サイバーセキュリティの人的側面

最悪のシナリオを想像してみてください。

高度なランサムウェア攻撃によって、データセンター全体が稼働を停止しました。セールス、カスタマー サービス、財務は、業務を遂行できません。あなたはシニアITリーダーとしてシステムの復元を任されていますが、解決策を見出すことに苦慮しています。

かねてから人員が不足していたチームは、休憩も休暇もほぼない状態で何週間も働き続けています。睡眠を取らずに**36時間も連続で対処にあたっている**実務担当者もいます。あなたは疲労が判断力の低下を招き、リカバリー作業そのものを危険にさらす可能性があることを懸念し始めています。

すぐに問題解決に参加し支援してくれる追加のリソースを切実に必要としていますが、どこを探せばよいのでしょうか。

小説の冒頭のようなこのシナリオは、Dellのお客様の実体験に基づいています。ここには、今日のサイバーセキュリティ環境において大きな課題となっている「人的要素」が如実に表れています。

最近のデータによると、この業界では約500万人のセキュリティ プロフェッショナルが不足しています。リソースの必要性が最も深刻に感じられるのはインシデント発生時ですが、その解決策が始まるのは、はるか上流です。

人材パイプラインの構築と育成から始める

必要なリソースを確保するための最初のステップは、次の方法で人材パイプラインを構築することです。

新卒採用活動とインターンシップ

地元の大学や専門学校との連携により、若手人材を安定的に確保できます。こうした人材は、時間をかけて育成することで、影響力の高いチーム メンバーになり得ます。

継続的なトレーニングと能力開発

時間と予算が常に逼迫する中でも、サイバーセキュリティ担当者は、ツールと脅威の両方の変化に対応する必要があります。

人材定着への注力

優秀な実務担当者、特に攻撃を回避した経験がある人材は、需要が高くなります。優秀な人材を引き留めることができなければ、他社に奪われます。

強力なチームであっても、攻撃を乗り切るためのストレス管理は不十分な場合があるため、必要になる前に追加のサポートを特定して、事前に計画を立てておきましょう。

サードパーティー リソースの評価

サイバーセキュリティのコンサルティングとスタッフ増強サービスを提供する企業は、継続的な運用時もインシデント発生時も、お客様のチームを支援できます。今は不要でも、こうした企業との関係を構築しておくと、必要なときにそれらのリソースにアクセスできます。

Dellは、仮想CISO (vCISO)、インシデント対応、サイバーセキュリティ アドバイザリーなど、既存のチームを強化できる多くのサービスを提供しています。

AIの利用

ログ分析、異常検出、低レベル アラートのトリアージ、専門的なトレーニングなど、サイバーセキュリティ ツールに組み込まれつつある新しいAI機能を活用して、リソースのギャップを解消し、運用ニーズに対応すれば、チーム メンバーは優先度の高いタスクに専念できる可能性があります。

リソースの課題はサイバー攻撃発生時に最も深刻化する

最初のシナリオが示すように、大規模なサイバー攻撃が起きると、組織は機能不全に陥り、主要なシステムと事業運営が麻痺する可能性があります。1分1秒が会社の経済的損失につながり、問題解決にあたるサイバーセキュリティ チームは莫大なプレッシャーにさらされることになります。

チームをできる限り最新化しておくことは、インシデント対応とそれに伴いチームが抱えるストレスに直接影響します。

従業員は最初の防衛線であるため、トレーニングは、セキュリティ担当者だけでなく、全従業員を対象に実施する必要があることに注意してください。

この事例は、サイバー防御の担い手が結局は人間であるという、核心的な課題を浮き彫りにしています。人には限界があり、その限界を超えると、どれほど優秀なプロフェッショナルでも失敗する可能性があります。精神的疲労、ストレス、バーンアウトは、サイバーセキュリティ体制において軽視できない要素です。

この課題に対する単一の解決策はおそらく存在しませんが、次の戦略は大きな効果をもたらす可能性があります。

強力なチームと人材パイプラインの構築
この課題に対する最も根本的な解決策は、非常事態の発生を回避することであり、冗長性を備えた強力なチームを構築することです。

攻撃に対する人的側面の計画
インシデント対応計画は極めて重要です。スタッフの管理、スケジュール調整、従業員のダウンタイム対応計画を盛り込む必要があります。

サードパーティー リソースの活用
外部のサイバーセキュリティ コンサルタントで、チームを増強させることができます。例えば、Dellのインシデント対応サービスでは、エキスパート チームを数時間以内にオンサイトに派遣し、評価、封じ込め、修復を直ちに開始できます。当社は、多くのお客様がサイバー攻撃を乗り越える支援をしてきました。

AIは有用であるが、万能の解決策ではない

AIは、サイバーセキュリティ ツールとプログラムを強化する大きな可能性を秘めています。その機能は、予測分析、カスタム トレーニング プログラムの開発、さらには脅威拡散前のプロアクティブな対処まで、最終的にはあらゆる領域を網羅するはずです。

さらに重要な点は、AIがインシデント発生時に防御側にリアルタイムのサポートシステムを提供できることでしょう。過去の攻撃データでトレーニングされた機械学習モデルは、過去の類似イベントに基づくアクションを推奨できます。

自然言語処理がサイバーセキュリティ ツールに組み込まれるにつれて、アナリストはシステムと直接連携して脅威を特定し、解決策を展開できるようになると思われます。

また、AIは行動パターンを監視して、人間のアナリストが（おそらく疲労が原因で）ミスを繰り返している可能性を指摘し、交代や新たな視点の導入を促すこともできます。

サイバーセキュリティ ツールには、高度化したAIツールが迅速に統合されているものの、特に強力な機能の多くは依然として開発中です。現時点では、AIは経験豊富な実務担当者、**特に、過去に攻撃を乗り越えた経験のある人材**のスキルを代替できないことに注意してください。

AIを活用するための推奨事項：

ツールがセキュリティ運用にどう役立つかを理解する
AIツールの詳細な分析を行い、最も効果的な場所に実装します。導入しやすいものには、高度な脅威検出、反復タスクの自動化、ID管理におけるAIの使用などがあります。

AIの未来に向けた計画
新しい機能がいつ利用可能になるか、それがチームにどのようなメリットをもたらすかを理解し、それらを実装するための計画を策定しましょう。

> リテーナー契約に基づき、インシデント対応、修復、リカバリーを請け負うパートナーを持つことがベスト プラクティスです」
>
> ***Jason Rosselot***
> デル・テクノロジーズ、サイバーセキュリティおよびビジネス ユニット セキュリティ担当*VP*

AIを人員計画に組み込む
自動化によって手作業が減ることで、セキュリティ チームの構成を進化させなければならない場合があります。セキュリティ情報を収集するだけでなく、分析し、それに基づいて行動するには、さらに優秀なリソースが必要になる場合があります。採用と能力開発の戦略をしかるべく調整してください。

AIがまだサイバーセキュリティ運用の重要な役割を担っていないとしても、いずれはそうなるはずです。しかし、経験豊富な熟練の実務担当者の代わりはできない点に留意してください。目標はあくまでも、AIを活用して業務を自動化し、人的資源を有効化し、最終的に攻撃を防止して、攻撃が発生した場合の影響を最小限に抑えることです。

サイバーセキュリティ成熟度の向上：一歩ずつ

サイバーセキュリティにおけるあらゆる要素と同様に、人的要素への対応は、一度で終わるものではなく、継続的な取り組みだと理解する必要があります。日々の小さな努力は、それが小さな前進であっても、時間の経過とともに変化を生み、積み重なっていきます。最高のテクノロジーやセキュリティ ツールさえ、最終的にはそれを運用する側の能力次第だと覚えておくことが重要です。

有効なDellの製品とソリューション

注目のDellソリューション	説明
Incident Response Services	業界の認定を受けたサイバーセキュリティ エキスパートで構成されるチームが待機しており、サイバー攻撃発生時に迅速に対応します。通常業務が再開されるまで、お客様と協力して脅威を排除します。
サイバーセキュリティ アドバイザリー サービス	エキスパートが、セキュリティ戦略における盲点の発見と対処、資産とデータの保護、継続的な警戒とガバナンスの徹底を支援するガイダンスを提供します。
vCISO	仮想の最高情報セキュリティ責任者およびサイバーセキュリティ エキスパートが、リスクの特定と管理を支援し、戦略的意思決定を導きます。
Managed Detection and Response	エンドポイント、ネットワーク、クラウド全体にわたる監視、脅威検出、調査、迅速な対応を提供することで、手作業を減らし、日々のセキュリティ運用を合理化します。お客様は、ご希望のXDRプラットフォーム（Secureworks® Taegis™ XDR、CrowdStrike Falcon® XDR、またはMicrosoft Defender XDR）を選択し、エキスパートによるガイダンス、四半期レポート、年間最大40時間のインシデント対応を受けることができます。

dell.com/cybersecuritymonthで今日のサイバーセキュリティの重要な課題に対処する方法をご紹介しています