NR Automate Security のご紹介

ネクストリード株式会社

Next Read

企業の皆様の “デジタル戦略策定とその実行” を支援しています。
現状分析を基にそれぞれのステージに合った最適な目標を設定、達成するために必要となる「つぎの足場」を考え、一歩一歩の活動をサポートします。

Strategy / Marketing

強みはどこにあるのか。どのようにデジタルを組み込み、優位性を形作るか。
本質的な課題を見極め、売上の向上につなげます。

Cloud Security

すべての企業に必須となった情報セキュリティ。
従来型のセキュリティとは一味違う、クラウド型モデルを提案します。

DX Development

データ・デジタル技術を活用し、日々の業務やビジネスモデルそのものを変革。
差別化と成長への基盤づくりを行います。

会社名	**ネクストリード株式会社** Next Read, Inc.
所在地	東京都港区六本木4丁目3番11号 六本木ユニハウス223号
取引銀行	三菱 UFJ 銀行 六本木支店
代表	**代表取締役　小国 幸司** Koji Okuni 外資系大手IT企業を経て、2016年からデジタル化推進やマーケティング活動の戦略・実行を支援するネクストリード株式会社を経営。大小さまざまな企業、プロジェクトの ”併走型” 支援を通じてデジタル化による業務改善や利益向上の実績を残す傍ら、総務省や厚生労働省、自治体などの「テレワーク推進」事業への協力など日本のテレワーク普及・推進活動にも尽力

NR Automate Security

【サービスの背景】

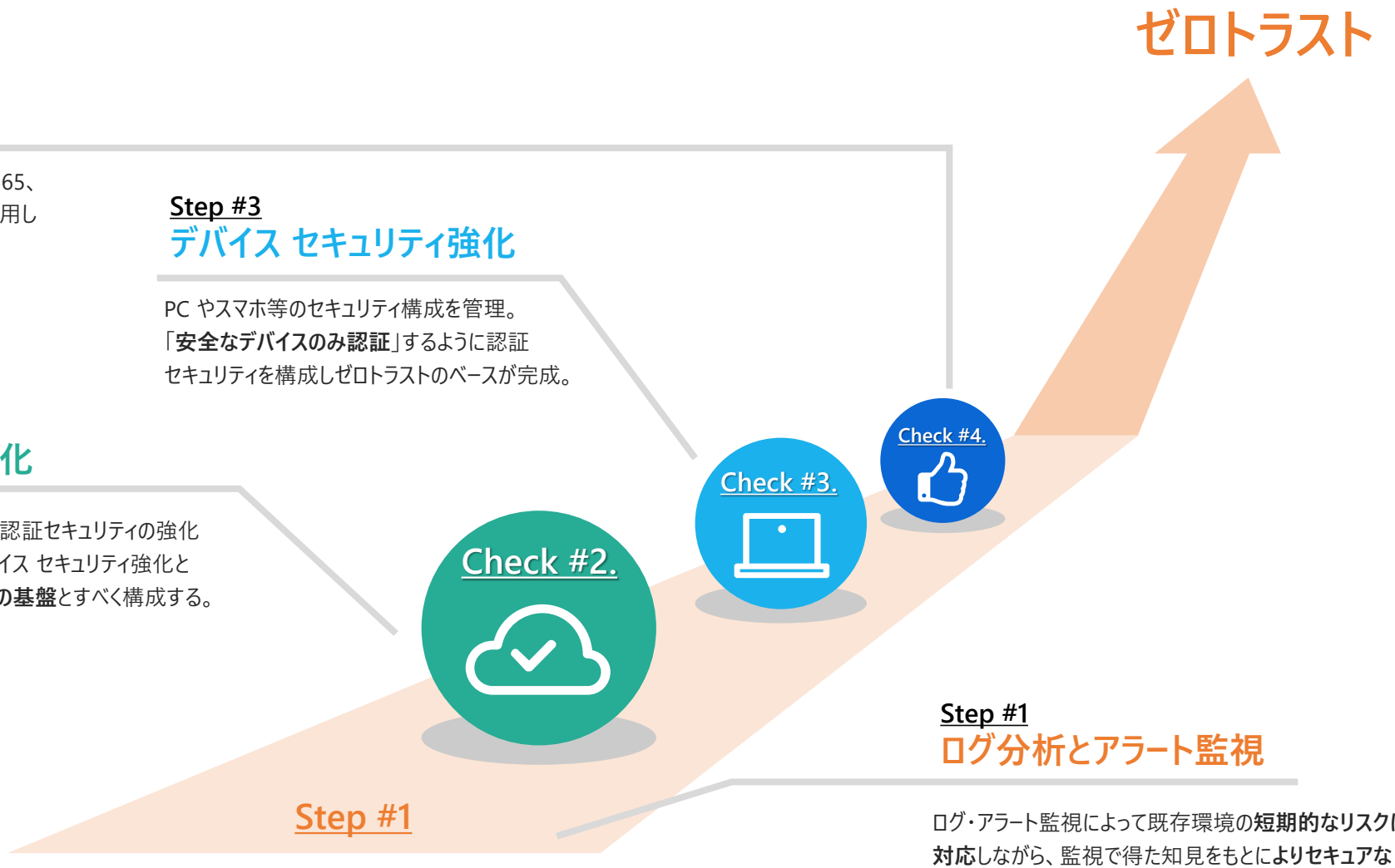
これまで弊社が DX を支援してきた多くのお客様で Microsoft 365 環境の**深刻なセキュリティ侵害**が見つかってきました。
社員数が数万人の企業だけではなく、数十人規模の企業であってもその傾向に変わりはありません。
全ての企業が脅威を正しく認識し、必要な対策を実施できるように、NR Automate Security の提供を開始しました。

【NR Automate Security とは】

全ての企業が安心して Microsoft 365 や他クラウド サービスを利用できるように、ネクストリードの脅威検出のスペシャリストが
アラート監視とログ分析による脅威検出を代行します。
脅威検出時にはネットワーク隔離やパスワード リセット等の**具体的な対応指示**をします。
また、監視運用で得られた情報をもとにセキュリティ向上 (攻撃面積最小化) のために実施すべき対策について、お客様担当者と
並走しながら中長期的なアドバイザリー (※) を実施します。

※アドバイザリーを行わずアラート対応に特化することで料金を抑えたプランもあります

監視サービスを越えたアドバイザリ サービス



Step #4
継続的なセキュリティ向上

セキュリティ トレンドや最新技術 (Microsoft 365、セキュリティ モデル、脅威インテリジェンス) を活用しながら、常に運用をアップデートし続ける。

Step #3
デバイス セキュリティ強化

PC やスマホ等のセキュリティ構成を管理。
「**安全なデバイスのみ認証**」するように認証セキュリティを構成しゼロトラストのベースが完成。

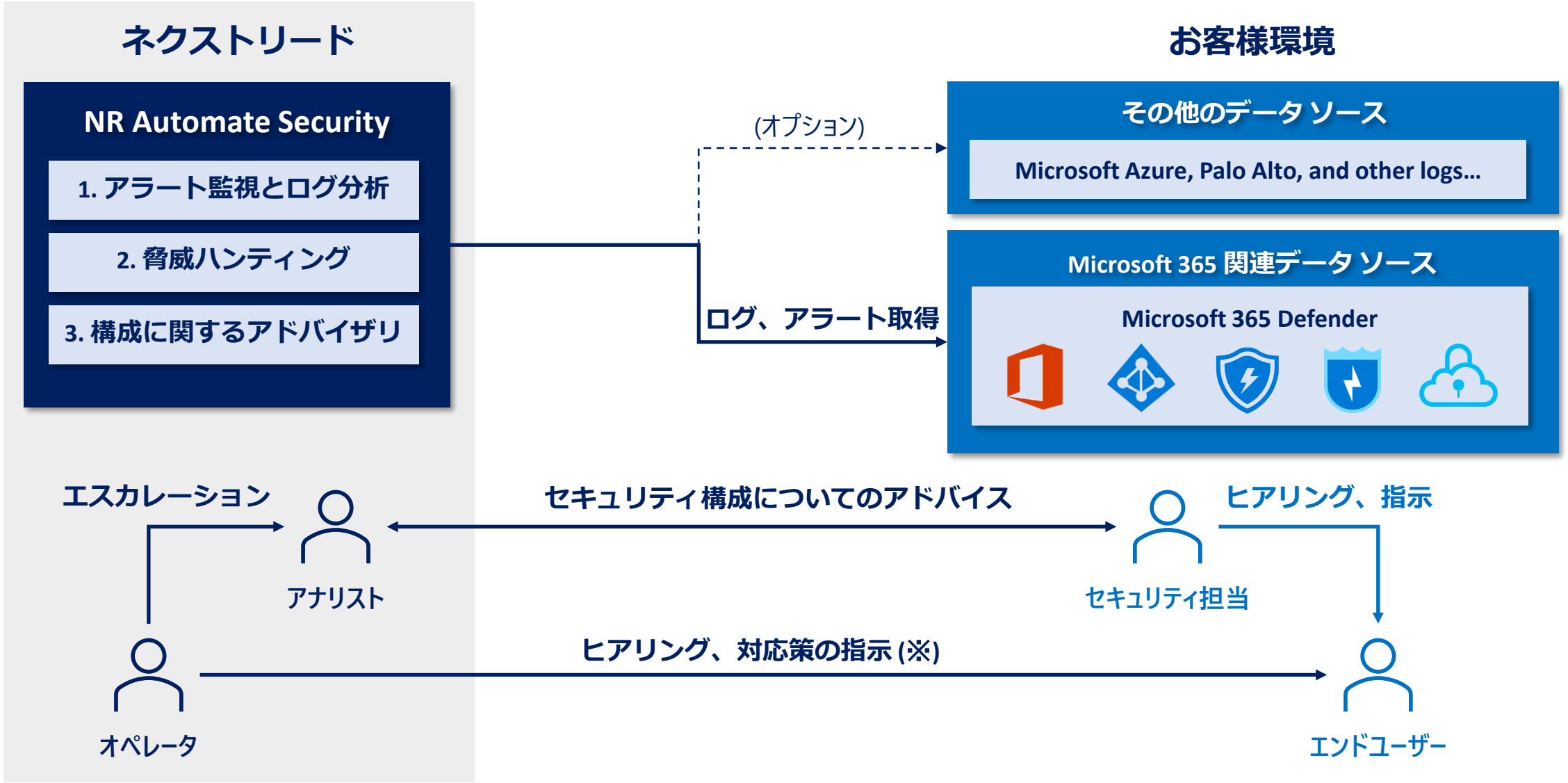
Step #2
認証セキュリティ強化

比較**導入しやすく効果が高い**認証セキュリティの強化を優先的に実施。後続のデバイス セキュリティ強化と合わせて、**盤石なゼロトラストの基盤**とすべく構成する。

Step #1
ログ分析とアラート監視

ログ・アラート監視によって既存環境の**短期的なリスクに対応**しながら、監視で得た知見をもとに**よりセキュアな構成を実現するための施策の優先順位を検討**する。

サービス構成イメージ



※エンドユーザーへの直接のヒアリングは Premium プランで選択可能

サービス プラン

		Premium	Standard	Basic
対象アラート	Azure AD Identity Protection アラート	○	○	○
	Microsoft Defender アラート	○	○	○
	カスタム ログ分析 (Microsoft 製品)	○	○	-
	カスタム ログ分析 (Microsoft 製品以外)	相談可 (追加費用)	-	-
サービス内容	アラート調査	○	○	○
	対応指示	○	○	○
	月次レポート	○	○	-
	構成アドバイザリー	月次ミーティング	レポート送付	-
	レスポンス (パスワードリセット、隔離等)	お客様指示により代行可	-	-
	運用のカスタマイズ	相談可 (追加費用)	-	-
連絡	連絡方法	Teams or メール	メール	メール
	連絡先	管理者 or ユーザー	管理者	管理者
価格	標準価格	490 円	330 円	250 円
	最低契約数	1,000	300	200

【補足】
・契約開始時の監視対象のユーザー数から月額を計算
・契約期間は 1 年で毎年の契約更新
・契約期間中に監視対象のユーザーが増加した場合は再計算となりますが、+10% までの増加分は次回契約更新まで猶予します
・お客様のご希望により通常とは異なる構成とする場合や、分析基盤へのログ取り込みで別途実費 (Azure VM や NW、ストレージ、Sentinel 等) がかかる場合があります

監視対象のアラートおよびログ

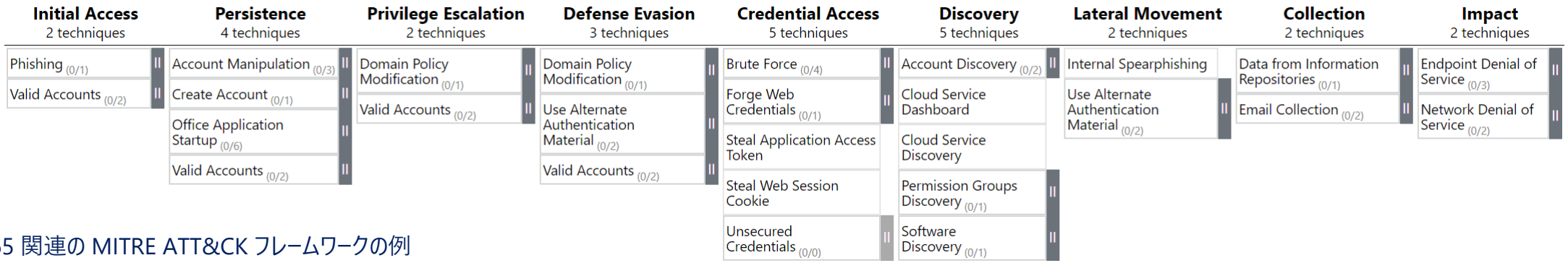
NR Automate Security の監視対象は大きく分けて「Microsoft 365 Defender のアラート」と「Microsoft 365 等のログ」に分けられます。
Microsoft 365 Defender のアラート監視を行うには別途ライセンスやポリシー設定等が必要です。(既に導入済みの場合を除く)
Microsoft 365 Defender を導入していない場合であっても、プランによってログから独自の分析ルールによりアラートを作成し、脅威を検出することができます。

種類	プロダクト	Premium	Standard	Basic	前提となる MS ライセンス	セットアップの主体
M365 アラート	Azure AD Identity Protection	○	○	○	単体ライセンス、または M365 E5 等の Suite ライセンス	**お客様自身が設定します** 設定の支援を希望される場合はご相談ください ライセンスを購入するだけで出力されるアラートもあります
	Microsoft Defender for Office 365	○	○	○		
	Microsoft Defender for Endpoint	○	○	○		
	Microsoft Defender for Identity	○	○	○		
	Microsoft Defender for Cloud Apps	○	○	○		
カスタム ログ 分析	Azure AD サインイン ログ	○	○		Azure AD Premium P1/P2	**ネクストリードが設定します** 独自の分析ルールを用いてログを分析することで アラートを生成します
	Azure AD 監査ログ	○	○		なし	
	Office 365 監査ログ (EXO/SPO/Teams)	○			なし	
	その他カスタム ログ (Palo Alto 等)	相談可			N/A	N/A

※上記ライセンスとは別に、調査用に Microsoft 365 E5 が最低 1 ライセンス必要です

カスタム ログ分析の領域

MITRE ATT&CK フレームワークの中で Azure AD や Office 365 の攻撃手法に着目し、それらの脅威を検知するための複数の検出ロジックを実装しています。
また、調査の中で新たに発見した脅威や攻撃トレンドに追随して検出ロジックをアップデートしています。



AAD/O365 関連の MITRE ATT&CK フレームワークの例

Tactic	Technique	Sub-technique	説明
Initial Access	Phishing	Spear phishing Link	ソーシャルエンジニアリングによりメール内のリンクをクリックするように誘導する
Persistence	Account Manipulation	Additional Cloud Credential	Azure AD にサービスプリンシパルを登録する
		Add Office 365 Global Administrator Role	Azure AD 全体管理者ロールにアカウントを追加する
		Exchange Email Delegate Permissions	メールボックスに追加の権限を付与する
Privilege Escalation	Domain Policy Modification	Domain Trust Modification	Azure AD の信頼済みドメインを追加したり、フェデレーションの設定を変更したりする
Credential Access	Brute Force	Credential Stuffing	Web サービスの侵害により漏えいした資格情報で Azure AD にサインインする
		Password Spraying	一般的に使用されるパスワードを使用してサインインを試行する
	Forge Web Credentials	SAML Tokens	SAML トークン署名証明書を入手して SAML トークンを偽造する
	Steal Application Access Token		悪意のあるアプリケーションからのアクセスに同意させることで OAuth アクセス トークンを盗む
	Steal Web Session Cookie		Cookie を盗んで不正にサインインする
Discovery	Account Discovery	Cloud Account, Email Account	Azure AD ユーザーや Email のリストを取得する
	Permission Groups Discovery	Cloud Groups	M365 管理者ロールと管理者を検索する (Get-MsolRole 等)
Collection	Data from Information Repositories	SharePoint	ポリシー、ネットワーク図、アーキテクチャ図、内部リソースへのリンクなどの情報をマイニングする
	Email Collection	Email Forwarding Rule	電子メールの転送ルールを設定する

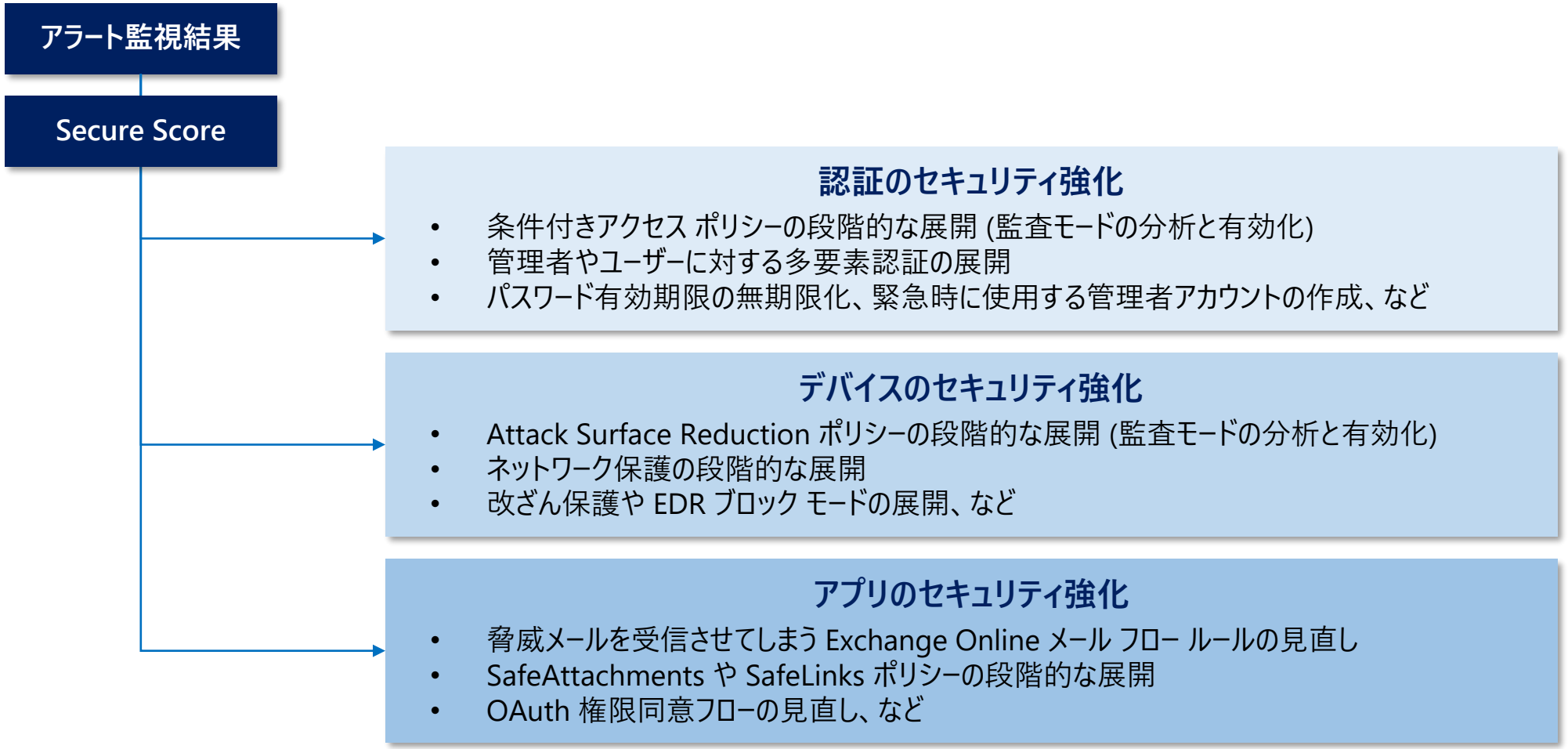
カスタム ログ分析ルール例

Office 365 ログ、Azure AD ログを分析するカスタム ルールの例です。(現時点で 30 程度あり、新しい脅威の発見により拡大していきます)
複数の分析ルールによる監視で Microsoft 365 に対する攻撃でよく使用される手法を見逃さず、攻撃が侵攻する前に封じ込むことを目指します。

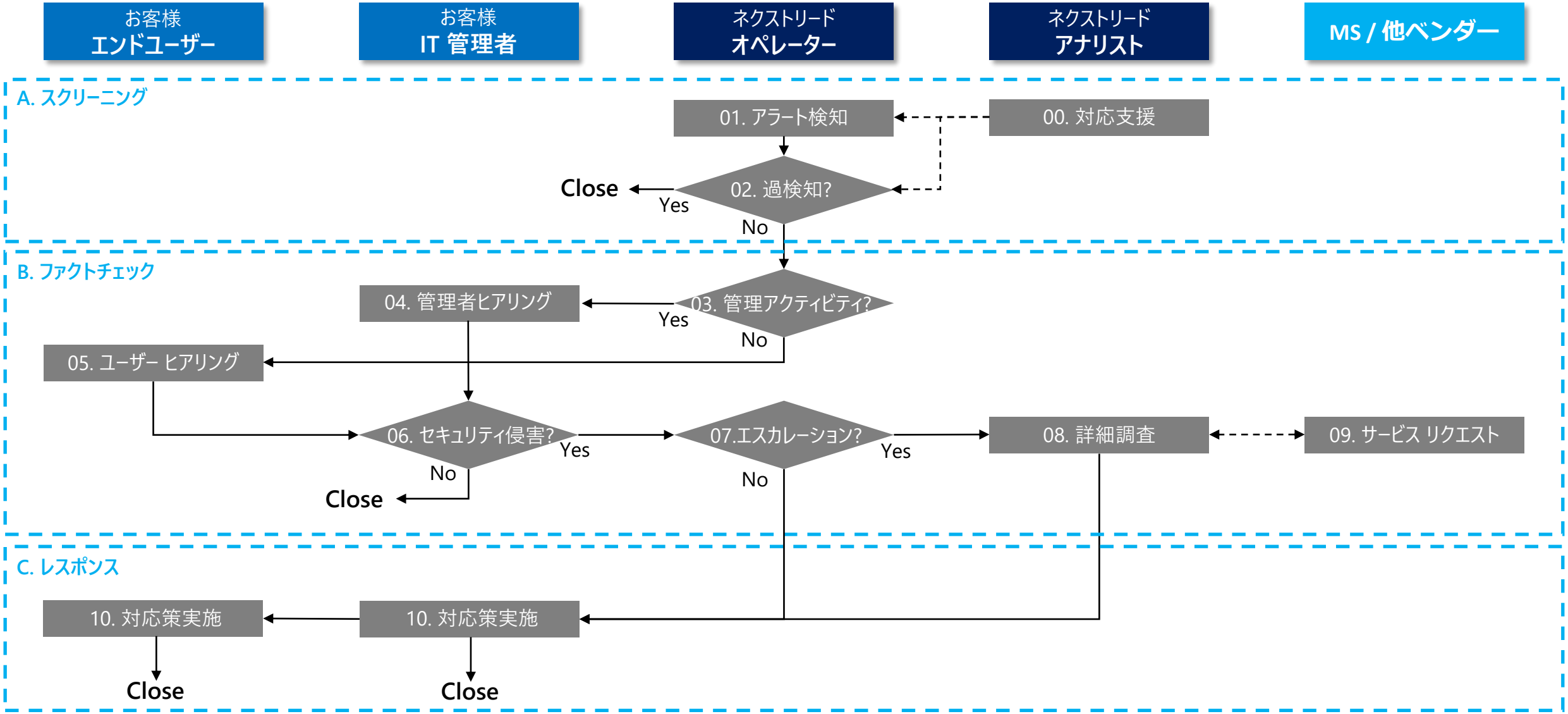
カテゴリ	分析ルール	説明
O365 ログ	SPO 共有ポリシーの変更	SPO の共有設定 (外部共有を可能にする変更など) の変更を検出
	MDO 脅威ポリシーの変更	EXO 脅威ポリシー (フィッシング検出、トランスポートルール等) の無効化や削除を検出
	攻撃ツールの検出	匿名化、ネットワークスキャン、リモート管理等の攻撃で使用されるツールを検出
	リスクがあるアクティビティ	リスクがあるサインインと評価された IP アドレスからの Office 365 アクティビティを検出
	匿名リンクの使用	匿名リンクの作成や一般的ではないユーザー エージェントからのアクセスを検出
	メール転送ルールの設定	メール転送ルールの設定を検出
AAD 監査ログ	ドメイン設定の変更	フェデレーションやドメインの認証関連の設定変更を検出
	管理者の追加	管理者の追加を検出
	OAuth 権限同意	主にメールに対する OAuth 権限 (読み取り、送信) の委任を検出
AAD サインイン ログ	ブラックリスト IP からのサインイン	ブラックリストに指定された IP アドレスからのサインインを検出
	複数の国からのサインイン成功	過去にサインインが成功した実績がない複数の国からのサインイン成功を検出
	リスクがあるサインイン	Azure AD がリスクを検知したサインインを検出
	PowerShell からのサインイン	PowerShell による EXO および AAD への接続を検出
	クラウド プラットフォームからのサインイン	Azure、AWS、GCP からのサインインを検出
	不審なユーザーエージェント	一般的ではないユーザー エージェント (Bot、クローラー等) からのサインインを検出

構成アドバイザリー

監視で得られた知見や Microsoft Secure Score の情報をベースに、より強固なセキュリティを実現するために実施する施策の優先度を決定。
業務影響を最小限にしながら Microsoft 365 のセキュリティ機能を展開するための並走型支援を実施。



アラート監視・対応フロー



※エンドユーザーへの直接のヒアリング (上記の 05) は Premium プランで選択可能

サービス提供までの流れ

NR Automate Security のサービス提供までの流れは下記の通りです。

1. **お問い合わせ**
   - NR Automate Security にご関心がある場合は contact@nextread.co.jp までご連絡ください
2. **脅威可視化アセスメント実施 (希望される場合)**
   - Microsoft 365 の現状の脅威を可視化するアセスメント「脅威可視化アセスメント Light」を実施 https://nextread.co.jp/nrassessment/
3. **お打ち合わせ (アセスメント結果の共有、サービスの説明など)**
   - アセスメント開始後、3 週間から 4 週間後を目途にアセスメント結果の報告会を実施
   - 上記の報告会と合わせて、NR Automate Security (監視サービス) の説明も実施
4. **お申込み、ご契約**
   - 監視対象のユーザー数やご希望を伺いお見積もり
   - 本申し込み後、ご契約
5. **サービス提供開始**
   - 合意した開始時期に基づき監視を開始

サービス提供条件

NR Automate Security のサービス提供条件は下記の通りです。

- **対応時間**
  - オペレーターによる連絡は平日 9:00-18:00 (脅威検出は 24 時間 365 日)
- **対応場所**
  - フル リモートでの対応
  - 連絡方法はメール、チャット等 (キックオフの打ち合わせで決定)
- **SLA**
  - アラート出力後 4 営業時間以内のアラート スクリーニング
    ※スクリーニング後の調査により "早急な対応が必要" と判断した場合のみオペレーターより連絡します
- **その他**
  - ネクストリード アナリスト/オペレーターが使用する 1 アカウントに対して全体管理者権限を付与いただきます
  - Microsoft 365 E5 ライセンスが少なくともテナントに 1 ライセンス必要です

NR YOROZU for Security

【NR YOROZU とは】

ネクストリード契約者 (デジタル化・データ設計、セキュリティ、マーケティングなど) 限定でオプション契約可能な「よろず相談」サービスです。
内容が複雑、切り分けに時間がかかる、メーカーへの問い合わせにも工夫が必要・・など悩みがちな課題をワンストップで対応します。

利用シナリオ実例

- 現在の環境を踏まえたサービスの使い方のポイントをアドバイスしてほしい
- ベンダー サポートを利用したが回答の意味が分からず、カウンターのメッセージを作成してほしい
- Azure の複数のサービスを利用していて問題が発生しているが、切り分けを支援してほしい

【NR YOROZU for Security とは】

NR Automate Security をご契約のお客様限定で、セキュリティに関するご相談が可能な NR YOROZU のミニ プランです。
20 万円/月をオプションとして契約に追加することで、**10 時間/月までエンジニアにセキュリティに関連するご相談が可能**です。

利用シナリオ実例

- 脅威メールが多く着弾しているので Microsoft Defender for Office 365 のポリシーをアセスメントしてほしい
- アラート内容の意味が分からないので分かりやすく説明してほしい
- セキュリティ強化施策を行っていく予定だが、プライオリティや進め方について意見交換したい

お問い合わせ

Next Read

contact@nextread.co.jp