DELL Technologies

サイバーセキュリティとゼロトラストの成熟度を高める

セキュリティ リスクによってイノベーションが阻害される事態を回避

サイバーセキュリティの現状を把握

対策が必要な領域を把握する

今日の脅威とそれを取り巻く環境は、複雑で急速に進化しており、堅牢なサイバーセキュリティ プラクティスを維持するにあたって、リソースや知識面の制限に直面することは少なくありません。進化するサイバー脅威に対抗し、イノベーションを阻害することなく環境の安全性を維持するには、サイバーセキュリティとゼロトラストの成熟度の向上が不可欠です。

サイバーセキュリティの現在の成熟度を、このチェックリストを利用して評価してください。組織の強みと脆弱性を把握することで、サイバーセキュリティの成熟度を高めるための適切な次のステップに進むことができます。

目次

詳細はこちら

サイバーセキュリティとゼロトラストの成熟度を高める方法の詳細はこちら

チェックリスト：

攻撃対象領域の縮小

攻撃対象領域とは、サイバー攻撃者によって標的または悪用される可能性のある環境内のすべてのポイントまたは領域を指します。これらのポイントには、ソフトウェアの脆弱性、構成ミス、脆弱な認証メカニズム、パッチ未適用のシステム、過度なユーザー権限付与、開かれているネットワーク ポート、不十分な物理的セキュリティなどが含まれます。ここに挙げる質問事項は、悪意のあるアクターが侵害する可能性のある脆弱性やエントリー ポイントを最小限に抑える方法を判断するのに役立ちます。

はい	いいえ	
☐	☐	システムとネットワークの脆弱性と弱点を特定し、タイムリーな修復と改善を可能にするために、評価、侵入テスト、侵害攻撃シミュレーションを定期的に実施していますか？
☐	☐	従業員を対象に、定期的なセキュリティ トレーニングを実施していますか？
☐	☐	多要素認証 (MFA) とロール ベース アクセス制御 (RBAC) を利用していますか？
☐	☐	重要な資産を分離し、ネットワークの異なる部分間のアクセスを制限するために、ネットワーク セグメンテーションを実施していますか？
☐	☐	セキュアなコーディング プラクティスを実装し、セキュリティ テストとコード レビューを定期的に実施して、Web アプリケーション ファイアウォール (WAF) を使用することで、一般的なアプリケーション レベルの攻撃を防ぎ、Web アプリケーションの攻撃対象領域を縮小していますか？
☐	☐	サプライ チェーンを保護するためのプロセスと手順を証明できる IT サプライヤーを選択していますか？
☐	☐	従来の境界ベースのセキュリティからシフトし、ゼロトラストの原則を採用していますか？
☐	☐	最小権限の原則を採用して、ユーザー アカウントとシステム アカウントがタスクを実行するのに必要な最小限のアクセス権のみを持つように制限していますか？
☐	☐	システムとソフトウェアに定期的にパッチを適用していますか？
☐	☐	セキュリティ ツールで、脆弱性をプロアクティブに特定するために AI/ML 機能を活用していますか？

チェックリスト：

脅威の検出と対処

サイバー脅威の検出と対処は、あらゆるセキュリティ戦略に不可欠な要素です。これには、ネットワーク トラフィック、システム ログ、その他の領域、セキュリティ データを監視および分析して、不正アクセス、侵入、マルウェア感染、データ侵害、その他のサイバー脅威の兆候を特定することが含まれます。ここに挙げる質問事項は、コンピューター ネットワーク、システム、または組織内の潜在的なセキュリティ インシデントや悪意のあるアクティビティをプロアクティブに特定し、積極的に対処する方法を判断するのに役立ちます。

はい	いいえ	
☐	☐	セキュリティ ツールとテクノロジーである Extended Detection and Response (XDR)、侵入検出システム (IDS)、侵入防止システム (IPS)、SIEM、ログ分析を使用して、ネットワークとシステムのアクティビティを継続的に監視していますか？
☐	☐	潜在的なサイバー脅威を示す可能性のあるパターン、異常、侵害の痕跡 (IoC) や攻撃の痕跡 (IOA) を特定するために、収集したデータを分析していますか？
☐	☐	可能性を迅速に検出してアラートを発する最新の可視化ツールと監視ツールを導入していますか？
☐	☐	ネットワーク トラフィックを監視して、サイバー攻撃が進行中であることを示す可能性のある異常なパターンや疑わしいアクティビティがないか確認していますか？
☐	☐	異常なデータ パターンや挙動をリアルタイムで分析してサイバー脅威を検出するのに役立つ AI/ML ツールを導入していますか？
☐	☐	セキュリティ アラートをより適切に管理し、IT エコシステム全体からセキュリティ イベント データの相関付けを開始するために、次世代の SIEM ソリューションの導入を検討していますか？
☐	☐	既存の脆弱性に優先順位を付けて対処し、新しい脆弱性に効率的に対応するために、脆弱性のテストと管理を実施していますか？
☐	☐	確認されたセキュリティ インシデントを調査して影響を軽減するためのインシデント対応計画を策定していますか？
☐	☐	サイバー攻撃の拡散を抑えるのに役立つインシデント対応アクションを迅速化するために、セキュリティ オーケストレーション、オートメーション、応答 (SOAR) ツールを組み込んでいますか？
☐	☐	インシデント対応計画には、封じ込めポリシー、コミュニケーション計画、コンプライアンス要件、フォレンジック分析、リカバリー プロセスが盛り込まれていますか？

チェックリスト：

サイバー攻撃からのリカバリー

サイバー攻撃からのリカバリーとは、セキュリティ インシデントが発生した後に、影響を受けたシステム、ネットワーク、データを安全で運用可能な状態に復元するプロセスを指します。これには、攻撃によって引き起こされた損害を軽減するための措置を講じて、侵害または中断されたサービスとデバイスを再構築し、インシデントを分析して今後の攻撃を防ぎ、組織の運営を通常の状態に戻すことが含まれます。ここに挙げる質問事項は、組織がサイバー攻撃から効果的にリカバリーできているかどうかを判断するのに役立ちます。

はい	いいえ	
☐	☐	サイバー攻撃を隔離して封じ込めるためのインシデント封じ込め対策を実施していますか？
☐	☐	インシデント発生後にシステムやデバイスを復元するためのプロセスはありますか？
☐	☐	データを保護する際に、データの分離、不変性、サイバー ヴォールトを活用していますか？
☐	☐	データが侵害、暗号化、削除された場合にデータをクリーンにリカバリーするための手順を確立していますか？
☐	☐	サイバー攻撃からのリカバリーを自動化または迅速化するために、AI/ML テクノロジーを活用していますか？
☐	☐	インシデントを継続的に評価し、攻撃を受けてリカバリーした後に改善すべき領域を特定していますか？
☐	☐	セキュリティの強化や法的措置または懲戒処分のためにフォレンジック分析を実施して、攻撃手法を理解し、侵害の範囲を判断して、影響を受けたシステムとデータを特定し、証拠を収集していますか？
☐	☐	サイバー攻撃とそれがデータや業務に与える潜在的な影響について、顧客、パートナー、ベンダーなどの関係者に通知する必要があることを組織は認識していますか？
☐	☐	ビジネスのリカバリーと SLA の適切な履行に自信を持つために、リカバリー戦略を年に複数回実践していますか？
☐	☐	組織のリカバリーをサポートするためにサービス プロバイダーと連携していますか？

サイバーセキュリティとゼロトラストの成熟度を高める

サイバーセキュリティに関しては、IT 組織が最悪のシナリオに備えて計画を立て、マルチレイヤー防御を構築することが不可欠です。絶え間なく進化するサイバーセキュリティの脅威ランドスケープでは、セキュリティ プラクティスを継続的に推進し、ゼロトラストの原則を採用することが重要です。これには以下が含まれます。

攻撃対象領域の縮小

環境を侵害するために悪用される可能性のある脆弱性とエントリー ポイントを最小限に抑えます。

サイバー脅威の検出と対処

潜在的なセキュリティ インシデントや悪意のあるアクティビティを積極的に特定して対処します。

サイバー攻撃からのリカバリー

セキュリティ インシデントの発生後に、安全であることがわかっている運用可能な状態に組織を戻します。

Dell は、プロフェッショナル サービスの専門知識を活用し、信頼できるビジネス パートナーと連携することで、進化するサイバー脅威から保護する包括的なセキュリティ体制を確立できるよう組織をサポートします。テクノロジーが進歩し続ける中、デジタル インフラストラクチャを保護し、デジタル領域での信頼を維持するためには、サイバーセキュリティへのアプローチの進歩も不可欠です。

DELL Technologies

デル・テクノロジーズについて

デル・テクノロジーズは、デジタルの未来を切り開き、働き方、生き方、行動を変革しようとする組織や個人を支援します。業界で最も広範かつ革新的でデータ時代にふさわしいテクノロジーおよびサービス ポートフォリオをお客様に提供しています。

詳細は、www.dell.com/securitysolutionsをご覧ください。