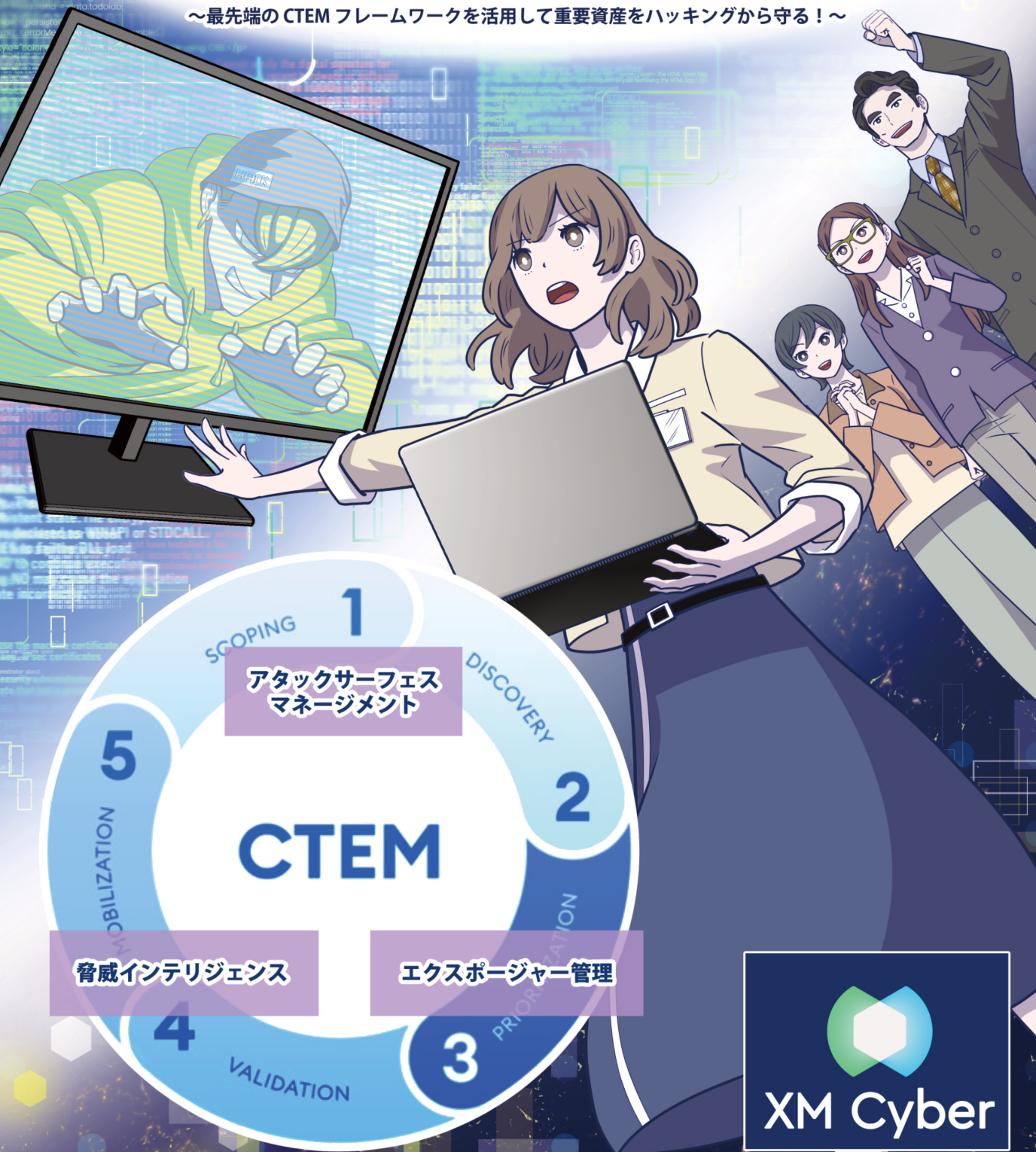
XM Cyberが実現する
包括的な予防型セキュリティ

～最先端のCTEMフレームワークを活用して重要資産をハッキングから守る！～



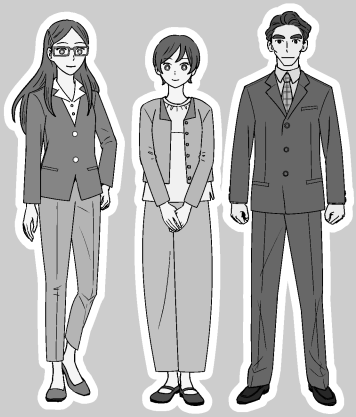
登場人物

●主人公

総合商社 フォーカス商事 情報セキュリティ課 所属。
セキュリティの最新動向に関心が高く、
自社の環境に危機感を抱いている。

●ハッカー

金銭を目的として、企業へのハッキングを
繰り返すプロハッカー。
様々なハッキング手段に精通している。



●大手工業

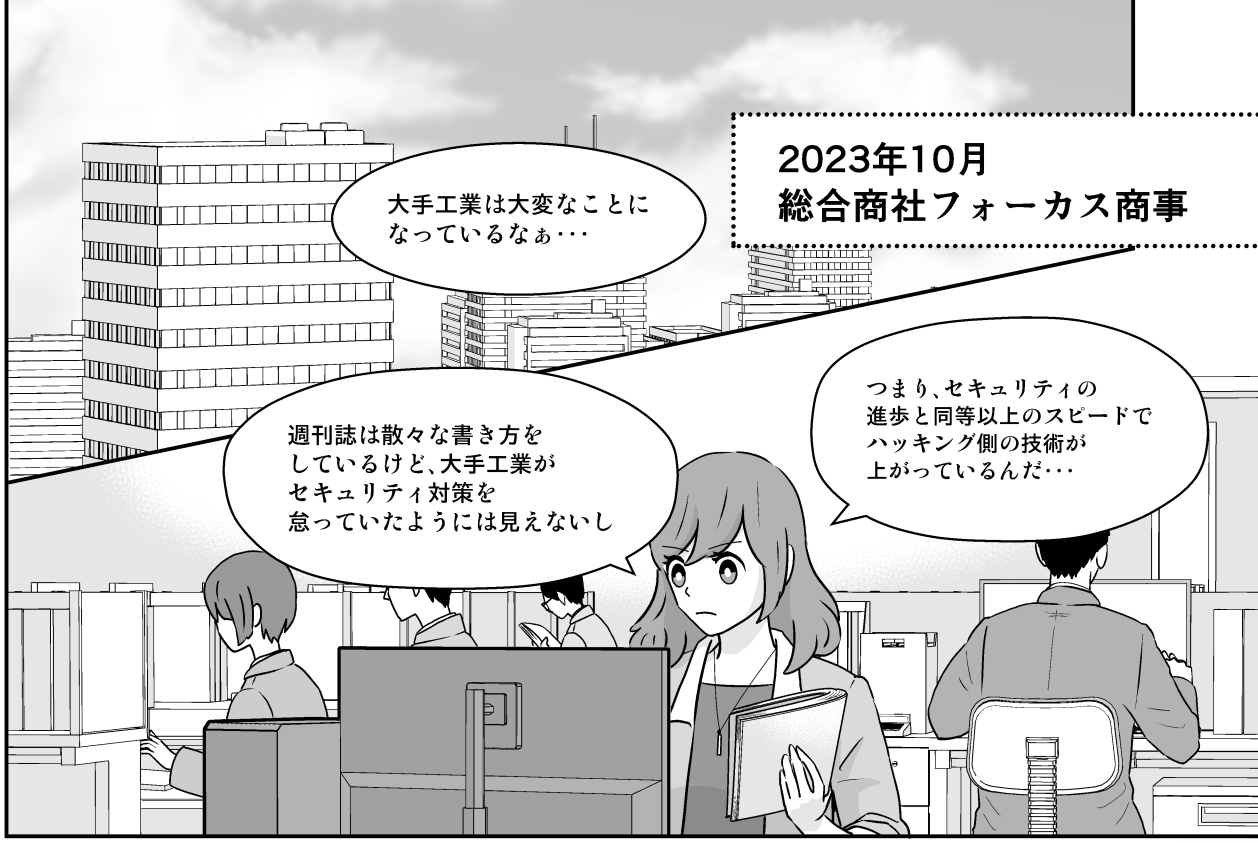
東証へ上場している製造メーカー。
セキュリティ対策に力を入れており、
自社でホワイトハッカーを雇うほど。

背景

企業のあらゆるデータがネットワークに繋がることで、サイバー犯罪の標的となるリスクが格段に上がっている。増え続けるクラウドサービスやデバイスは到底管理しきれず、企業が気付かずに放置されているセキュリティホールが無数に存在する。
2024年。このような環境で、とある企業がハッキングの危機に晒されていた。
果たして企業は重要データを守り切ることができるのか……。

2023年7月
上場企業　大手工業


おお、これが今回の
レポートか
お疲れさま
report
演習とわかっていても
毎回ヒヤヒヤします
地道にやって
いくことが
大事だからな
とはいえペネトレーションテストを
行うことで、一つずつ改善しているよ
ペネトレーションテスト：擬似的にハッキングをかけることで
実際の侵入を受ける前に対策するセキュリティ手法
た、大変です！
顧客データに
不正アクセス
されました！
落ち着いてくれ
今回のテストは
終わったばかり
だろう？
違います！本当に
データが盗まれたんです！
なんだって！？
WEEKLY
BUSINESS
徹底追求
流出疑惑の真実!?
ずさんなセキュリティ？
大手工業が陥った落とし穴とは…
関係者極秘インタビュー
「脆弱性を適切に管理されていなかった」
事件発生から１ヶ月後も
被害の全容見えず
Central NEWS
速報
特集
経済
エンタメ
スポーツ
【速報】大手工業、顧客データが流出！？



Newsroom

プレスリリース

Gartner、2024年のサイバーセキュリテ
トップ・トレンドを発表

ガートナージャパン株式会社（本社：東京都港区、以下Gartner）は、2024年の
のトップ・トレンドを発表しました。本トップ・トレンドの推進要因には、ジェ
セキュリティ意識の低い従業員の行動、サードパーティのリスク、継続的な脅威
でのコミュニケーション・ギャップ、セキュリティに対するアイデンティティ・
6つが挙げられます 。
シニアディレクターアナリストのリチャード・アディスコット（Richard Addis
います。「生成AIは、対処すべき新たな課題としてセキュリティ・リーダーを悩ま
を活用することで、オペレーション・レベルでセキュリティを強化する機会とな
すべき不可避の勢力となりましたが、セキュリティ・リーダーには、自分たちが
外的要因はほかにもあり、それらにも引き続き対処しなければなりません」
2024年は、組織のレジリエンスやサイバーセキュリティ部門のパフォーマン
入れて、幅広いプラクティス、技術的機能、構造改革をセキュリティ・プログラム
セキュリティ・リーダーがこれらの外的要因による複合的な影響に対処するよ
の6つのトレンドは、これらの領域にわたり、幅広い影響をもたらします。
バイスプレジデントアナリストの儀田優一は次のように述べています。「これら
においても重要な論点になりますが、各トレンドの及ぼす影響や優先順位は各
で成熟度が高くない組織においては、ここに挙げた6つ以外に優先させるべき取
もある点には留意が必要です。一足飛びに高いレベルに到達することは不可能
リーダーは、各トレンドに対して短中長期的な視点から議論し、戦略的ロードマ
あります」
トレンド1：生成AIに対する短期的な懐疑論と長期的な期待の高まり
ChatGPTやGeminiのような大規模言語モデル（LLM）アプリケーションは、生成

1週間後

会議中

時代の背景

拡がり続ける
アタックサーフェス

コロナ禍に浸透したリモートワークや
クラウド利用により
攻撃を受けるリスク箇所が拡大

サイロ化された
セキュリティ対策

クラウド、エンドポイント、
ネットワークなどの個々の対策では
攻撃の全体像がわからない

膨大な修正リスト

根拠の弱い、脆弱性リストだけでは
設定ミスやクレデンシャルなど
を含めた優先順位付けができない

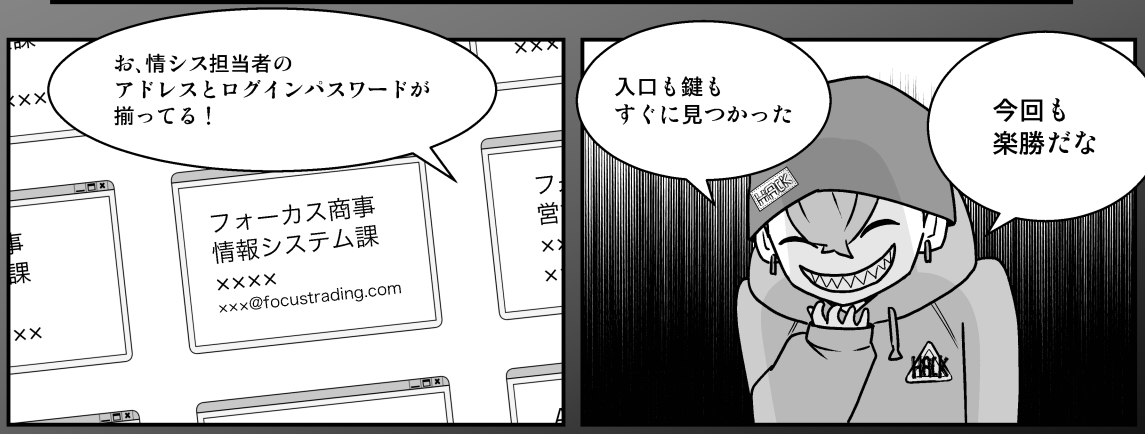
そこで
我が社が導入するべき
最先端のソリューションを
紹介します

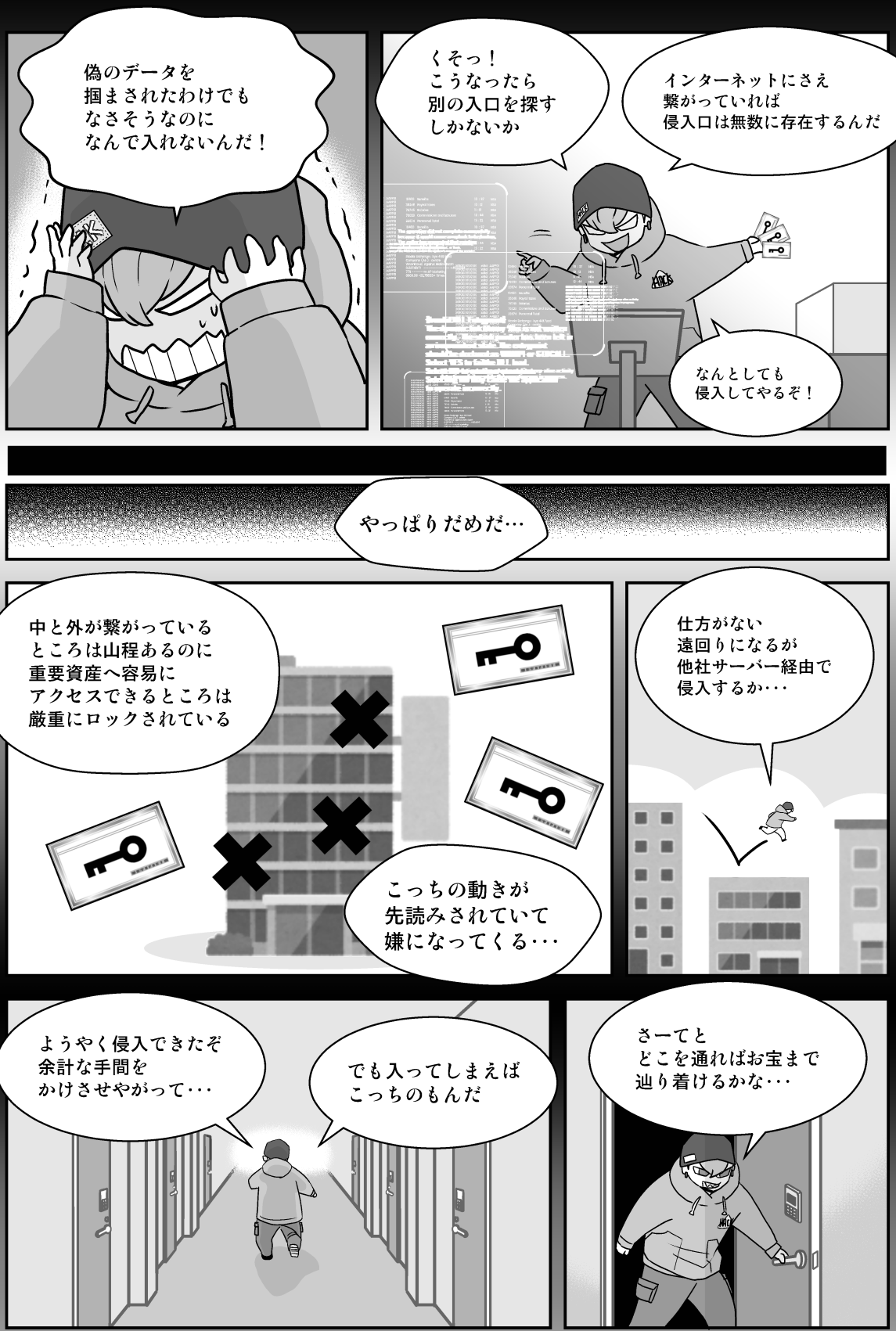
【サイバーキルチェーン／ハッキングの 7ステップ】

1. 偵察(Reconnaissance)：標的となる個人、組織を調査する。例えば、インターネット、メール情報、組織への潜入等が挙げられる。
2. 武器化(Weaponization)：攻撃のためのエクスプロイトキットやマルウェア等を作成する。
3. デリバリー(Delivery)：マルウェアを添付したメールや悪意あるリンク付きメールを仕掛ける。また、直接対象組織のシステムへアクセスする。
4. エクスプロイト(Exploitation)：標的にマルウェア等攻撃ファイルを実行させる。または、悪意あるリンクにアクセスさせ、エクスプロイトを実行させる。
5. インストール(Installation)：エクスプロイトを成功させ、標的がマルウェアに感染する。これでマルウェア実行可能となる。
6. C&C(Command & Control)：マルウェアとC&Cサーバーが通信可能となり、リモートから標的への操作が可能となる。
7. 目的の実行(Actions on Objectives)：情報搾取や改ざん、データ破壊、サービス停止等、攻撃者の目的が実行される

※ここからはイメージで
お送りします。

ダークウェブ：
通常の方法ではアクセスできないようになっており、非合法な情報やマルウェア、麻薬などの取引の温床となっている。




偽のデータを
掴まされたわけでも
なさそうなのに
なんで入れないんだ！
くそっ！
こうなったら
別の入口を探す
しかないか
インターネットにさえ
繋がっていれば
侵入口は無数に存在するんだ
なんとしても
侵入してやるぞ！
やっぱりだめだ…
中と外が繋がっている
ところは山程あるのに
重要資産へ容易に
アクセスできるところは
厳重にロックされている
こっちの動きが
先読みされていて
嫌になってくる…
仕方がない
遠回りになるが
他社サーバー経由で
侵入するか…
ようやく侵入できたぞ
余計な手間を
かけさせやがって…
でも入ってしまえば
こっちのもんだ
さーてと
どこを通ればお宝まで
辿り着けるかな…


くそ
また開かない！
Error
途中までは上手くいくのに
お宝が近くなると急に
セキュリティレベルが
高くなっている
Error
素人じゃ存在にすら
気付かないはずの裏道まで
念入りにロックされているし
通れる道はいくつもあるのに
ゴールだけには辿り着けない！
これじゃ答えのない迷路だ！
合鍵は使えない！
出入り口が塞がっている！
侵入できても重要なルートは
肝心なところで途切れている！
こっちの手口が
全て読まれていて
何も上手くいかない
じゃないか！
いつまでもこんな会社に
付き合っていられるか！
もうやめだ！

2023年10月

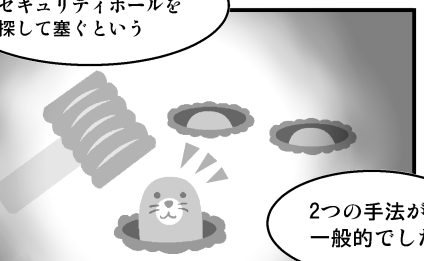
CTEM

具体的な手段を
ご紹介する前に

皆さんは“CTEM”
という言葉を
ご存知でしょうか

従来のセキュリティは
侵入を受けてから事後的に
被害を食い止めるか

前もって場当たり的に
セキュリティホールを
探して塞ぐという



2つの手法が
一般的でした

ですが、ガートナーが提唱する
CTEMは考え方が異なります

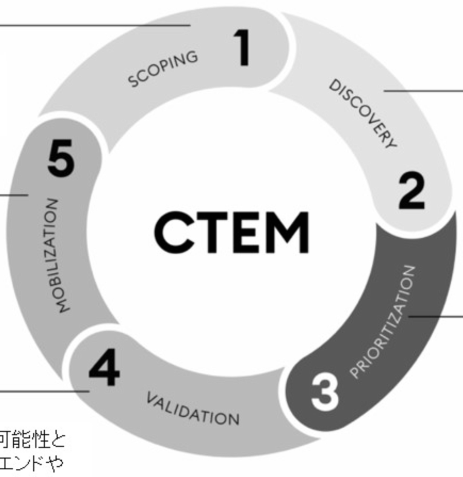
脆弱性や設定ミス、
クレデンシャルなどを
網羅的に予防します

5つのステップで
セキュリティホールを
可視化、評価、優先順位付け、
検証、対策します

これらは継続的かつ
事前に行われるので

これまでは難しかった
効率的な予防策を実現します

Continuous Threat Exposure Management (CTEM)



スコーピング

脅威の状況と重要資産に対する
攻撃シナリオのスコープ決め

ディスカバリー

ハイブリッドクラウド環境におけるCVE、
ミスコンフィグ、クラウド、アイデンティティ
リスクの発見

動員

IT 改善ガイダンス、チケット管理、
進捗管理により、セキュリティリスク
に対するチームを動員

優先順位付け

サイバー脅威の優先順位付けと、
重要資産への攻撃経路のマッピング

検証

重要資産への潜在的な攻撃可能性と
到達可能性を検証し、デッド・エンドや
チョーク・ポイントを特定

XM Cyberは、全ステップでご支援
特にステップ2、3、4を自動化

続いて、**CTEM**を
実現するための
具体的なアクションを
3つ紹介します

エクスポージャー管理
Continuous Exposure Management

最も重要なのは
侵入ルートを
事前に塞ぐことです

サイバー犯罪は侵入経路が
非常に見えにくく

一度でも侵入を許すと
内部で様々な侵入ルートを
構築されます

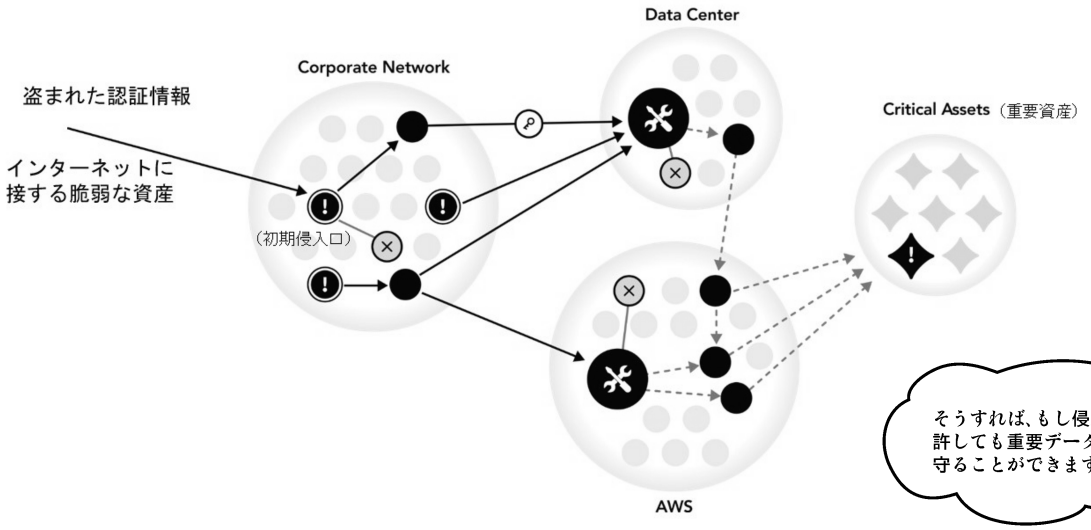
しかし、セキュリティホールや
その繋がりを可視化すれば

より多くのルートに
繋がりやすいポイントを
優先的に対処できます

オンプレとパブリッククラウドの
外部攻撃サーフェスから組織全体の
セキュリティ・エクスポージャーを
継続的に発見

すべてのエクスポージャを全体
的な攻撃経路にマッピングさせ、
攻撃される可能性(Exploitability)
と影響を分析・評価

複数の攻撃経路の「チョーク・ポイント」
を特定し、効率的に重要資産を保護
するための修正ガイダンスを得る



そうすれば、もし侵入を
許しても重要データは
守ることができます

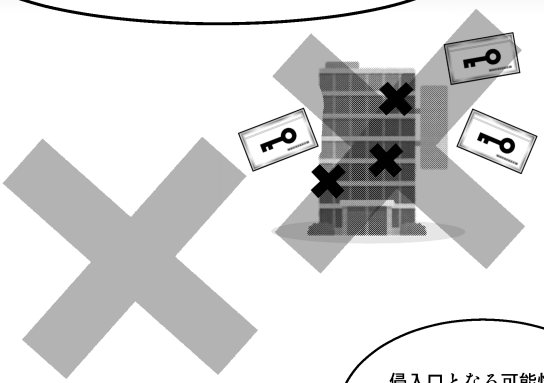
脅威インテリジェンス
Exposed Credential Management

その準備として
脅威インテリジェンスによって
ダークウェブを巡回し、企業の
情報流出の有無をチェックします

もし流出している
パスワードなどを発見したら
ハッキングに使用できるのか
テストし、“合鍵”の存在や
有効性を事前に確認します

アタックサーフェスマネジメント
External Attack Surface Management

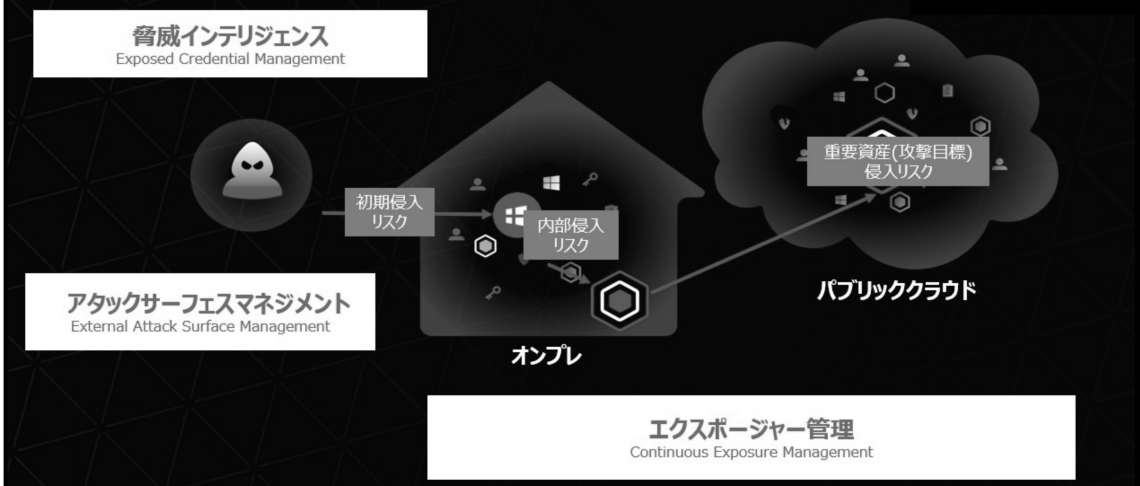
また、アタックサーフェスマネジメントによって
通常では把握が難しい侵入口を可視化します



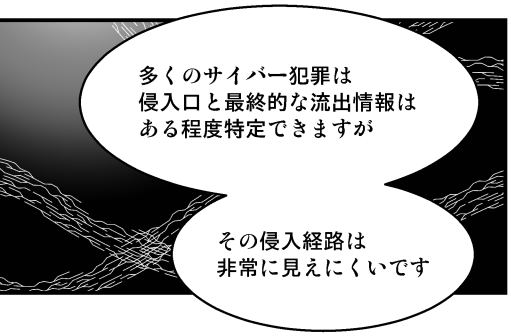
企業が把握していない
外部接点は
鍵が付いていないドアの
ようなものです

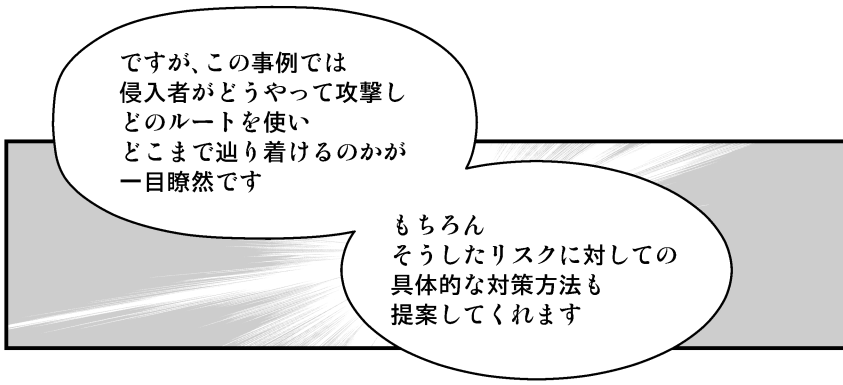
侵入口となる可能性の
あるドアを把握し
前もって施錠することが
重要なのです

XM Cyberの製品イメージ



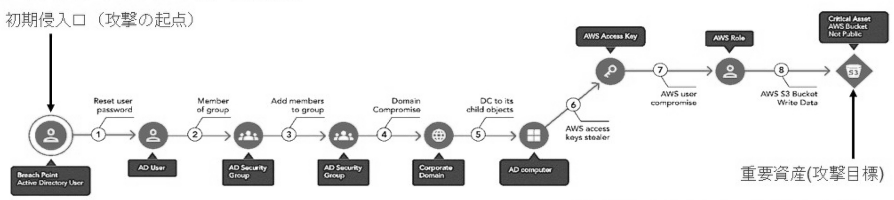
© XM Cyber 2024



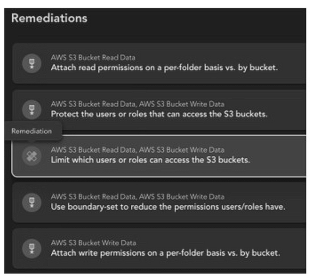


攻撃プロセスを可視化し、修正方法をご案内

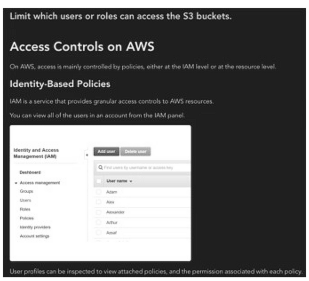
①攻撃プロセスを可視化



②複数の修正方法をご提示（解決策、緩和策）



③修正方法をより丁寧にご案内



XM Cyber ～CTEM支援プラットフォーム～

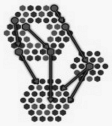
4. 再評価しセキュリティレベルをスコアリング
継続的に組織全体のセキュリティ状況を解析
数値で見える化し、最新の状況を確認

1. 複合的なリスクを検出
組織内のエクスポージャーを洗い出し
リスクがどこに潜むかを特定

CTEM
with
XM Cyber

3.修正方法を具体的にご案内
優先順位に応じた修正箇所に対し、
修正方法をマニュアルレベルでご案内

2. アタックパスにより優先順位づけ
効率的にラテラル・ムーブメントを遮断できる
踏み台地点や、重要資産への経路を特定



4 © XM Cyber 2024 XM Cyber

XM Cyberで実現できること

1. 膨大な脆弱性・セキュリティ課題の管理工数削減
2. ハイブリッドクラウド環境のセキュリティ強化・重要資産堅牢化
3. マルウエア対策・ランサムウエア対策の強化
4. サプライチェーン対策の強化
5. ホワイトハッカーの熟練の視点をもった、システムのリスク診断

XM Cyber

お問い合わせはこちら

xm.japan@xmcyber.com