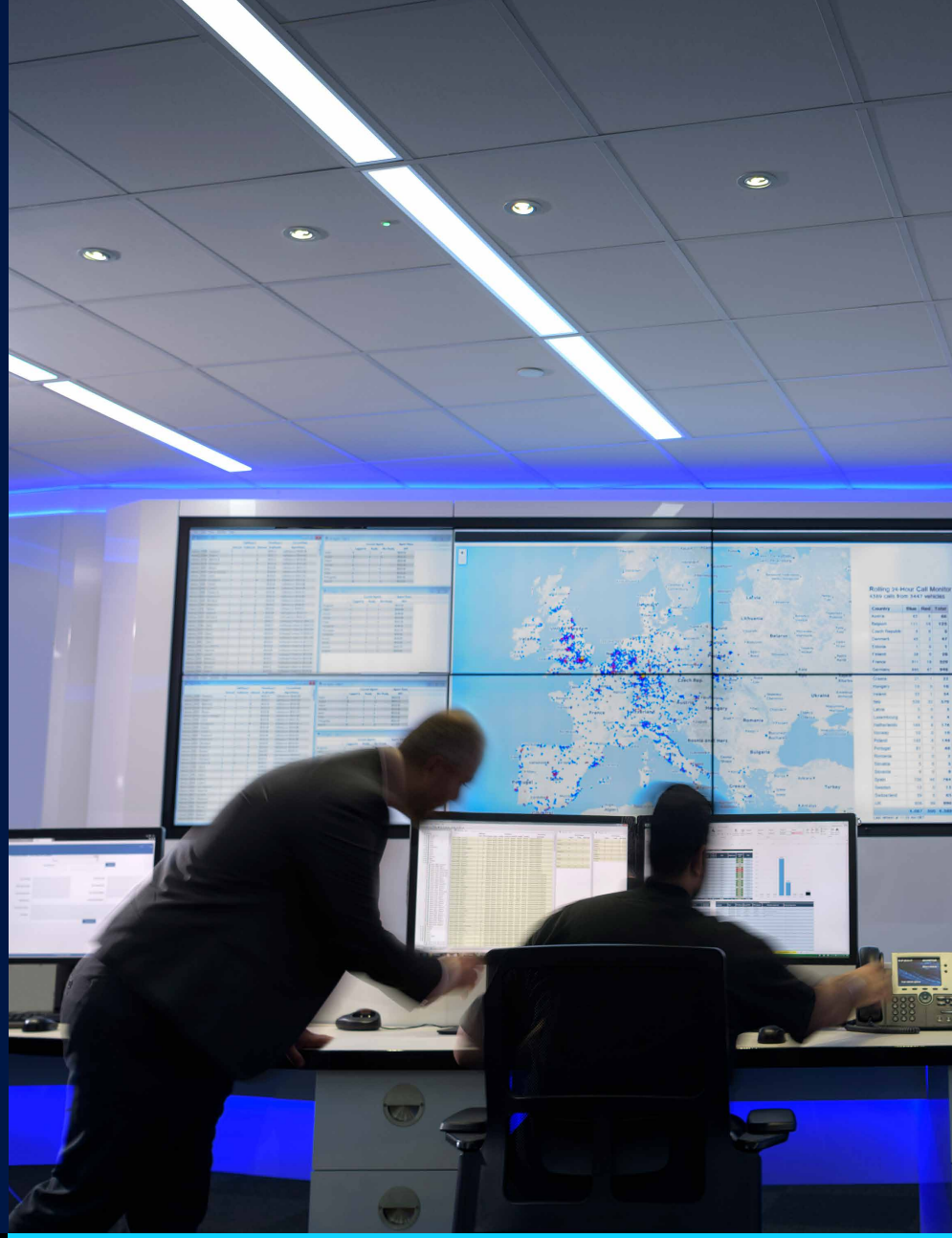
デセプションの実例

Zscaler Deception が検出した実際の脅威トップ 10



デセプションを活用したアクティブディフェンスで標的型攻撃を阻止

デセプションは、通常の防御をすり抜ける人為的な攻撃をあぶり出す最も効果的な手法の一つです。攻撃者の戦術を妨害し、ミスを誘発することで、脅威を的確に検知します。

Zscaler Deception プラットフォームは、攻撃者が組織の環境内でどのように行動するかを予測する戦略を基に設計されており、この仕組みによって、世界中の組織に影響を及ぼす深刻な脅威の検出を可能にしています。

本書では、Zscaler の世界規模のデコイ ネットワークで検出された主な攻撃例を紹介します。

検出された実際の脅威トップ 10

01 北朝鮮の APT 攻撃
02 人為的なランサムウェア攻撃の初期活動
03 内部偵察とスキャン活動
04 クレデンシャル スタッフィング攻撃
05 MikroTik ルーターへの攻撃活動
06 分散型総当たり攻撃
07 X 線装置のコントローラーへの侵害
08 MedusaLocker ランサムウェアの拡散
09 ランサムウェアを早期に警告
10 シャドー RDP

実例 1

世界的な複合企業を標的とした北朝鮮の APT 攻撃

インシデントの詳細

デコイに対する SMB ポート スキャンを検知

- Zscaler Deception が NTLM ユーザー名を取得
- 調査結果から、このユーザーが侵害されていたことが判明

トリアージと調査

- 正規のドメインと類似する C2 ドメインを確認
- 既知のシグネチャーがない 2 つの DLL を特定
- DLL にはハードコードされた認証情報と、コマンドを受信するためのローダー コードが含まれていたことが判明
- 担当部門の調査により、北朝鮮の「Hidden Cobra」というグループが仕掛けた標的型攻撃であることを特定

デセプション戦略

- 攻撃される可能性が高いインフラの重要部分を特定し、そのエリアにデコイを配置
- Zscaler Threat Hunting を通じて、エンドポイントの調査とトリアージをさらにサポート

結果

- Zscaler Deception だけが環境内でアラートを発信した

ポイント

環境の制約と目標に合わせてカスタマイズされたデセプション戦略は、アクティブ ディフェンスを成功させるための重要な要素です。

実例 2

小売業者を狙ったランサムウェア オペレーターの初期活動を検知

インシデントの詳細

デコイ サービス アカウントがペイシェント ゼロの不審な動作を検知

- 2021 年 5 月 8 日、あるシステムが Active Directory デコイ内のサービス プリンシパル名 (SPN) レコードをスキャン

ペイシェント ゼロが SMB 経由でラテラル ムーブメントを実行し、デコイに移動

- 2021 年 5 月 13 日、NTLM 認証により SYSTEM アカウントの侵害が判明

ランサムウェアが WinRM 経由で拡散

- 2021 年 6 月 10 日、デコイがポート 5985 でのポート スキャンを確認

2021 年 6 月 13 日、ランサムウェアが WinRM 経由で展開

- 不十分な対応により、ネットワーク内で複数のサーバーがランサムウェアに感染

デセプション戦略

- アカウント侵害を検出するために Active Directory デコイを設置
- ラテラル ムーブメントを検出するために DC および DMZ 内にネットワーク デコイを設置

結果

- Zscaler Deception は、ランサムウェア攻撃が発生する 1 か月前に攻撃の予兆を検知し、アラートを発信した

ポイント

Active Directory デコイは、ランサムウェア攻撃の兆候を特定して警告する最も信頼できるツールの一つであるため、セキュリティ部門には、これらを優先して調査することが求められます。

実例 3

大手金融機関で発生した内部偵察とスキャン活動

インシデントの詳細

攻撃者が侵害されたルーターを通じてネットワーク内に侵入

- 侵害されたルーターを使って、SSH など複数のポートでデコイと広範囲にやり取りし、偵察活動を実行

攻撃者は 3 つの SSH デコイで数百のコマンドを実行し、6 時間以上にわたり活動

- root/root でログイン
- 状況を把握するためのコマンドを実行
- カスタム ネットワーク スキャナーのバイナリーを作成しようとする試み
- /etc/passwd および /etc/shadow からパスワードを取得しようとする試み
- デコイを踏み台として利用しようとする試み (ブロック)
- TCPDump を使用してネットワークを監視しようとする試み

デセプション戦略

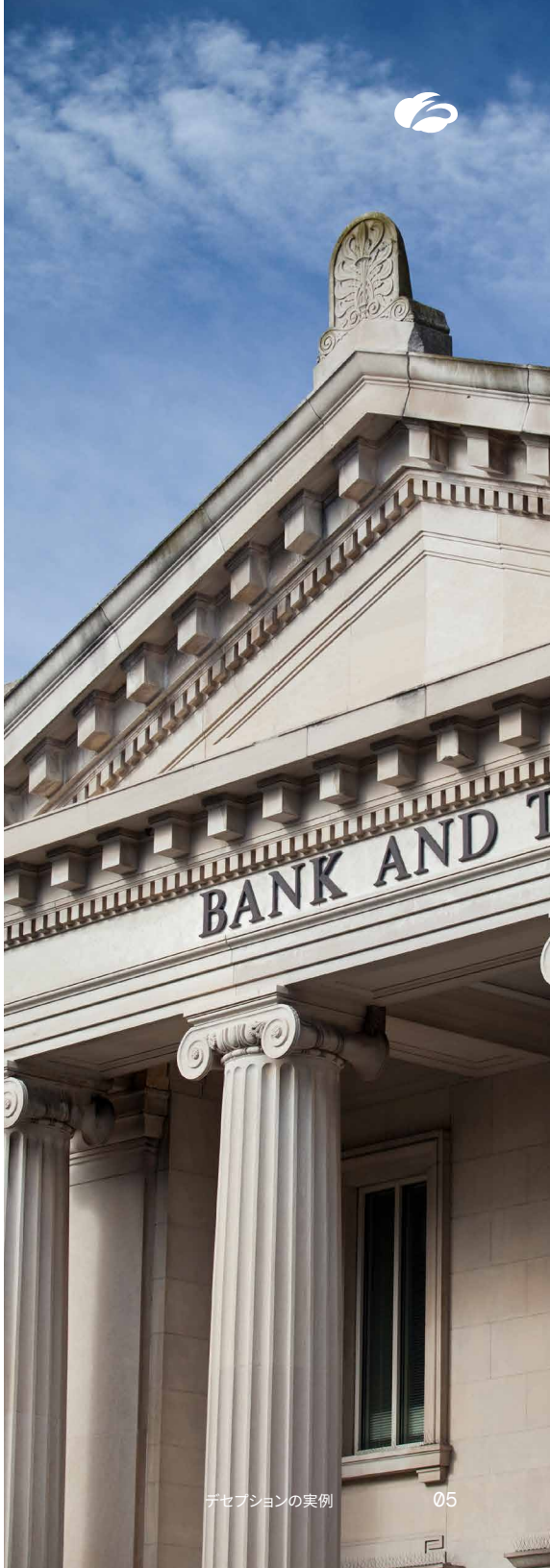
- 攻撃者を検知するだけでなく、その戦略や目的が明らかになるまで引き付け、封じ込める高インタラクション型のネットワーク デコイを使用

結果

- 攻撃者がデコイを調査している間に、組織は侵害されたルーターを特定してセキュリティを確保し、さらなる被害を防ぐことができた

ポイント

人為的な攻撃はターゲットの防御戦略を分析し、従来の検出制御を避ける特徴があります。この事例では、通常 EDR がインストールされていないルーターが標的にされました。セキュリティ部門は、このようなデバイスを模倣したデコイを設置し、高度な攻撃者を早期に検知する必要があります。



実例 4

重要な顧客を抱える法律事務所へのクレデンシャル スタッフィング攻撃

インシデントの詳細

インターネット経由でアクセス可能な Citrix デコイがクレデンシャル スタッフィングに関するアラートを発信

- 200 以上の侵害されたドメイン認証情報がデコイに送信
- 攻撃はロシアのクラウド サービス プロバイダーのインフラから開始

対応と封じ込め

- オーケストレーション機能を活用して、ファイアウォールのブロック リストをリアルタイムで更新
- デコイを踏み台として利用しようとする試み (ブロック)
- TCPDump を使用してネットワークを監視しようとする試み

デセプション戦略

- 認証情報のテストを試みる攻撃者が標的としやすい、インターネット経由でアクセス可能なアプリを模倣したデコイを設置
- マネージド脅威ハンティング サービスを活用

結果

- Zscaler Deception は、攻撃者の注意をデコイに向けさせることで本番環境の資産を保護し、キル チェーンの初期段階で攻撃を阻止した

ポイント

リモート アクセス サービスやアプリケーションのゼロデイ脆弱性または既知の脆弱性を模倣した、インターネット経由でアクセス可能なデコイを活用すれば、攻撃の初期段階での侵害を阻止できます。

実例 5

MikroTik ルーターへの攻撃活動

インシデントの詳細

カスタムの MikroTik SSH デコイがアラートを発行

- 8291/tcp、8728/tcp、22/tcp (SSH) などの既知の MikroTik RouterOS ポート上のデコイでスキャンを実行
- GO ベースのツール (SSH-2.0-Go) を使用してカスタム デコイの SSH サービスとやり取り
- 認証情報を標的とした総当たり攻撃を試行
- 状況を把握するためのコマンドを複数実行
- インターネットから取得して実行するようにスケジュールされたタスクを作成

デセプション戦略

- 環境で利用されている特定のコンポーネントを模倣したデコイを設置

結果

- 攻撃の発生源が特定され、積極的に封じ込められた
- ログを細かく調査することなく、認証情報やコマンドといった重要なデータに即座にアクセスできたため迅速な対応が可能になった

ポイント

デセプションは、その信ぴょう性とリアリティに大きく依存します。攻撃者をおびき寄せるには、本物を巧妙に模倣し、十分な機能性を持つデコイが必要です。今回のケースでは、SSH デコイが攻撃者を混乱させ、使用されたツールと C2 サーバーの特定を成功させました。

実例 6

大手金融機関を狙った総当たり攻撃

インシデントの詳細

境界デコイが複数の総当たり攻撃を検知

- 攻撃は複数の発信源から発生
- デコイへの攻撃試行には、悪用されやすいデフォルトの認証情報の組み合わせが使用されていることが判明
- タイムスタンプから、攻撃者が BurpSuite と Nuclei Scanner を使用して Web アプリケーションを手動で悪用していることを特定

対応と封じ込め

- オーケストレーション機能を活用してファイアウォールのブロック リストをリアルタイムで更新し、認証情報を送信する発信源をブロック
- 攻撃の発信源は、攻撃から 3 日が経過した時点で初めて脅威インテリジェンスに記録

デセプション戦略

- リモート アクセス アプリケーションやその他のサービスのゼロデイ脆弱性または既知の脆弱性を模倣した、インターネット経由でアクセス可能なデコイを設置
- マネージド脅威ハンティング サービスを活用

結果

- 戦術に基づき複数の発信源をブロックする機能を活用することで、影響を抑制した

ポイント

Zscaler が提供するインターネット経由でアクセス可能なデコイは、従来の脅威インテリジェンス フィードでは見逃されがちな独自のプライベート脅威インテリジェンスを生成し、差し迫った攻撃に即座に対応するための信頼性の高い早期警告システムとして機能します。

実例 7

病院を標的とした人為的な標的型攻撃

インシデントの詳細

APT グループに関連する PsExec のような動作をデコイで確認

- 発信源は X 線装置のコントローラー
- DCE/RPC プロトコルを使用してデコイのサービス制御マネージャーにアクセスし、サービスを開始 (PsExec の動作)
- ラテラル ムーブメントに使用される一般的なポート (135、445、3389) を複数のデコイでスキャン
- RemCom RemoteAdmin というリモート アクセス ツールを検出
- 調査により、Mimikatz のようなツールが使用されていることが判明

デセプション戦略

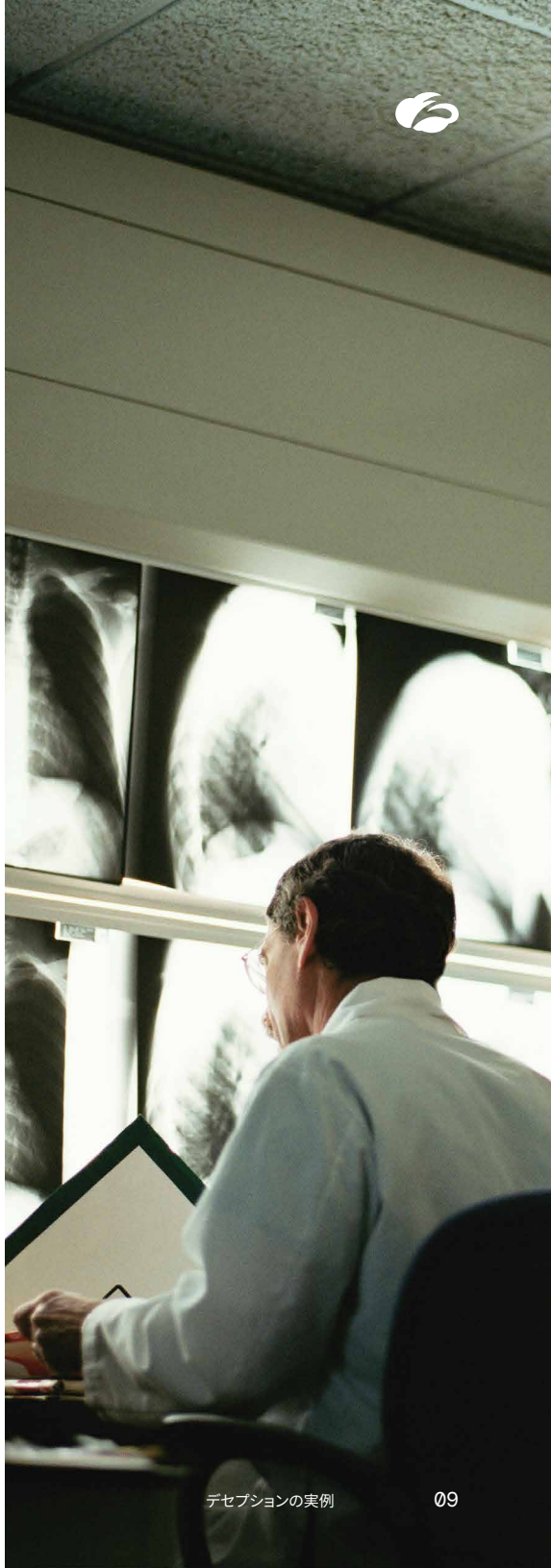
- 病院の重要な医療機器があるエリアにデコイを戦略的に設置
- デコイに誘導するエンドポイント ルアーを配置

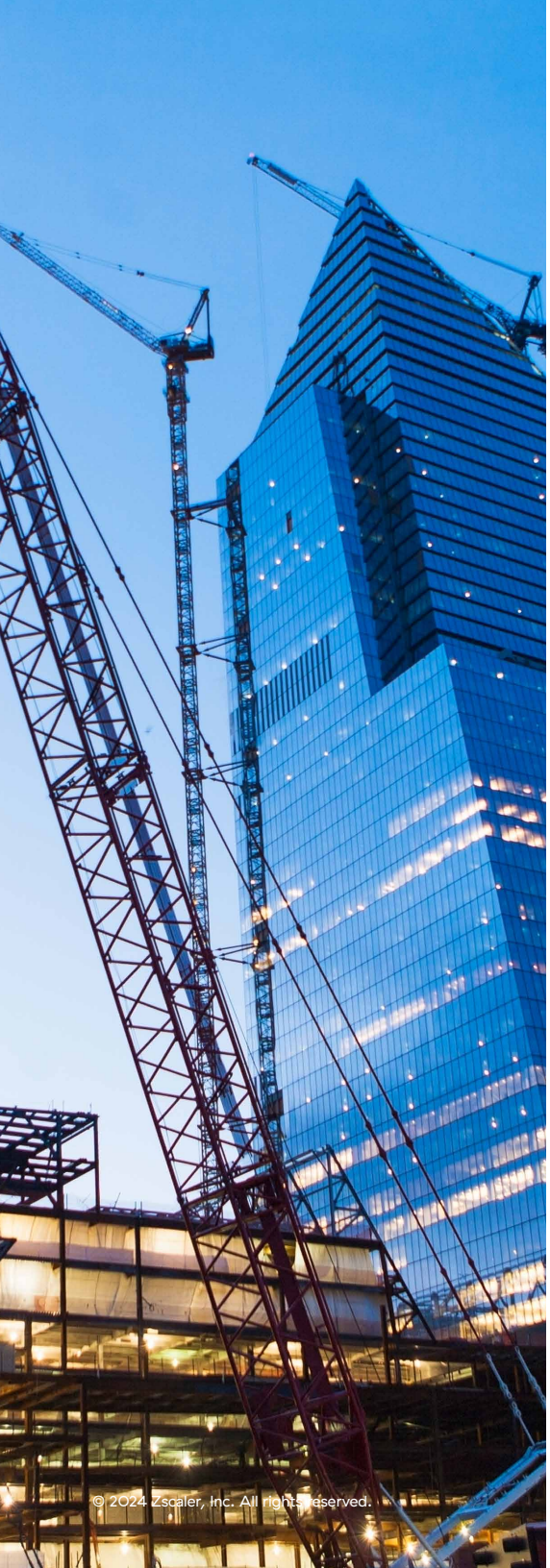
結果

- 標的型攻撃のタイムリーな検出と封じ込め

ポイント

従来の脅威検出ツールを導入できない病院機器や IoT デバイス、POS システムには、デセプションを活用した防御が非常に効果的です。





実例 8

複合企業で発生した MedusaLocker ランサムウェアの拡散

インシデントの詳細

デコイのファイル共有が暗号化されたことを示すアラートが発信

- 50 以上の発信源がデコイの SMB 共有にアクセス
- デコイのファイル名が「.ReadInstructions」という拡張子に変更
- 取得されたユーザー名は特権アカウントに属していることが判明

デセプション戦略

- ランサムウェアのユース ケースに特に関連するアクティビティーを監視するため、重要なセグメントに SMB 共有型デコイを設置

結果

- 侵害されたサーバーを迅速に隔離し、ランサムウェアの拡散を最小限に抑えた

ポイント

少数のデコイであっても大きな効果を発揮する可能性があります。大規模展開が難しい場合でも、デコイを戦略的なエリアに設置すれば期待以上の成果が得られます。

実例 9

侵害の予兆を早期に警告

インシデントの詳細

グローバル製造企業において、侵害された特権アカウントを使用してデコイにアクセスされたことを示すアラートが発信

- 発信源が複数のデコイ共有にアクセス
- 使用された NTLM ユーザー名は ThreatParse ルールを使用して解析され、特定のキーワード (adm、svc、bkp など) を基に特権アカウントの可能性があることが判明
- アカウントは侵害されたドメイン管理者であることを確認

デセプション戦略

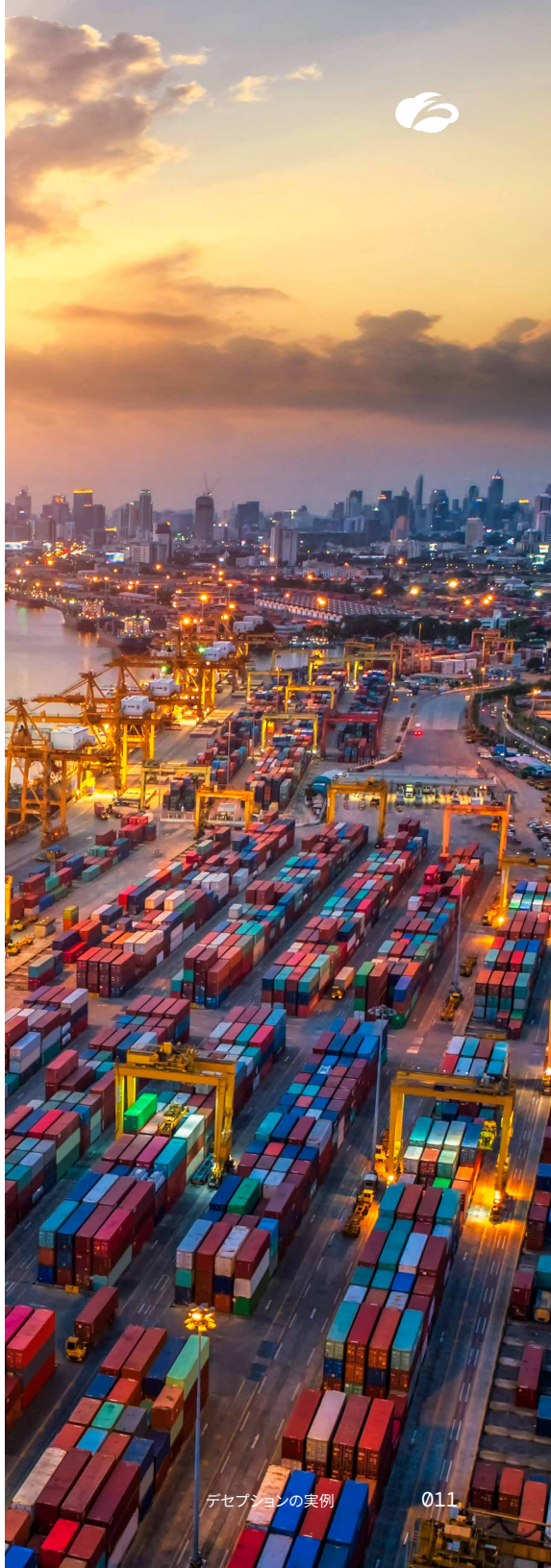
- 制約のある環境下でも、Active Directory やエンドポイント ルアーを使い攻撃者をデコイに誘導
- 特定のデコイに対する動きに合わせたカスタム ルールと電話アラートを設定

結果

- Zscaler Deception は、FBI がダーク Web で収集した情報に基づいて別途発令した警告より 1 週間早く、ランサムウェアの活動を検知した

ポイント

環境に制約がある場合でも大きな成果を得られます。従来の検出制御は広範囲での展開が求められますが、デセプションは限定的な適用範囲であっても目標達成に大きく寄与します。



実例 10

FMGC 企業で検出されたシャドー RDP

インシデントの詳細

デコイ ユーザーに対するログオン試行の失敗を検知

- デコイ アカウントへのログオンが繰り返し失敗
- Windows ログを解析したものの、発信源の特定には至らず
- 認証の流れを追跡する根本原因分析 (RCA) を顧客とともに実施
- インターネットに公開された RDP がある Azure システムを特定

デセプション戦略

- 共通辞書に含まれる名前を使用して AD デコイ ユーザーを作成

結果

- 初めての特殊な検出事例として成功
- 重大なビジネス リスクを生む可能性がある設定ミスを特定
- このケースから得られた知見を活用して、マネージド サービスを利用する他の顧客においても同様の問題を 3 件特定し、迅速に対処

ポイント

デセプションは攻撃者の意図を基に攻撃を検知するため、従来のシグネチャーやヒューリスティックなどの従来の手法では見逃されがちな未知の脅威を効果的に特定できます。

デコイは長年使用されてきたセキュリティ戦略の一つですが、その機能と役割は今日のデジタル世界の課題に対応するために進化を遂げています。動的で戦略的、そして秘匿性の高いデコイは、脅威を軽減する手段としてだけでなく、貴重なインテリジェンスを収集するためのツールとしても活用されています。このインテリジェンスは即座に Zscaler のセキュリティ クラウドに統合され、全体的な防御を強化します。

デコイを使ったセキュリティ対策の詳細については、こちらをご覧ください：
zscaler.com/jp/products/deception-technology

Zscaler について
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SASE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、www.zscaler.com/jp をご覧ください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/jp