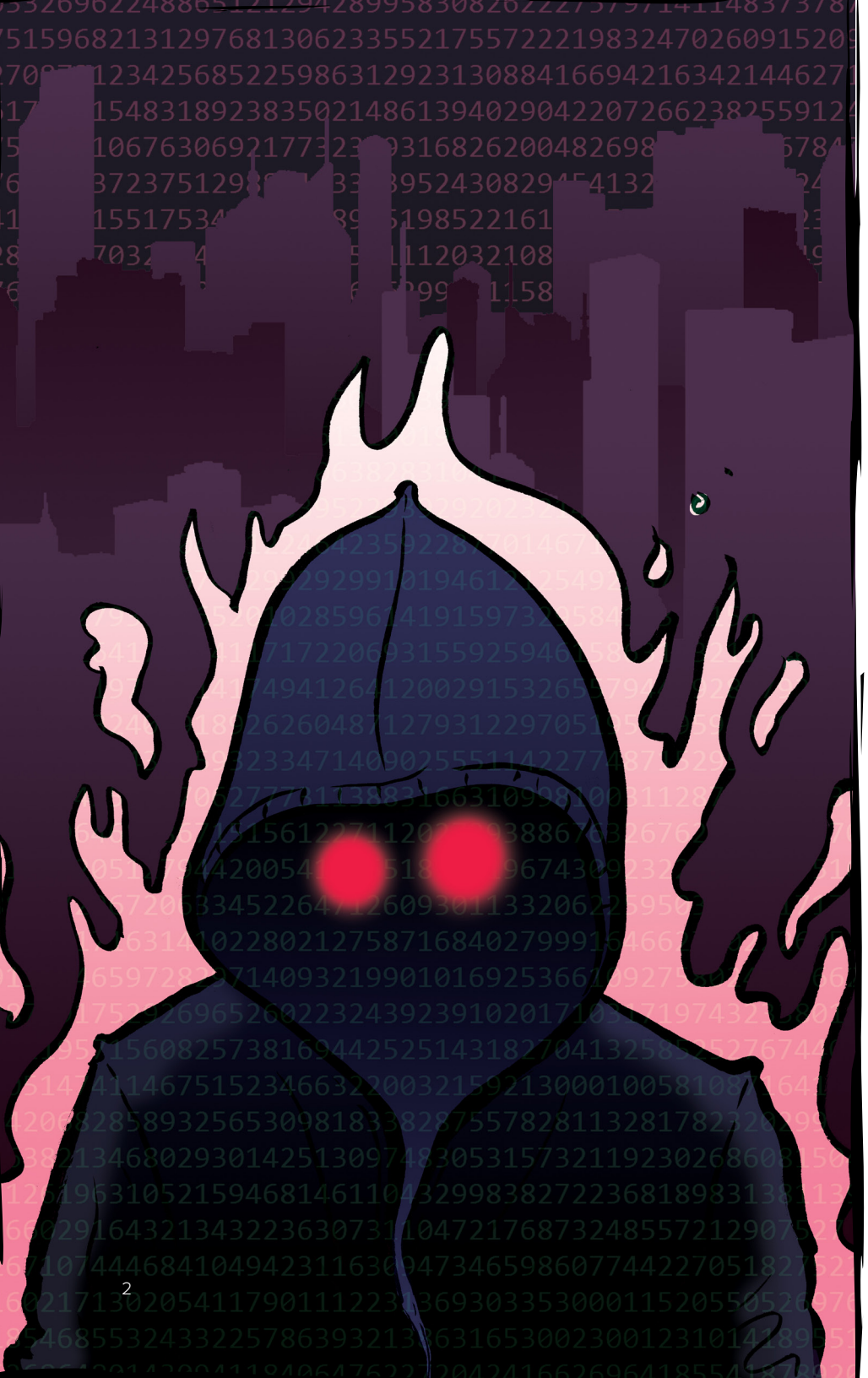
究極のサイバーレジリエンス: ADセキュリティ犯罪への対策ガイド

ハイブリッドActive Directoryを
リスク、脅威、災害から守ります。

Quest



はじめに

サイバーセキュリティの世界では、Active Directory（AD）が重要です。Active Directory（AD）は、各組織の基盤として、環境全体のあらゆる重要なリソースに認証と承認の機能を提供しています。Active Directoryを適切に管理し、安全を確保することが、ビジネスの継続性と成功にとって不可欠であると言えます。

これを言葉にするだけなら簡単ですが、実現は困難です。AD環境は複雑であり、また進化を続けているからです。さらに、Active Directoryの抱える価値は大きいため、サイバー犯罪者が狙う最大のターゲットになります。こういった危険な攻撃者は、狡猾で手口も徹底しており、Active Directoryを制御できれば企業全体をも意のままにできることを理解しています。 そのため、ADを制圧するという目標の達成を目指して、次々と新しい戦術、ツール、および手法を作り出しているのです。

Microsoftの報告によれば、2021年には、Azure ADアカウントに対して250億件以上のブルートフォース攻撃がありました。また、Microsoftデジタル防衛レポート2022によると、攻撃の影響を受けた顧客の88%が、ADおよびAzure ADセキュリティのベストプラクティスを導入していなかったとのことです。さらに、このMicrosoftのレポートでは、攻撃から回復した顧客に見つかった問題点をランキングとして報告していますが、その中でもActive Directoryの設定が安全ではなかったことに注目していました。

攻撃による脅威は現実です。これは、「もし発生したら」という問題ではなく、「実際発生した場合」を想定すべき問題なのです。ランサムウェア、内部の攻撃者、設定ミス、その他の災害など、危険が目の前に迫っています。多くの場合、攻撃対象となるのがハイブリッドActive Directoryです。攻撃者は、重要なIDシステムの設定ミスやセキュリティが弱い箇所を探し出し、広範囲のアクセス権を奪取して、ビジネスに影響を与えようとしています。

ただし、まったく打つ手がないというわけではありません。この電子書籍では、Questがハイブリッド ADサイバーレジリエンスの完全なライフサイクルを実現し、 攻撃を受ける前、攻撃の最中、攻撃終了後のリスクを低減する方法を紹介します。AD Active Directoryセキュリティの脅威を打ち倒しましょう。

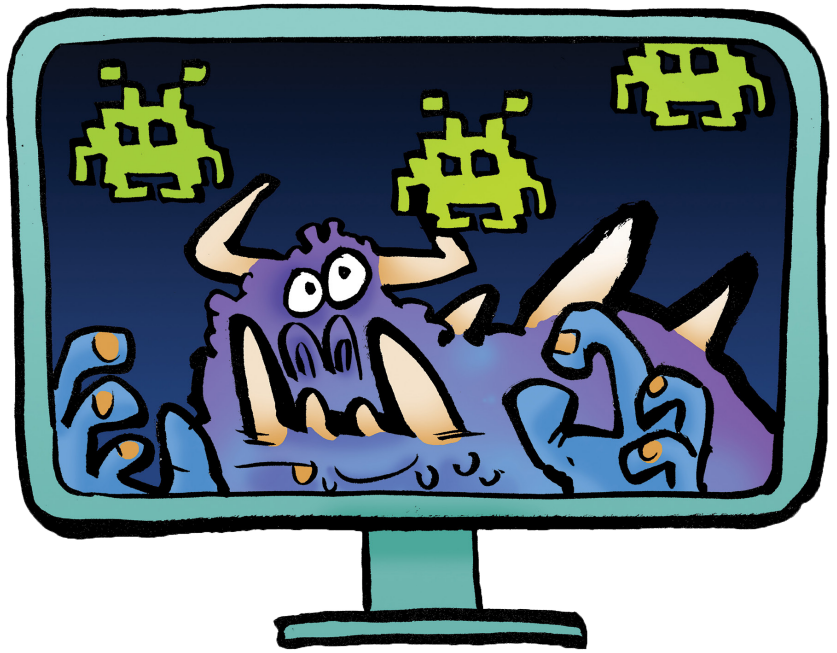
ハイブリッドADのサイバーリスク管理フレームワークを確立する

多くの企業では、セキュリティインフラストラクチャの隙を無くすため、NISTなどの一般的なフレームワーク（または地域、業界、国独自のフレームワーク）に、セキュリティリスク管理プログラムを採用しています。NISTフレームワークでは、サイバーセキュリティのリスクからインフラストラクチャを保護する際に考慮すべき基準、ガイドライン、および実践内容を定めています。

NISTフレームワークは、以下の柱（原則）で構成されています。

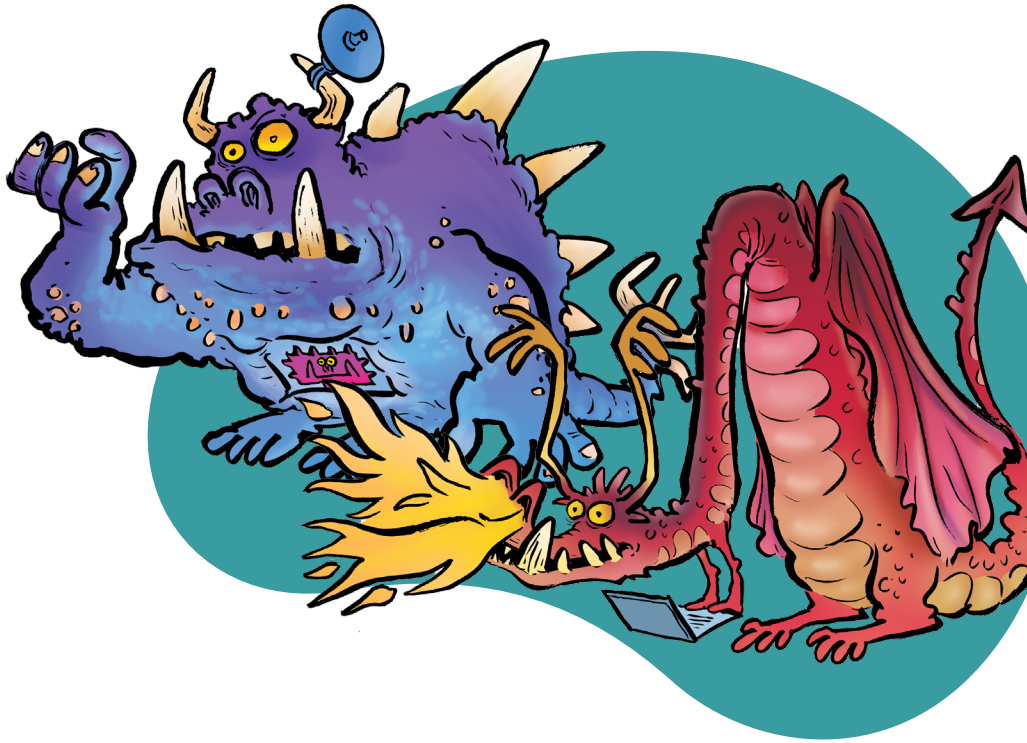
- **特定**: 保護が必要な資産と、存在する弱点を確認する
- **保護**: 安全および防御対策を確立し、重要な資産を保護する
- **検知**: セキュリティ上の問題およびインシデントを調査する
- **対応**: セキュリティインシデントを阻止するための対応策を構築する
- **復元**: 災害発生時に、機能とデータを復元する

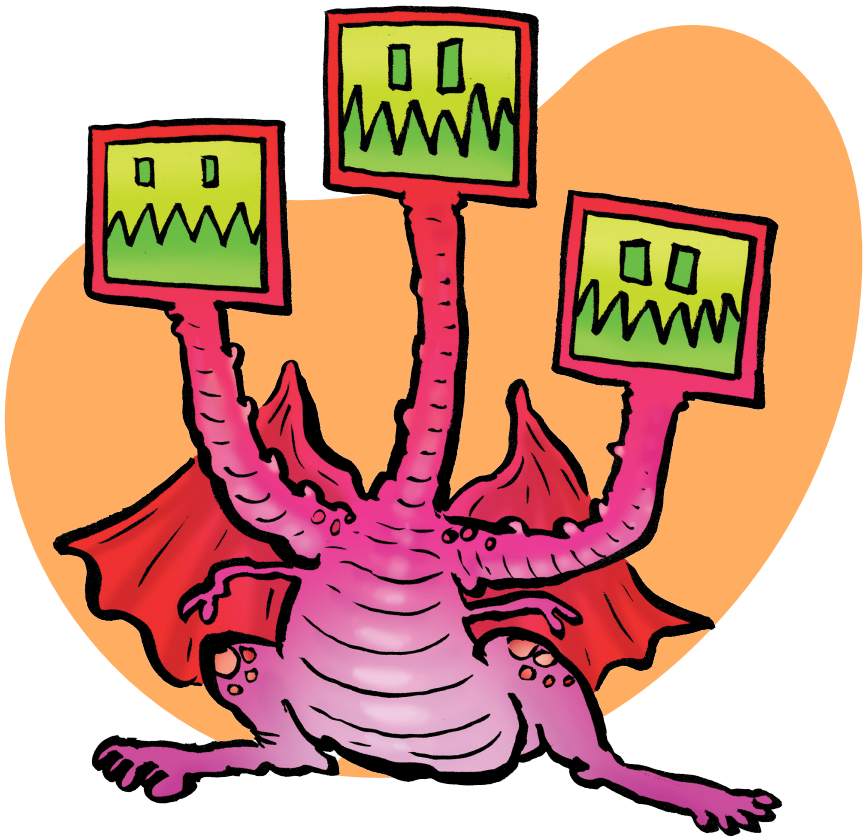
それぞれの柱の内容を実現することが、Active Directoryの安全確保の鍵となります。ただし、多くの企業では、NISTの各原則における目標達成を目指す際に困難に直面しています。



Quest

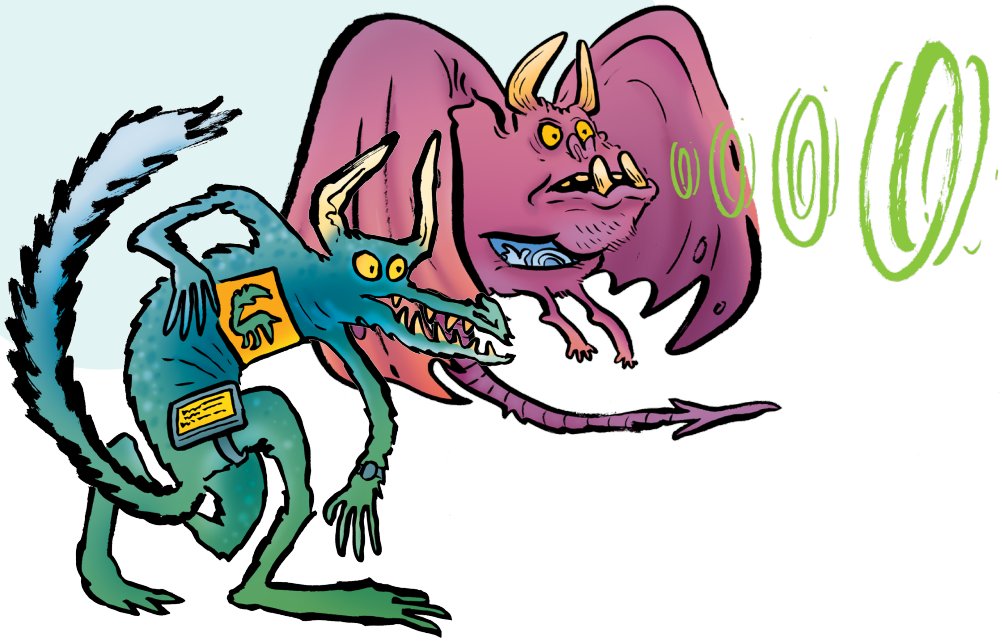
- **特定の問題**: 組織がオンプレミスやクラウドに拡大すると、ユーザ、グループ、権限、およびアプリケーションなど、Active Directoryの重要な側面の可視性が不足していると気付くことが多くなります。これは、誰がどの情報へのアクセス権を持っているのかがよく分からないということです。また、多くの組織では、最重要の資産、すなわち「Tier 0」資産が何であるかを特定できていません。AD内にどのような権限が存在し、Tier 0資産には何があるのかを把握することが、最終的にリスクを特定するための第一歩になります。攻撃者が利用できそうな既存の経路や弱点の特定についてはどうでしょうか。インフラストラクチャ全体への入り口として機能してしまう、重要な経路を特定できるでしょうか。Active Directoryの重要コンポーネントを詳細に把握しておかなければ、日常的な脅威から自社を守り、リスクの特徴を正確に理解することは事実上不可能になります。





- **保護の問題**: 現代の組織ではAzure ADやOffice 365を導入していますが、これはActive Directoryへの依存度が高まるだけという結果となり、攻撃対象領域が倍増し、ランサムウェアなどの攻撃を受ける可能性も高まってしまいます。残念ながら、ADの脆弱性の管理は手間と時間がかかり、多くの場合システムが提供する監査ツールでは実行できません。グループ・ポリシー・オブジェクト（GPO）の制御と管理も気の遠くなるような作業です。特に、かなり以前のチームが作成したまま放置されていたGPOが1つ詳細不明になっているような場合、ネットワーク内の数千ものシステムに関わるセキュリティ体制に甚大な影響を与える可能性があります。Office 365のテナントもどんどん拡大されますが、この管理と保護についてはどうでしょうか。Active Directory環境は進化と拡張を続けています。これは、対応の必要がある脆弱性や資産も同様に進化と拡張を続けるということです。

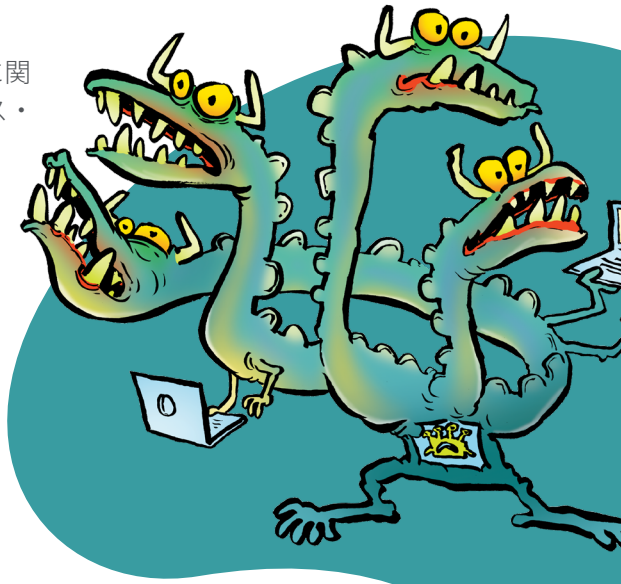
Quest



- **検知の問題**: オンプレミスとクラウド両方の設定に対し検知を行う場合、ユーザと管理者による変更およびアクティビティの項目はセキュリティ上重要ですが、Office 365とAzure ADのセキュリティログでは、オンプレミスとクラウドのアクティビティの統合ビューは提供されません。システムが提供するツールでは、悪用方法、脆弱性、および疑わしいアクティビティを簡単には特定できません。したがって、手遅れにならないように、新たな異常が発生するたびに慌てて正体を突き止めなければなりません。
- **対応の問題**: 「手遅れ」に関連して考えてみましょう。奇妙なアクティビティが進行中であることを確認した場合、次にどうすればよいでしょうか。多くの組織では十分な対応システムを備えていません。そのため、迅速な調査と分析や、変更以前の正常に機能していた設定や権限の復元（必要な場合）を効率的に実行することができません。IT部門の能力と、システム提供のツールに頼るだけでは、労力と時間を浪費して、前述のような設定や異常を探すことになります。また、次に取るべきステップも不明瞭になってしまいます。

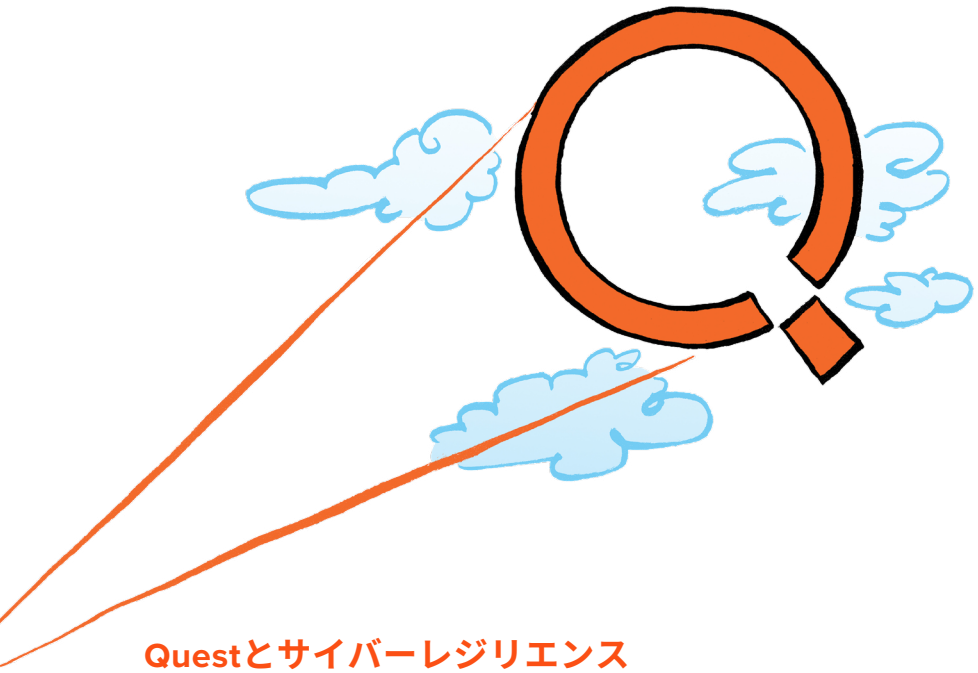
- **復元の課題**: ディザスタリカバリ計画をテストするための最悪のタイミングは、災害が進行中の時です。ところが、それが現実になってしまう事態が頻繁に発生しています。Microsoft提供の『Active Directory Forestのリカバリガイド』では、自動化しない限りエラーが発生しやすく、時間も浪費してしまう手順の概要を40種類ほど紹介しています。プロセスを手作業で実行する、またはネイティブのツールを使用するという状態では、マルウェアの再感染、ダウンタイムの延長、損失の増大といったリスクを高めるだけです。アクセス権があったとしても、自信を持ってバックアップを使用することができなくなるため、攻撃者がさらに損害を与える余裕が生まれ、組織は財政面と評価面の損失を被ることになります。最初に復元すべきドメインとユーザはどれか分かりますか。コミュニケーション計画はどうでしょうか。侵入を受けるだけでも大変な混乱を生みますが、テストしていない計画を使えば混乱はさらに長引き、悪化の一途をたどります。保険で対応できそうにも思えますが、ポリシーの細部を覚えているでしょうか。今の手順で間違いなく損失を回復し、運用状況を元に戻せるのでしょうか。 この混乱の原因としては、あまり役に立たないツール、使用するツール間の連携不足、不適切なサポート、境界セキュリティへの過剰な投資（および不十分な導入）、ID保護に対する投資不足が挙げられます。

Active Directoryのセキュリティに関しては、サイバー・レジリエンス・インフラストラクチャのあらゆる側面を警戒する必要があります。わずか1つの柱に弱点があれば、Active Directory全体、ひいては企業全体が崩壊の危機に直面します。攻撃者は、サイバー・レジリエンス・フレームワークの柱の1つが軽視されるタイミングを心待ちにしています。それは、他のActive Directory環境に「どうぞお入りください」と言っているに等しい行動だからです。



Quest

では、NISTフレームワークのあらゆる側面を確実に導入し、多数存在するADセキュリティの問題に対処できるような方法はあるのでしょうか。確実な解決方法はあるのでしょうか。



Questとサイバーレジリエンス

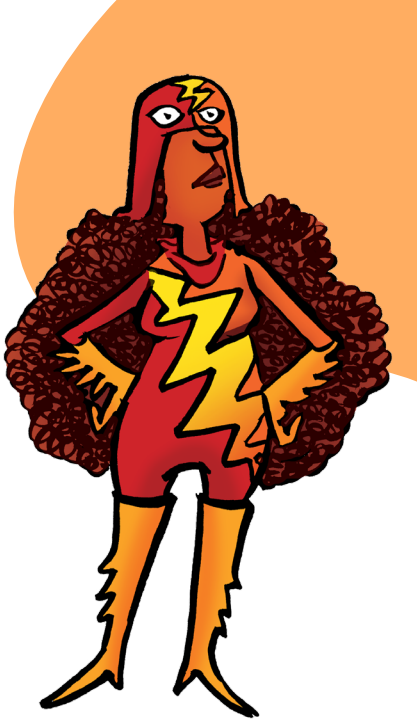
Questでは、NIST Frameworkのすべての階層で多層防御を提供するハイブリッドADサイバーレジリエンスのアプローチを提供しているため、攻撃前、攻撃中、攻撃後のリスクに対処できます。

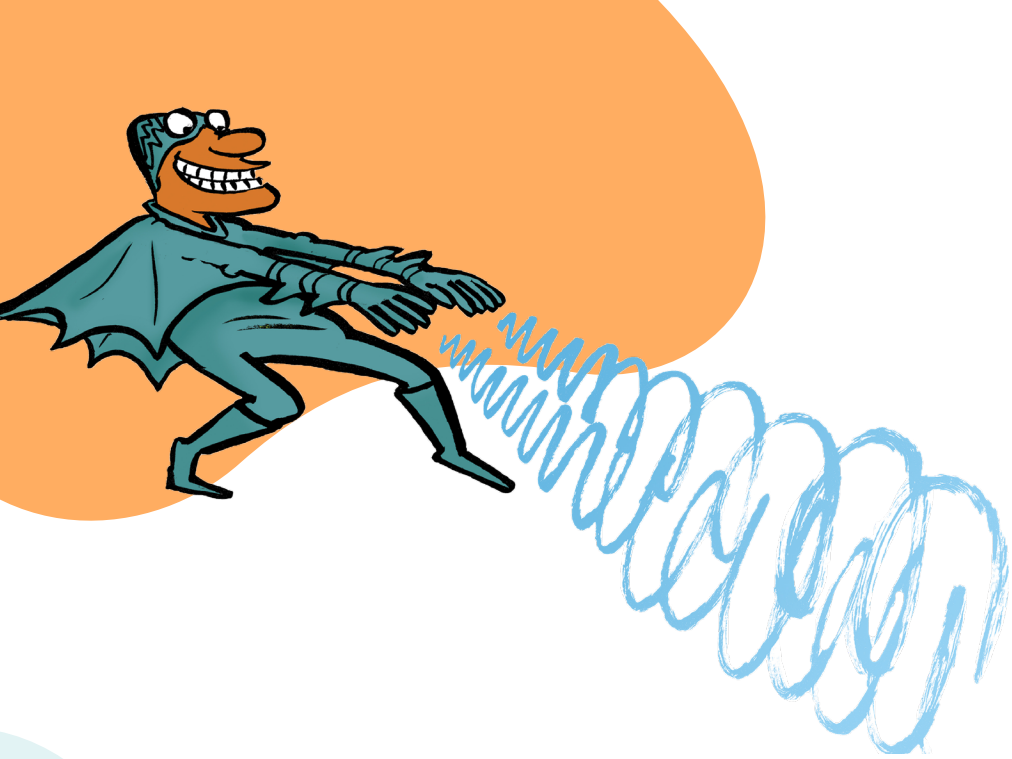
当社のハイブリッドADサイバー・レジリエンス・スイートのソリューションは、動的な総合防御機能と連携する相互補完型ソリューションで、以下の内容を実現します。

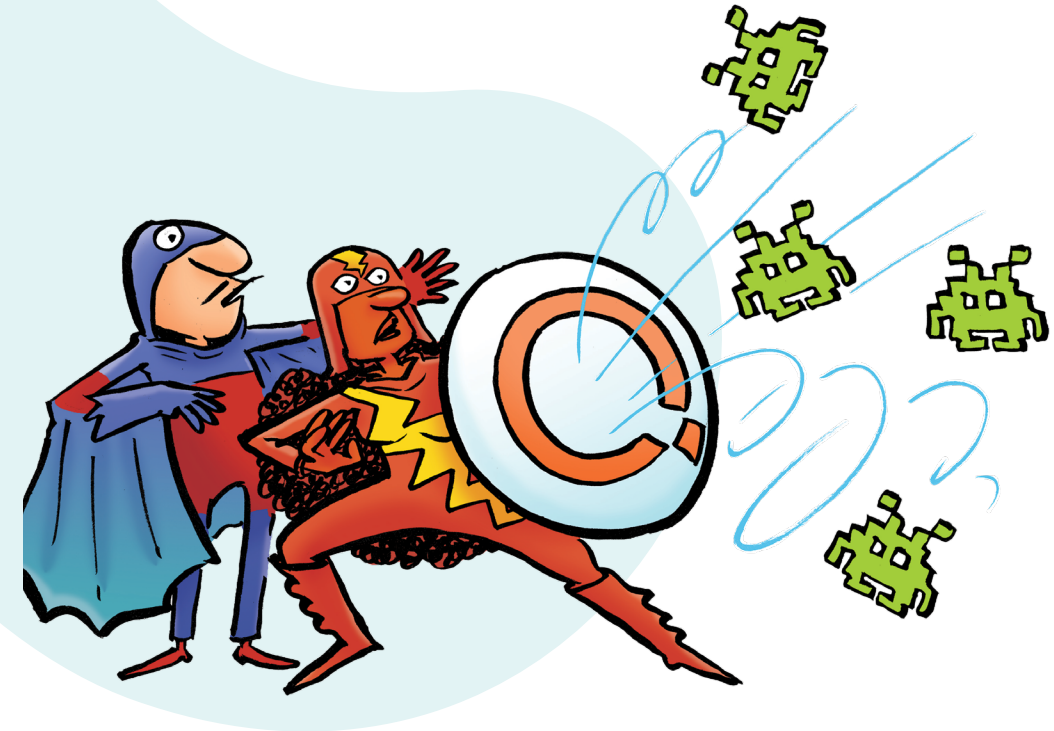
- 露出インジケータ（IOE）を**特定**し、攻撃者がお客様の環境を所有するために取り得る攻撃パスの優先順位を設定する。
- 攻撃者が重要なグループやGPO設定を変更したり、ADデータベースに侵入して認証情報を盗んだりできないように、 お客様の環境を**保護**する。

- リアルタイム監査、異常検知、およびアラート機能により、侵害インジケータ（IOC）を**検知**する。
- 脅威に**対応**し、情報を迅速に収集して、調査を高速化する。
- 大小に関わらず、あらゆる攻撃からADを**復元**し、数日、数週間、あるいは数ヶ月という期間ではなく数分で、業務、データ整合性、お客様満足度を復旧させる。

では、このパワフルなソリューション群は、どのようにしてハイブリッドAD環境を激しい攻撃から保護しているのでしょうか。以下にスイートごとの機能と、各機能の連携状況について説明します。







Quest AD Risk Assessment Suite

AD Risk Assessment Suiteは、当社の主力製品であるChange AuditorとOn Demand Audit Hybrid Suiteの2つを組み合わせたものです。また、パワフルなSpecterOps BloodHound Enterpriseも付属しており、環境の潜在的な脅威を特定および検知し、環境を保護します。AD Risk Assessment Suiteでは、以下のことが可能です。

- ユーザやグループの変更を含むADおよびAzure AD環境全体のセキュリティに関するすべての変更、オフラインコピーや不正なドメインレプリケーションによるADデータベースの流出などの悪用を完全に監査できるようになります。
- 不正なドメインレプリケーション、ADデータベースのオフライン抽出、およびGPOリンクなどの脅威を早期に検出し、コストのかかるランサムウェア攻撃を軽減および回避します。
- どの権限を乗っ取られたかにかかわらず、まず重要なグループやGPOの設定変更を阻止し、資格情報を狙ったADデータベースの持ち出しから攻撃者をブロックします。

Quest AD Risk Protection Suite

AD Risk Protection Suiteでは、Risk Assessment Suiteのすべての機能と合わせて、パワフルなソリューションのGPOADminも使用可能で、GPOの管理とガバナンスをシンプル化できます。AD Risk Protection Suiteにより、以下のことが可能です。

- Active Directoryのグループポリシー管理において重要な手順である展開の前に、変更内容が変更管理のベストプラクティスに準拠していることを確認します。
- 自動アテステーションによりGPOを継続的に検証します。これは、サードパーティのグループポリシー管理ソリューションに欠かせません。
- GPOのバージョンを素早く簡単に並べて比較する先進の機能で、さまざまな期間で行われるGPO監査を改善し、設定の一貫性を検証します。
- GPOの変更によって望ましくない影響が発生した場合は、動作中のGPOに素早く戻します。数秒のうちに環境を再び円滑に運用することができます。

Quest

QuestハイブリッドADサイバー・レジリエンス・スイート

最初の2つのスイートで、NISTフレームワークの原則の半分以上（特定、検知および保護）がカバーされますが、最後のハイブリッドADサイバー・レジリエンス・スイートはフレームワークの残り部分（対応と復元）をカバーします。ハイブリッドADサイバー・レジリエンス・スイートを使用すると、どのようなサイバー関連のイベントが発生しても、確実に最大限のセキュリティで対応できます。ハイブリッドADサイバー・レジリエンス・スイートは、他のスイートに含まれる製品の他に、イベントに対応するIT Security Searchと、Recovery Manager Disaster Recovery EditionおよびOn Demand Recoveryを追加し、規模の大小やオンプレミスかクラウドかを問わず、あらゆるリカバリのニーズに対処します。これにより、次のことが可能になります。

- 手動ADフォレスト・リカバリ・プロセスのすべてのステップを自動化します。
- ADバックアップを侵害から保護し、マルウェアの再感染リスクを排除します。
- Azure AD Connectにより同期されていないクラウド専用オブジェクトを復元
- ハイブリッドADのバックアップおよびディザスタリカバリ計画を実演し、検証します。

まとめ

Questは、NIST Cybersecurity Frameworkに対応した多くの階層に多層防御を提供する、完全で継続的なADおよびOffice 365のサイバー・レジリエンス・ライフサイクルを実現します。当社のソリューションは連携し、また互いに補完し合うことで、将来的に問題となり得る弱点を克服し、サイバーレジリエンスとビジネス成果の目標を達成します。

世界各地のサイバー攻撃者に対抗する、Questによるサイバーレジリエンスのストーリーが今始まります。

Quest

Questについて

Quest はますます複雑になる IT 環境において、新たなテクノロジーのメリットを実現にするソフトウェアソリューションを提供します。データベースとシステムの管理からActive DirectoryとMicrosoft 365の移行および管理、そしてサイバー・セキュリティ・レジリエンスまで、Questは次のIT課題を今すぐ解決できるよう、お客様をサポートします。世界中の13万社を超える企業とFortune 500の95 %が、次のエンタープライズイニシアチブのプロアクティブな管理と監視を実現し、複雑なMicrosoftの課題に対する次のソリューションを見つけ、次の脅威に事前に対処できる Quest を信頼しています。Quest Softwareは今「次」に備えます。詳細については、www.quest.comをご覧ください。

本書の使用に関して不明な点がありましたら、以下までお問い合わせください。

www.quest.com/JP-JA/company/contact-us.aspx