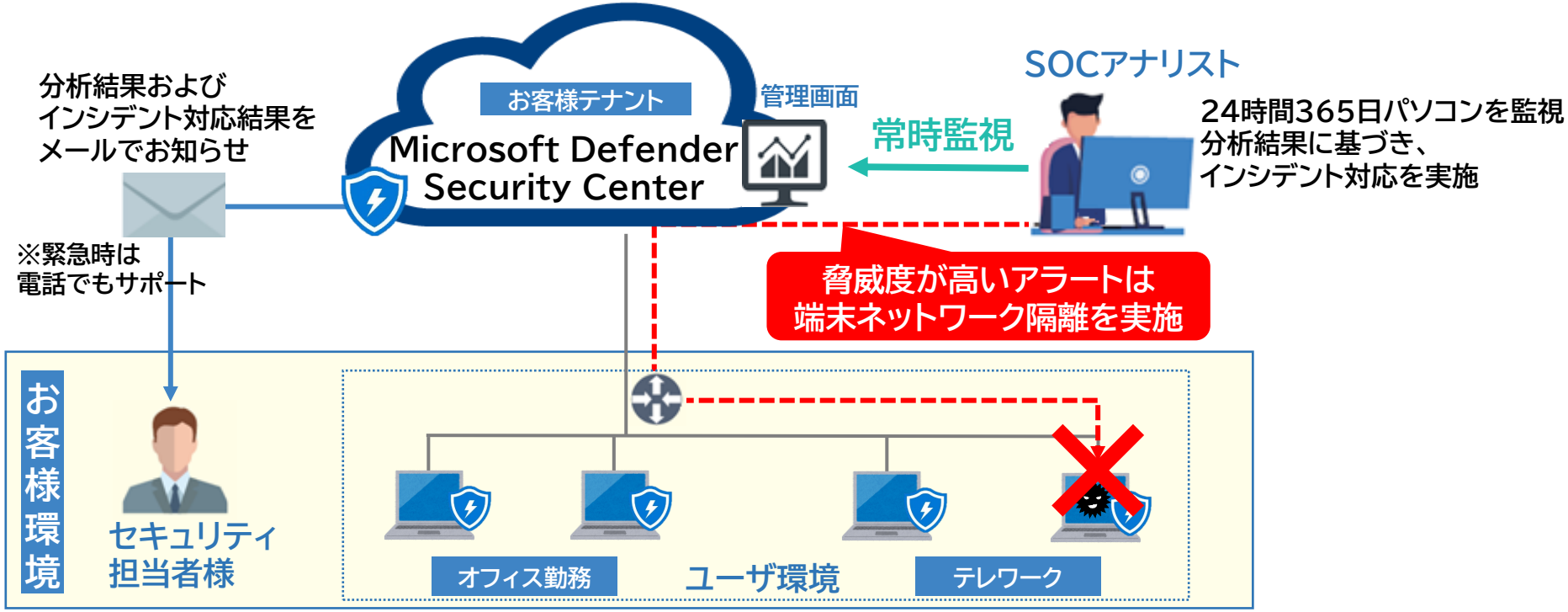
サービス概要

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



SOC/MSSの必要性

- 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

SOC/MSSの実例

「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。

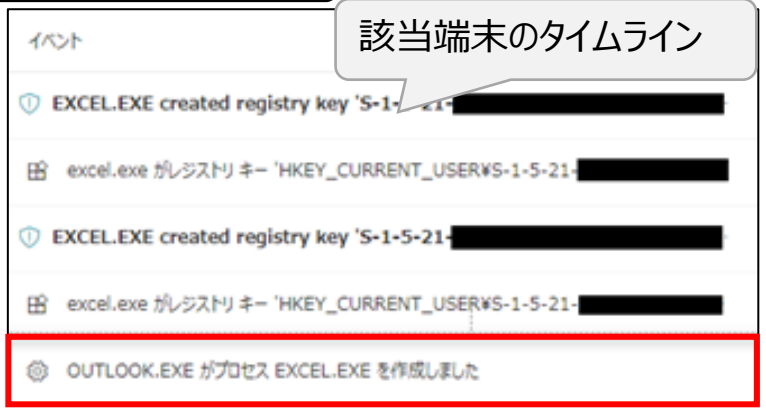
警告の名前	タグ	重大度	調査の状態	状態	カテゴリ
'Emotet' malware was detected		情報	Remediated	解決済み	マルウェア
'EncDoc' malware was detected		情報		解決済み	マルウェア
A malicious file was detected based on indi...		低	Remediated	解決済み	マルウェア
'EncDoc' malware was prevented		情報	Terminated by system	新規	マルウェア
'Emotet' malware was detected		情報	Terminated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

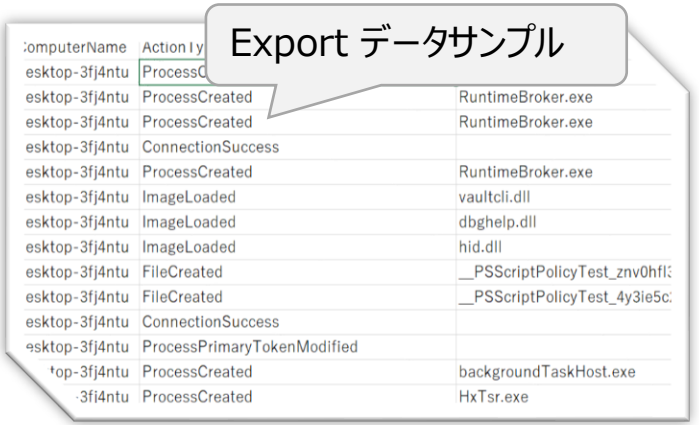
製品側の重大度は「Low」

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）

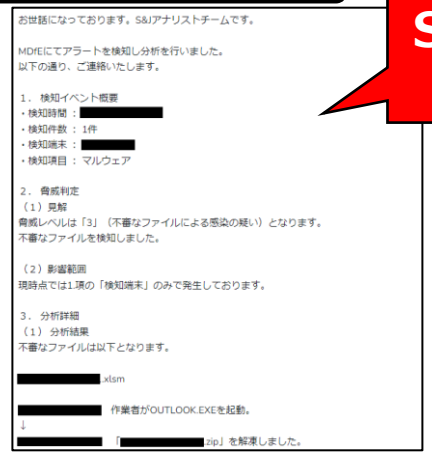
分析イメージ



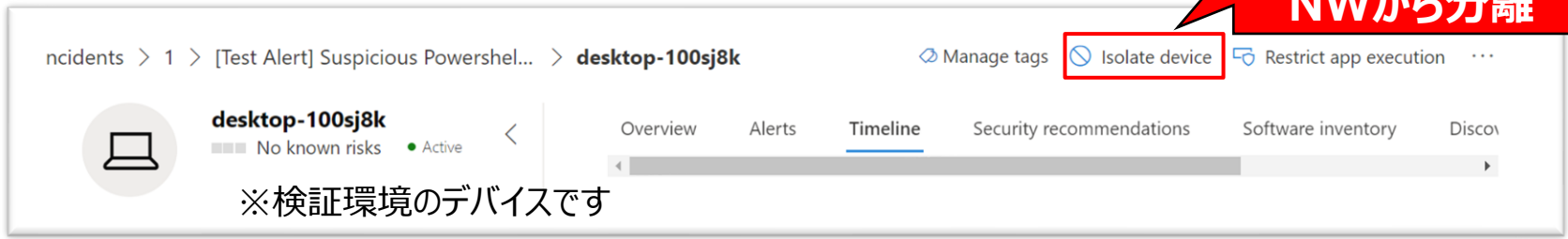


etc.

対応イメージ



**SecurityFREEポータルから
エスカレーションを実施**



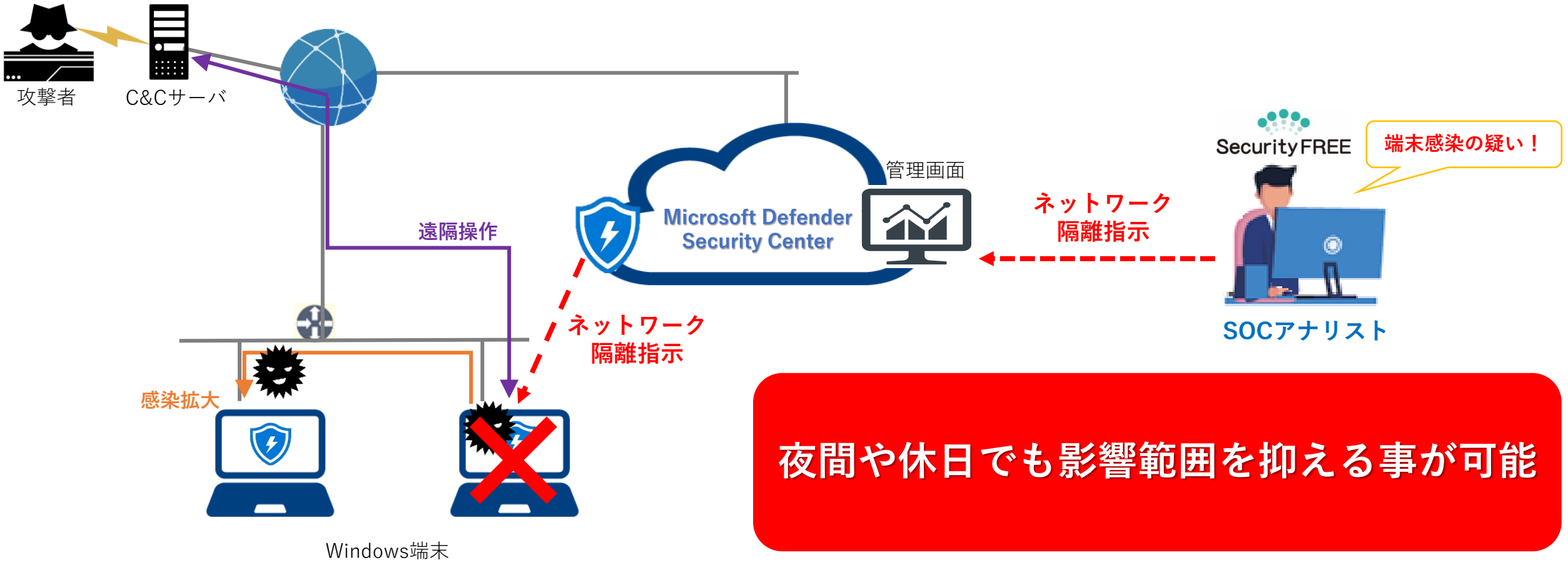
※検証環境のデバイスです

**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。



夜間や休日でも影響範囲を抑える事が可能

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

何が起こったか、
専門家でなくても把握できる

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。

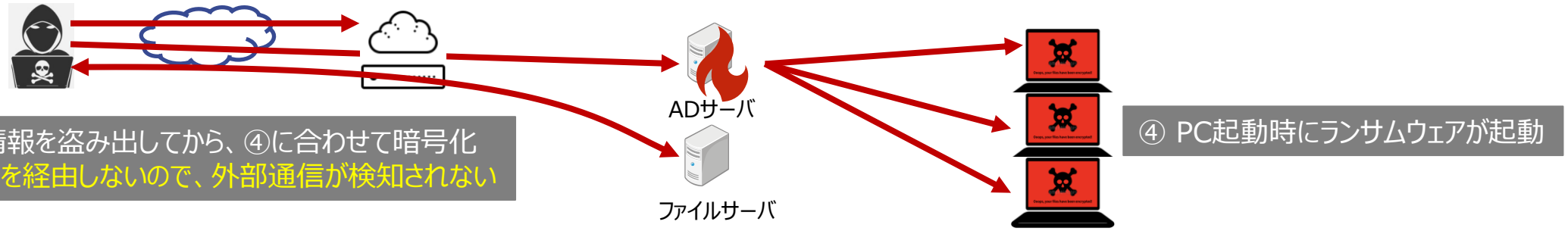
対処方法まで案内されるため
専門家でなくても安心

ちなみに・・・

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、パスワードス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



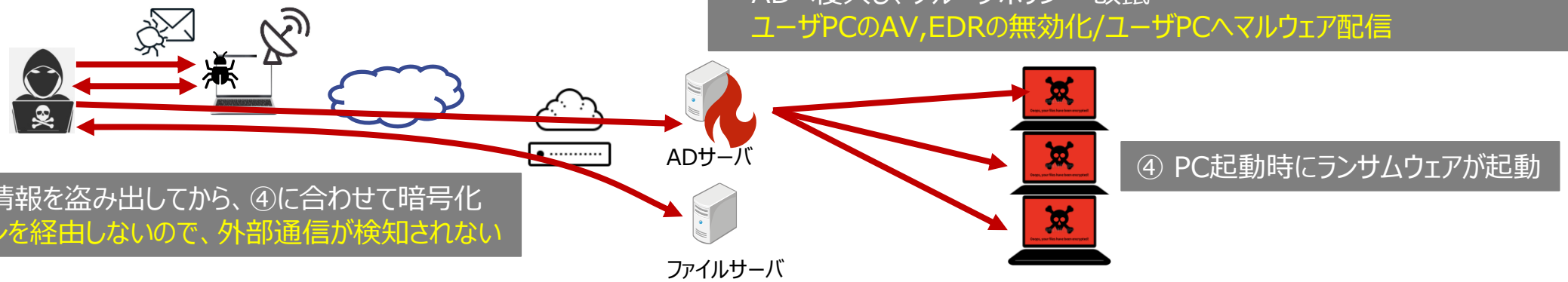
③ 機密情報を盗み出してから、④に合わせて暗号化
プロキシを経由しないので、外部通信が検知されない

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、パスワードス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	偵　察	攻撃対象の情報収集	
2	攻　撃	GW攻撃（UTM/VPN）	端末攻撃（メール/Web）
3	乗っ取り	・マルウェア/PowerShell実行 ・コールバック ・攻撃ツールをダウンロード ・端末の遠隔操作　等	・認証回避などで侵入 ・コールバック ・攻撃ツールをダウンロード ・遠隔操作　等
4	ネットワーク内偵察	・ネットワーク構成の調査 ・攻撃に利用できる脆弱性等の調査　等	
5	侵入拡大	・ADサーバにアクセスし、パスワードの変更、権限昇格等の試行 ・NASにアップロードされたファイルの権限、実行ユーザー等の確認　　等	
6	情報漏えい	・取得した情報を外部に転送	

GW監視で対策

パソコン監視（EDR)で対策

AD診断/監視で対策

GW監視で対策

本セッションのまとめ

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