
Microsoft 365 運用の第一歩！
【Microsoft365安心サポート＜Security＞】はじめました
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

本セミナーで分かること

サービス背景

- サービスで取り扱っている製品自体の概要
- 製品単体の場合の運用
- よくある悩み

サービス内容

- サービス概要
- サービス全体イメージ
- サービス提供範囲
- 対応製品一覧

お客様が得られるメリット

- 解決できる課題
- サービスの強み

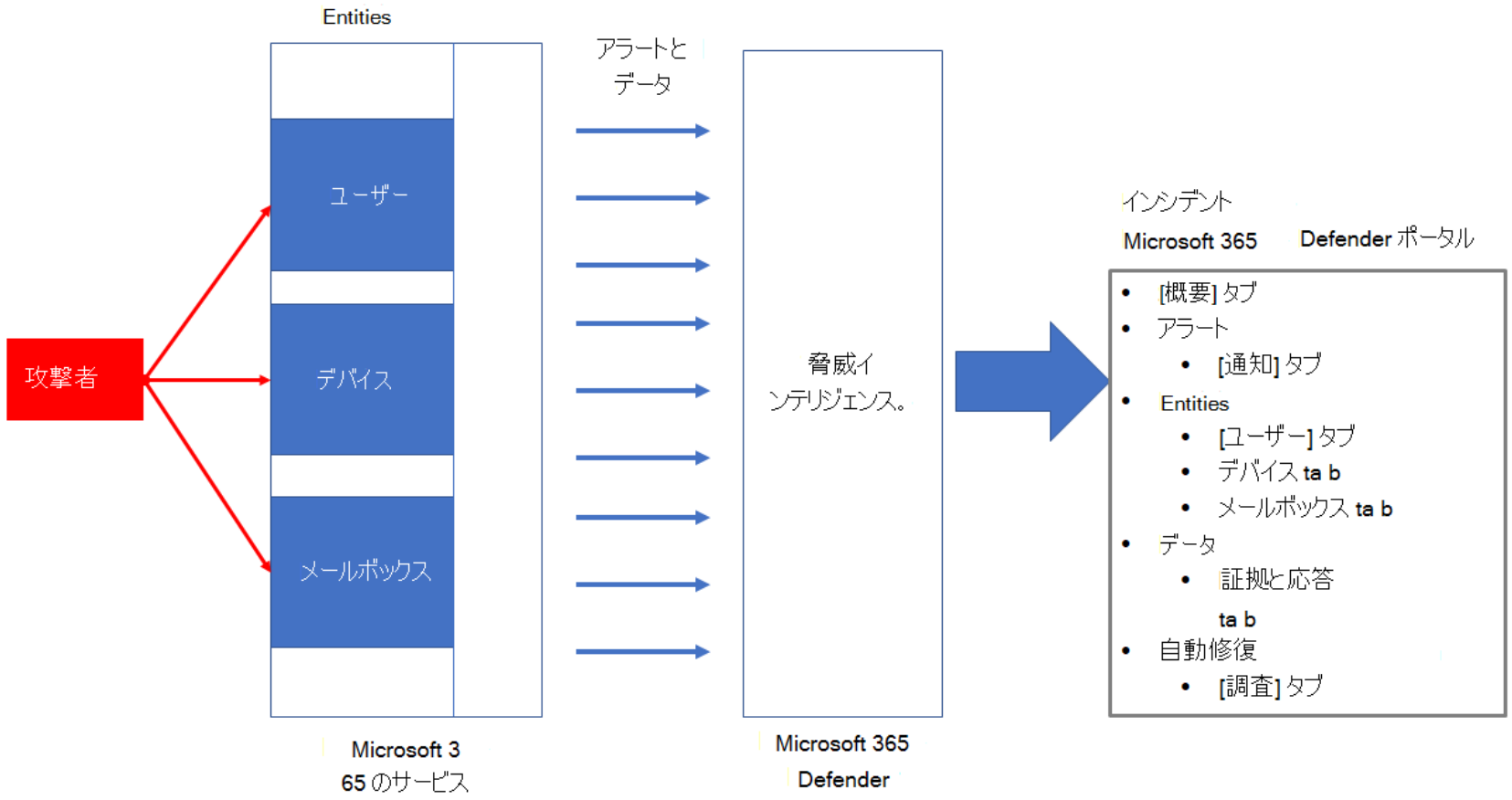
もくじ

もくじ

はじめに
–取り扱う製品自体について–

M365 Defenderを使用したアラート調査

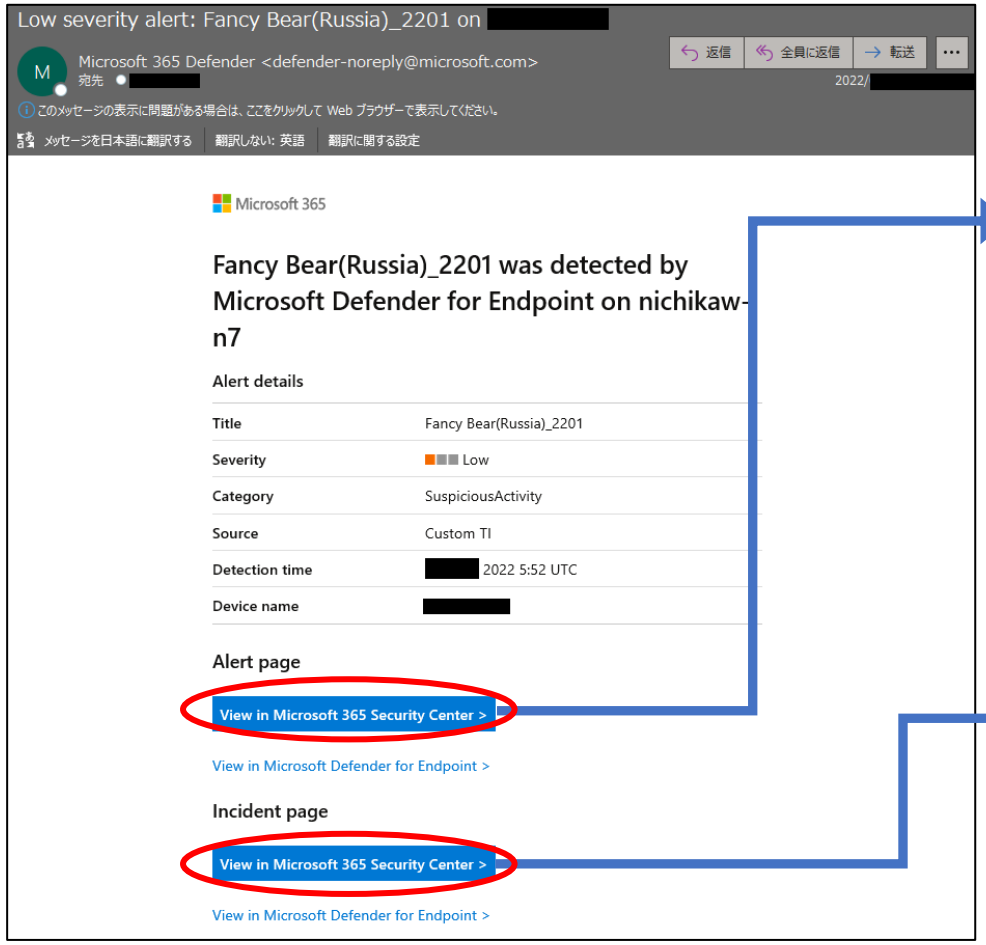
Microsoft 365サービスおよびアプリは、疑わしいイベントやアクティビティを検出すると
アラートを作成します。

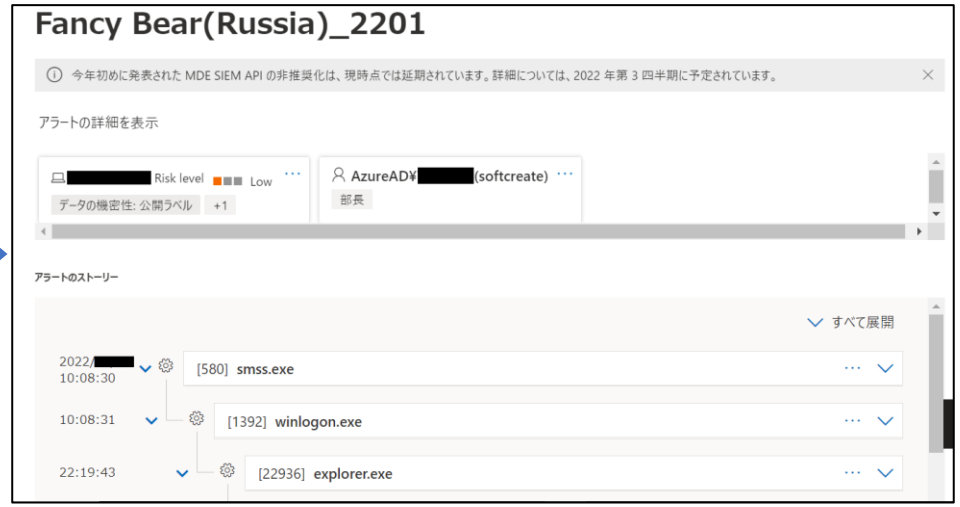


https://docs.microsoft.com/ja-jp/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

M365 Defenderを使用したアラート調査

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。





Microsoft365 安心サポート＜Security＞が必要な理由

【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]

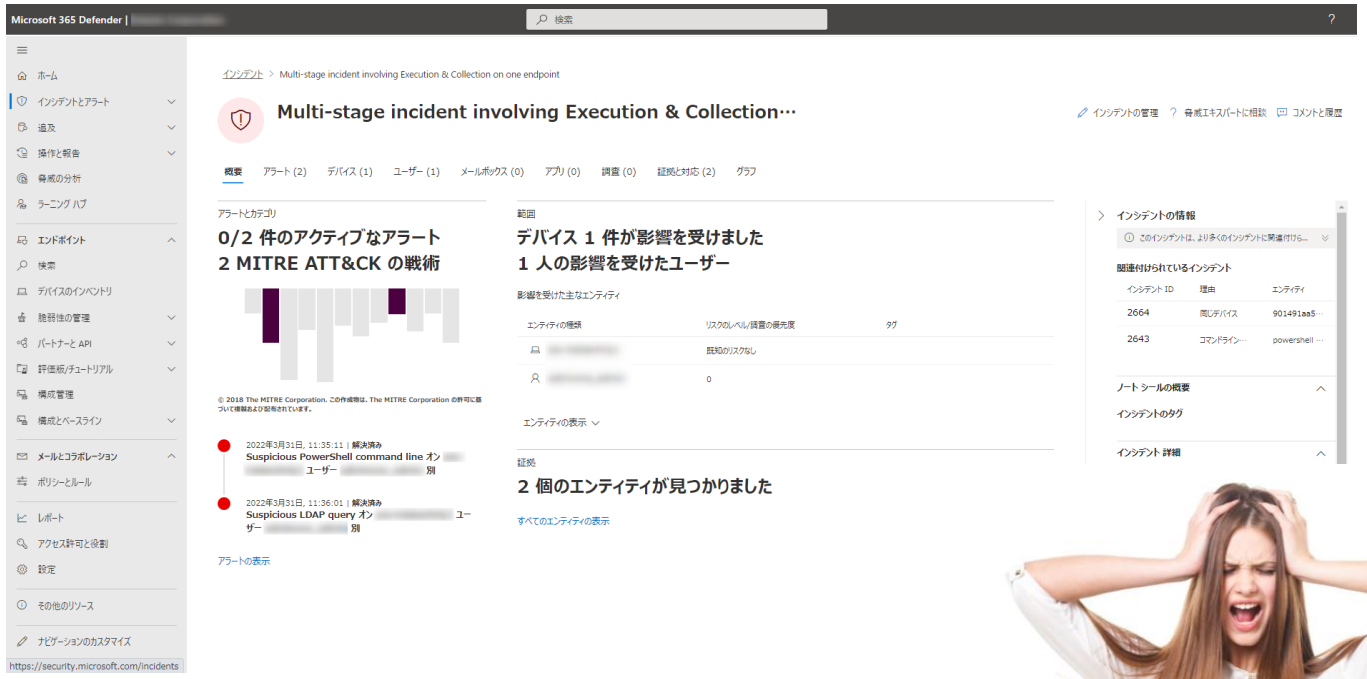
Alert page

View in Microsoft 365 Security Center >

View in Microsoft Defender for Endpoint >

Incident page

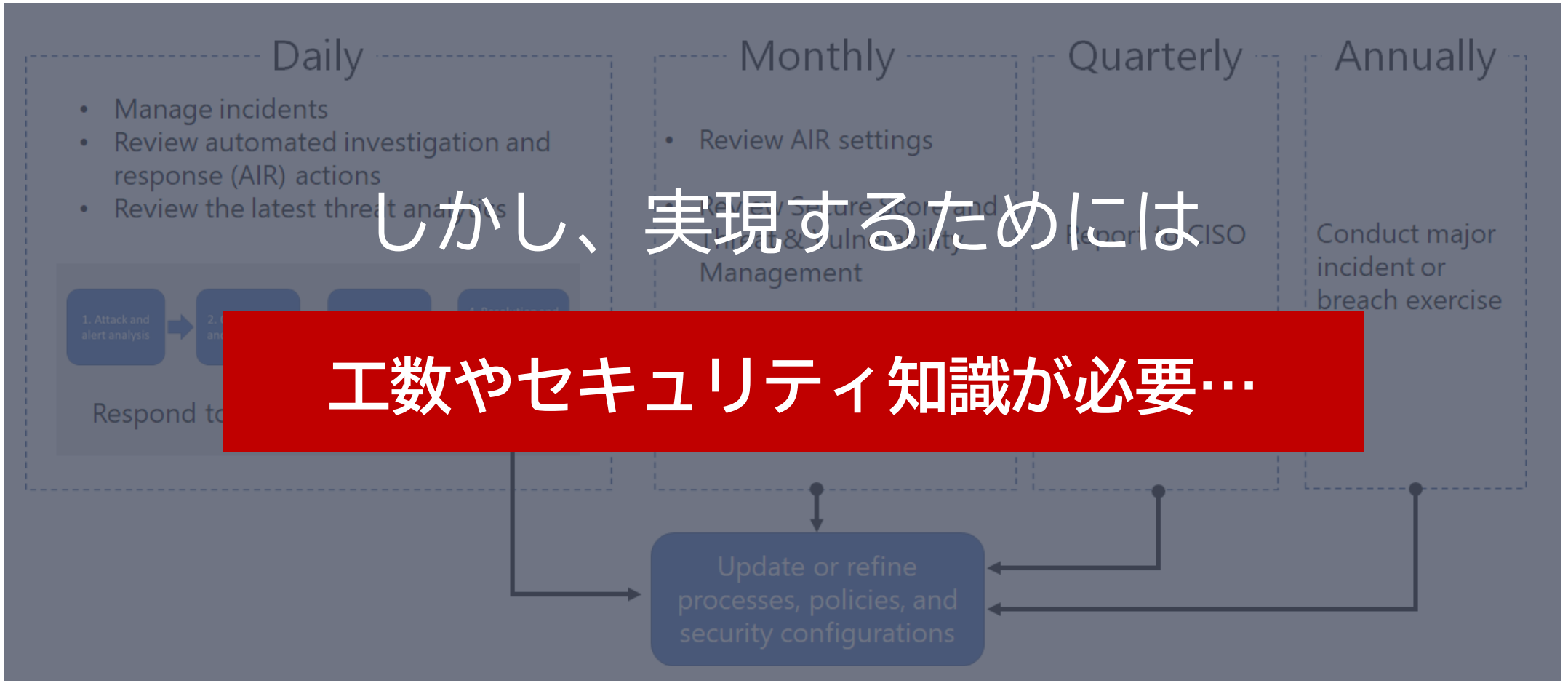
View in Microsoft 365 Security Center >



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・・・

インシデント対応、アラート調査の課題

Microsoft社は、Microsoft 365 Defenderのセキュリティ操作の例として、以下を示しています。



しかし、実現するためには

工数やセキュリティ知識が必要…

インシデント対応、アラート調査の課題

情シス本来の業務に集中できない！

かといって24h/365dのSOCは高額・・・

そこで…

皆様のノンコア業務の負担を減らす
「ちょうどいい」支援サービスをはじめました。

もくじ

サービス内容

「Microsoft365安心サポート＜Security＞」とは？

ご依頼いただいたMicrosoft 365 Defender及びAzure Active Directoryで発生したアラートに対して、お客様のSecurity Centerを調査し、アラート内容を回答するサービスです。

◆提供時間：弊社営業日の9時～18時
◆連絡手段：メールのみ

1．アラート調査

メールでアラート調査をご依頼ください。
※ご依頼時には、アラートメールを添付してください。

2．アラート見解報告

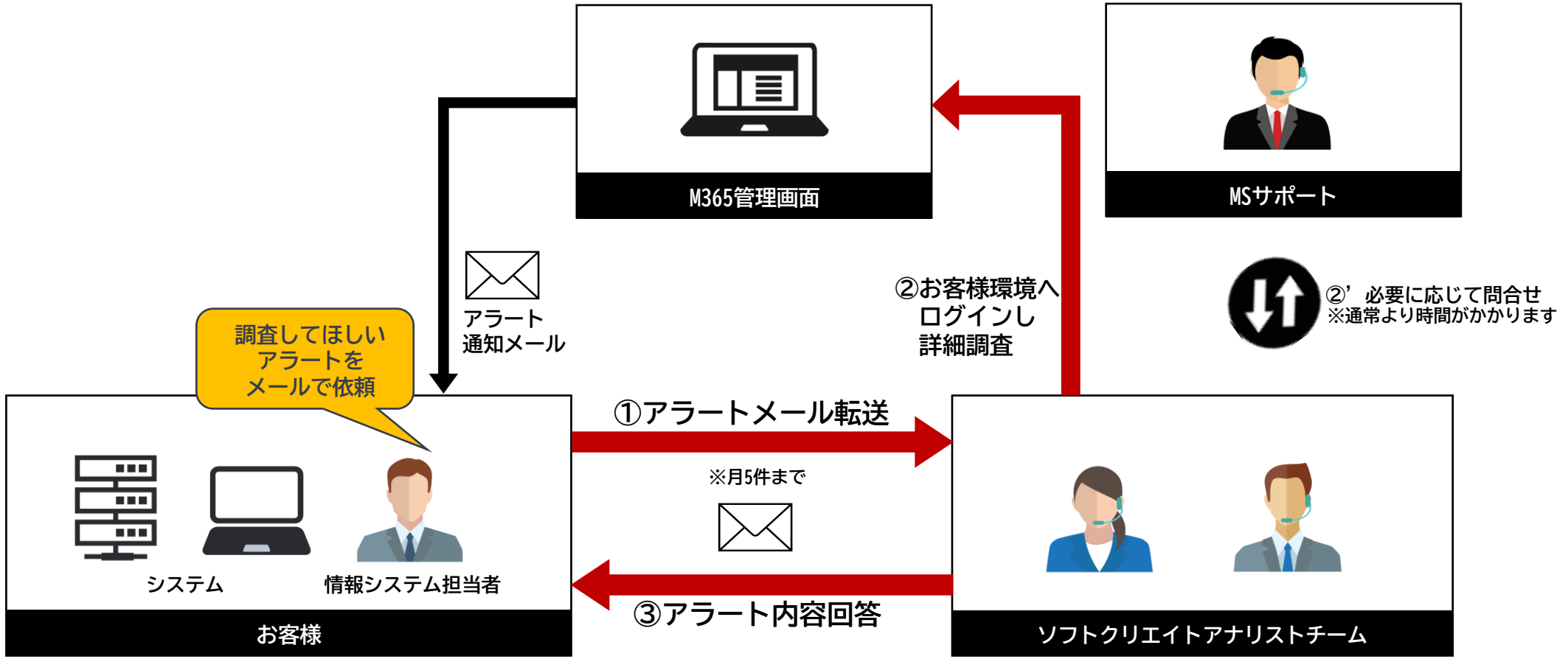
ご依頼いただいたアラートについてM365管理画面で調査し、アラート内容についての見解をメールで報告します。

3．報告に対する問合せ

弊社からの報告内容に対するお問合せについては回数制限なく、回答させていただきます。

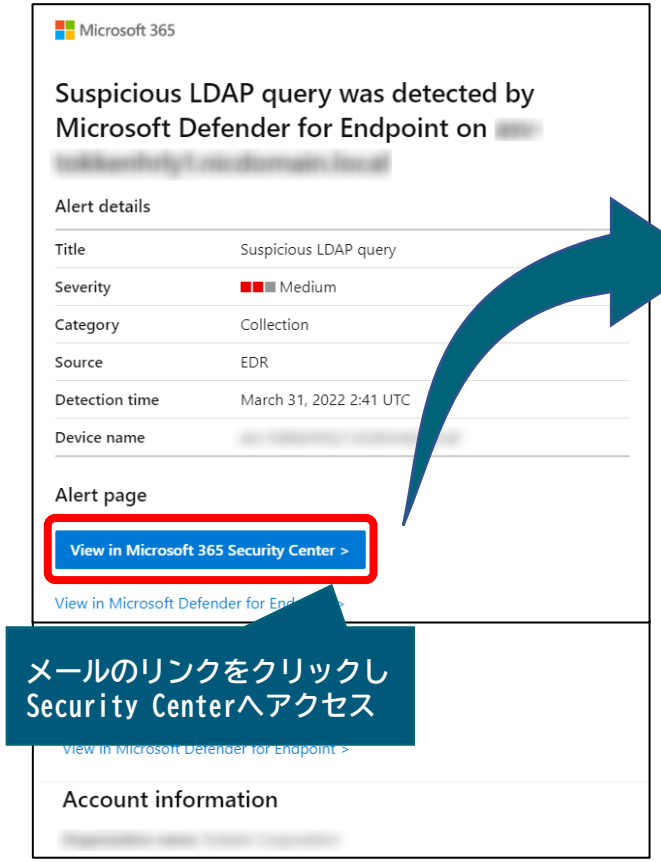
サービス全体イメージ

Microsoft365で発生したアラートメールをソフトクリエイトに転送頂くだけで、
アラート内のイベント概要、詳細、Security Centerでの推奨事項を回答いたします。



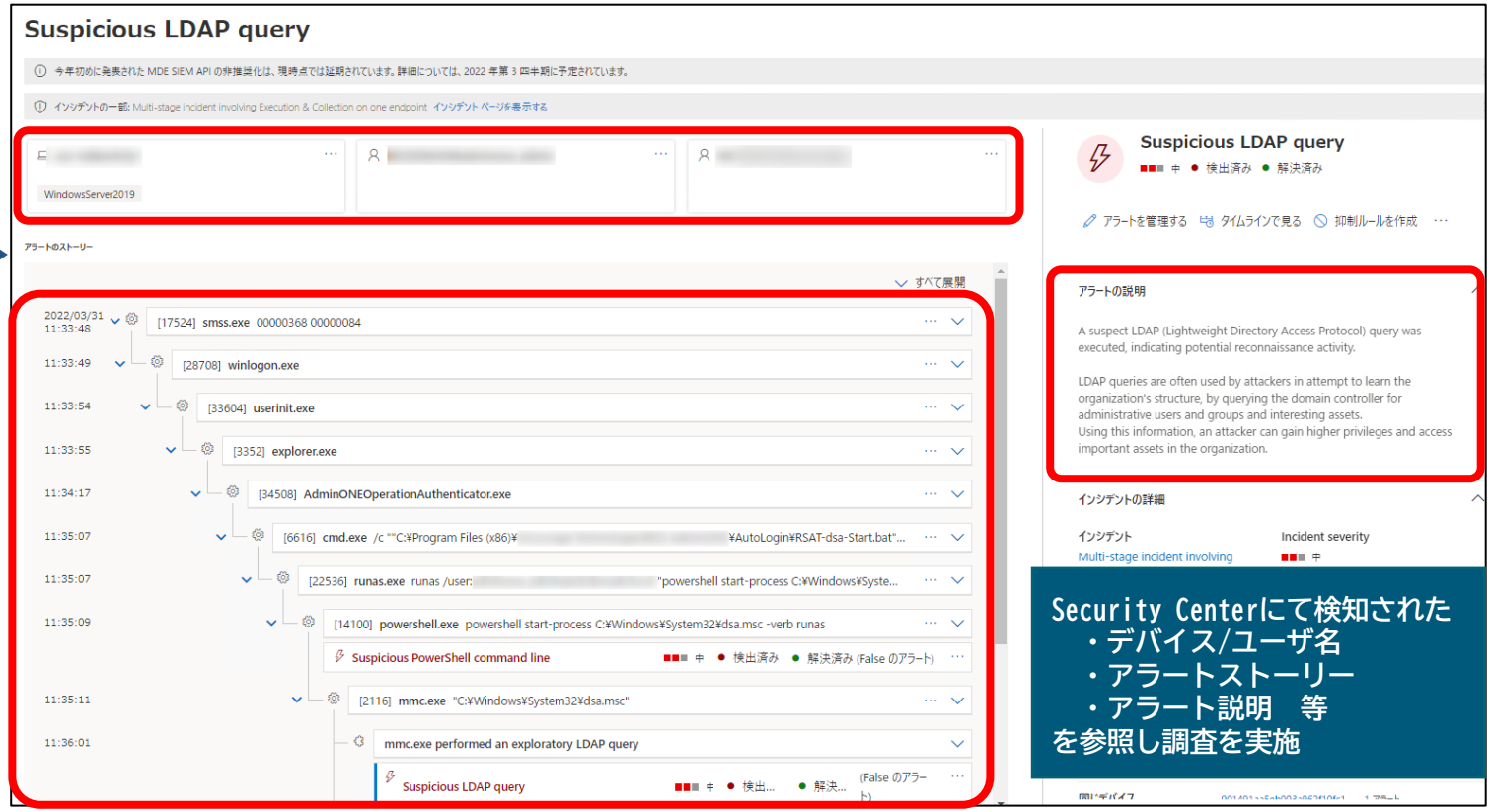
報告までの流れ(アラートメール-実画面)

アラートメール



メールのリンクをクリックし
Security Centerへアクセス

Security Center



Security Centerにて検知された
・デバイス/ユーザ名
・アラートストーリー
・アラート説明　等
を参照し調査を実施

アラート内容回答サンプル

株式会社テスト
〇〇様

平素お世話になっております。
ソフトクリエイトアナリストチームです。

お問い合わせいただきましたアラートについて、
調査結果を以下にご報告いたします。

■検知イベント内容：
Malware incident on one endpoint
（エンドポイント端末1台でのマルウェアに関連するインシデント発生）

■検知イベント概要：
・発生日時：
2022年3月3日 14:02:29
└ 検知数：2件
①Malware was detected in a zip archive file
（zipアーカイブファイルでマルウェアと思しきファイル検出）
②'Keygen' hacktool was prevented
（「Keygen」というハッキングツールが防止された）

何が検知のきっかけに
なったか分かりやすい

・検知ホスト（ユーザ名）：
test-n4（test）

・パス：
C:¥Users¥xxxxxx¥Downloads¥CNDv2 Module 02 Administrative Network Security.zip

・ファイル名：
CNDv2 Module 02 Administrative Network Security.zip

検知されたイベントについて
エンジニアの目線で補足

■検知イベント詳細：
検知ホストにて、"Keygen"と呼ばれるソフトウェアの「プロダクトキー」を不正に生成するツールを検出しました。

検知されたツールは、セキュリティ情報サイトVirusTotalの各エンジンで、「32/64」で危険性の指摘が見られ、リスクが高いものと判断されました。

検知名にある「Keygen」とは、ソフトウェアのライセンスキーを生成・取得するプログラムです。
ソフトウェアの利用においては、インストールの際に、
正規の購入者しか知り得ないパスコードの入力が要求される場合がありますが、
「keygen」はこの認証を突破することができる文字列を生成するプログラムです。

業務利用で無い場合は、該当端末はマルウェアに感染している可能性がございます。
また、今回検知されたツールが悪用された場合、情報漏洩や
著作権の侵害、別のマルウェアへの感染が発生する可能性があります。

ただし、アラート内容から、該当ツールはいずれもウイルス対策機能でブロックされており、以降で不審なアラートが確認されていないことから、
検知ホストへの影響は少ないと推察いたします。

■推奨事項（M365Defenderからの引用）：
Collect artifacts and determine scope
•Review the machine timeline for suspicious activities that may have occurred before and after the time of the alert, and record additional related artifacts (files, IPs/URLs)
（中略）

Microsoft社の推奨事項
が把握できる

以上となります。
よろしくお願いいたします。

M365セキュリティアラート調査について

調査を希望されるMicrosoft365製品のセキュリティアラートがありましたら、弊社に専用窓口にアラートメールを転送してください。

Script dropped and launched was detected by Microsoft Defender for Endpoint on [redacted]

Alert details

Title	Script dropped and launched
Severity	Medium
Category	Execution
Source	EDR
Detection time	[redacted] 23:59 UTC
Device name	[redacted]

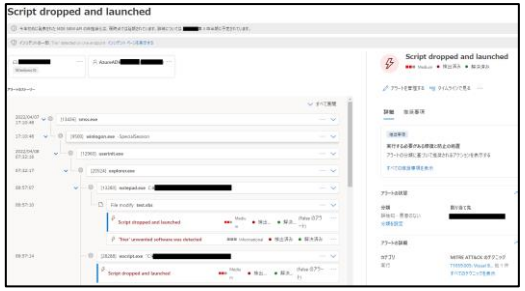
Alert page

View in Microsoft 365 Security Center >

View in Microsoft Defender for Endpoint >

Incident page

View in Microsoft 365 Security Center >



このアラートがどういう内容か分からない！

弊社がアラート内容を調査し、Microsoftの推奨事項とともにご報告します。
※MSに確認が不要：SLO 4時間
※MSに確認が必要：2～3営業日

株式会社[redacted]
[redacted]様

平素お世話になっております。
ソフトクリエイトアナリストチームです。

お問い合わせいただきましたアラートについて、
調査結果を以下にご報告いたします。

■検知イベント名：
Script dropped and launched
（スクリプトがドロップされて起動されました）

■検知イベント概要：
・発生日時：[redacted] 08:59
└ 検知数：4 件
①Script dropped and launched（3 件）
②'Trier' unwanted software was detected（1 件）

・デバイス名：[redacted]
・ユーザ：[redacted]
・検知ファイルパス：C:¥[redacted]

■検知イベント詳細：
スクリプトファイルがドロップされ、当該デバイスにて起動された際の挙動が検知されました。

上記の VBScript は、Microsoft Defender で、PC の動きを変更するような、望ましくないアプリの可能性があると判定されました。
（望ましくないアプリとは、ユーザーの十分な同意なしにインストールされ、コンピューターの動作を遅くさせたり、予期せぬ広告を表示させる等を行うアプリケーションカテゴリです。）

ただし、今回検知されたファイルは、マルウェア調査サイト VirusTotal で検出率「0/69」であるため、
既知のマルウェアである可能性は低いと考えられます。

■推奨事項（M365Defender からの引用）：
A. Validate the alert.
1. Review the alert and check the tool or process that dropped and launched the script file.
2. Check the device timeline for other suspicious activities.
3. Locate unfamiliar processes in the process tree. Check files for prevalence
4. Submi
5. Identif
ehaviors.

意味が分かったので、何をすべきか見えてきた！

対象製品

本サービスの調査対象は以下8製品です。

- Microsoft Defender for Endpoint P2
- Microsoft Defender for Bussiness
- Microsoft Cloud App Security
- Microsoft 365 Defender
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Endpoint Manager admin center
- Azure Active Directory

弊社他サービスとの棲み分け

弊社では、M365運用支援サービスとSOCサービスを提供しています。

M365運用支援サービス		外部SOCサービス
Microsoft365 安心サポート	Microsoft365安心サポート ＜Security＞	Security FREE
対応時間：平日9:00-18:00 サービス内容： M365の仕様や管理画面等での操作に関する質問に回答します	対応時間：平日9:00-18:00 サービス内容： M365とAADから通知されるアラートの調査とSecurity Centerの推奨事項を回答します	対応時間：24時間365日 サービス内容： Microsoft Defender for Endpointのアラートに対してSOCアナリストが対策を案内、脅威度に応じて端末を隔離します

詳細は次のスライドで説明します。

弊社他サービスとの棲み分け

提供サービス		M365運用支援サービス		外部SOCサービス
		安心サポート	Microsoft365安心サポート ＜Security＞	Security FREE
サービス提供時間		平日9:00～18:00	平日9:00～18:00	24時間365日
連絡(通知)手段		メール	メール	メール (ポータルサイト)
QA	操作方法	○	×	×
	製品仕様	○	×	×
	アラート見解	×	○	×
インシデント対応	調査範囲	問い合わせメールのみ	Security Center	Security Center
	ログ調査	×	○	○
	調査結果報告	×	○	○ (高リスク時は荷電)
	対処方法案内	×	○ (Security Centerの推奨事項)	○ (SOCアナリストの推奨事項)
	端末隔離	×	×	○
	相関分析	×	×	○
ポータルサイトの提供		×	×	○

もくじ

お客様が得られるメリット

こういったお悩みを解決できます

「アラートが出ているがどこを見れば良いか分からない」

「端末隔離まで実施するべきか分からない」

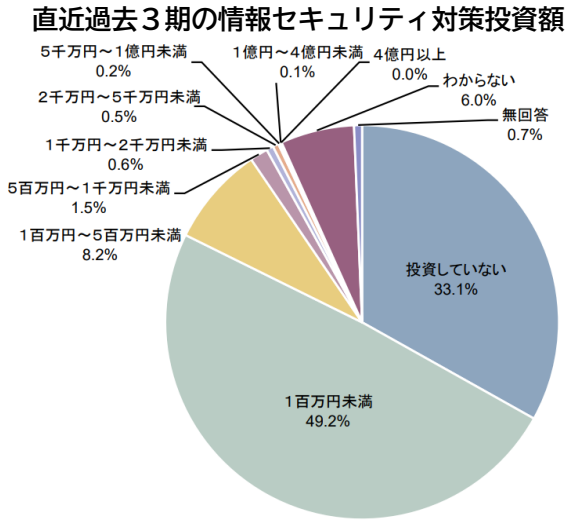
「アラート調査する工数・人員が足りない」

M365のアラートに対してセキュリティサービス部門が回答いたします

サービスのおすすめポイント

比較的お手頃な価格帯！

IPAの調査によると、日本の中小企業がセキュリティに投資する金額は「100万円未満」が最も多くなっています。

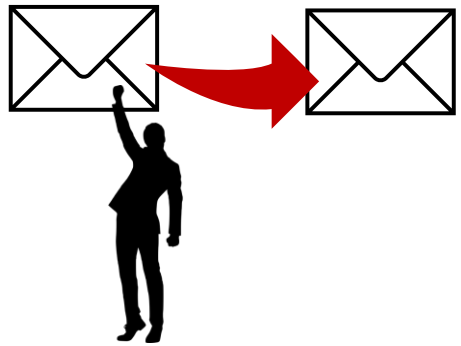


年間100万円以下に抑えられます。

https://www.ipa.go.jp/files/000097060.pdf

問い合わせ方法が簡単！

アラートメールをお問い合わせ窓口に転送していただくだけでOKです。



シンプルイズベスト。

M365運用の第一歩に！

M365を導入したが、アラート調査できるか不安だから支援してほしいという方にピッタリです。

また、将来、24h365dの監視を行いたくなった場合にはすぐにグレードアップもできます。

M365安心サポート
≪Security≫

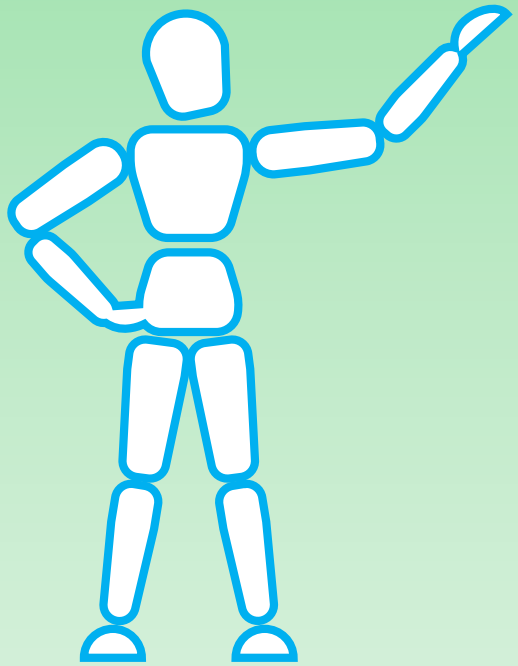
Security FREE

もくじ

さいごに

本セミナーに参加された方へ

リリースキャンペーン（先着１０社）



１回分のお試し券プレゼント

トライアル申込書を記載するだけ

本セミナーで伝えたかったこと

M365およびAzure ADを導入したけど…

管理画面の見方が分からない
アラートメールが来ても調べ方が分からない
アラート対応するための時間が足りない

こういったお悩みは解決できるので、
自社で抱え込まず、お気軽にお問い合わせください！

「安心」をあなたに。

Microsoft365安心サポート＜Security＞