テクニカルレポート

セキュリティ体制の現状を動的に可視化する リスクスコアの解説

リスクスコアの算出方法の理解

2024年1月
トレンドマイクロ

エグゼクティブサマリー

レジリエンスのあるセキュリティ体制を構築するには、企業環境で使用されるシステムとアプリケーションによって直面するサイバーリスクの量を徹底的かつ包括的に理解する必要があります。Trend Vision One – Attack Surface Risk Management (ASRM) は、日々更新される指標を継続的に可視化することにより、迅速かつ正確なリスク評価を可能にします。 これにより、複雑な情報が精査され、会社全体のリスクスコアだけでなく、個々の資産ごとのリスクスコアが算出されます。当社の統合サイバーセキュリティプラットフォームであるTrend Vision Oneは、脆弱性、エクスポージャ、および既存のセキュリティコントロールデータを取り込み、分析することにより、デバイス、パブリックドメイン、IP、アプリケーション、クラウド資産、およびIDなどのサイバー資産を継続的に監視します。 さらに、Extended Detection and Response(XDR)に用いられるテレメトリおよび脅威インテリジェンスフィードを使用して、動的にリスクスコアを算出します。

このリスクスコアは、以下2つの変数を表します。

1. 攻撃者が企業環境へのアクセスを成功させる可能性
2. 1のようなインシデントの潜在的な影響度

プラットフォームはこれらの要因を考慮し、0から100の間の整数で結果を示し、 組織の資産に対する全体的なリスクを表します。

現在のセキュリティ体制をダイナミックかつ正確に可視化することで、リスクの優先順位付けと対応について十分な情報に基づいた意思決定を行うことができます。 さらに、セキュリティアナリストは、リスクスコアと固有のパラメータに基づいて、手動または自動化されたアクセス制御を実行できます。 セキュリティ製品やツールに対して、資産のステータスとそれに関連するリスクスコアおよびエンドポイントのリスクスコアについて、プラットフォームが継続的にクエリします。 これにより、セキュリティリスクのパラメータに影響するイベントが発生した場合、プラットフォームがユーザを強制的にサインアウトするか完全に無効にすることで、イベントに対処します。

米国標準技術研究所(NIST)*Guide for Conducting Risk Assessments*（NIST SP 800-30, Revision One）の Guide for Conducting Risk Assessments(NIST SP 800-30 Rev.1)では、リスクは「発生しうる状況または事象によってエンティティが脅かされる度合であり、通常、(i)その状況または事象が発生した場合にもたらされる負の影響 、および(ii)発生する可能性」と定義されています。このリスク評価実施ガイドでは、リスクには組織の資産、個人、関係する他の組織、国だけでなく、組織のミッション、機能、イメージ、さらにはレピュテーションまで含まれると言及しています。つまり、リスクは単なる技術的な側面のみならず、社会的な影響を与えうることを認識しておく必要があります。

リスクを定量化することで、リスクを受け入れるか、軽減するか、回避するかを決定することができ、セキュリティチームがゼロトラストアーキテクチャをより効果的に運用できるようになります。

継続的なリスクスコア算出の利点

ゼロトラストセキュリティモデルとは、あらゆるエンティティの暗黙の信頼を排除する手法です。 従来のアーキテクチャ、デバイス、およびIDは、企業のローカルエリアネットワーク (LAN) 、または他の許可されたネットワークあるいは地理的に限定されたネットワーク内で、信頼されたルールに準拠していました。しかし、今日の複雑で動的な環境は、モバイルデバイスやIoTデバイスなど、クラウドサービスとインフラストラクチャを物理的なゾーン全体に拡大しています。

その結果、すべてのエンドポイントは、すべてのトランザクションを検証しなければならないという状況に直面しました。

ゼロトラストモデルの基盤は、ユーザIDとアクセスを追跡しながら、継続的にリスクを評価する必要があります。 このような複雑化に対処するために、ゼロトラストセキュリティモデルには、継続的かつ洞察的な監視機能が必要です。これにより、最新かつ動的な環境でのアクティブなリスクと潜在的なリスクの全体像を把握できます。

トレンドマイクロのZero Trust Secure Access (ZTSA) ソリューションは、これらのニーズに対処できる仕組みを整えています。 セキュリティオペレーションチーム (SOC) が調査する前に、自動化された対応オプションを使用して脅威を軽減することが理想的です。 そしてさらに重要なことは、本格的な侵害が発生する前にリスク軽減することです。Trend Vision Oneは、セキュリティ制御の構成に関わる設定、資産の重要性、脆弱性、脅威活動など、リスクスコアにさまざまな要素を取り入れており、資産タイプごとに組織全体のリスクスコアを算出します。

次に、アナリストはこれらのスコアを使用して、注意が必要な箇所を正確に判断し、最初に対処する必要があるリスクを優先付けすることができます。 さらに、経営陣とリーダーは、リスクスコアの相対比較とベンチマークを有効にすることができます。これは、組織のセキュリティ体制が時間の経過とともに改善または低下しているかどうかを判断するのに役立ちます。 さらに、リスクスコアにより自社のセキュリティ体制を同じ業界、地域、および組織規模の他企業平均と比較できます。

機密性、完全性、可用性(CIA)の3要素

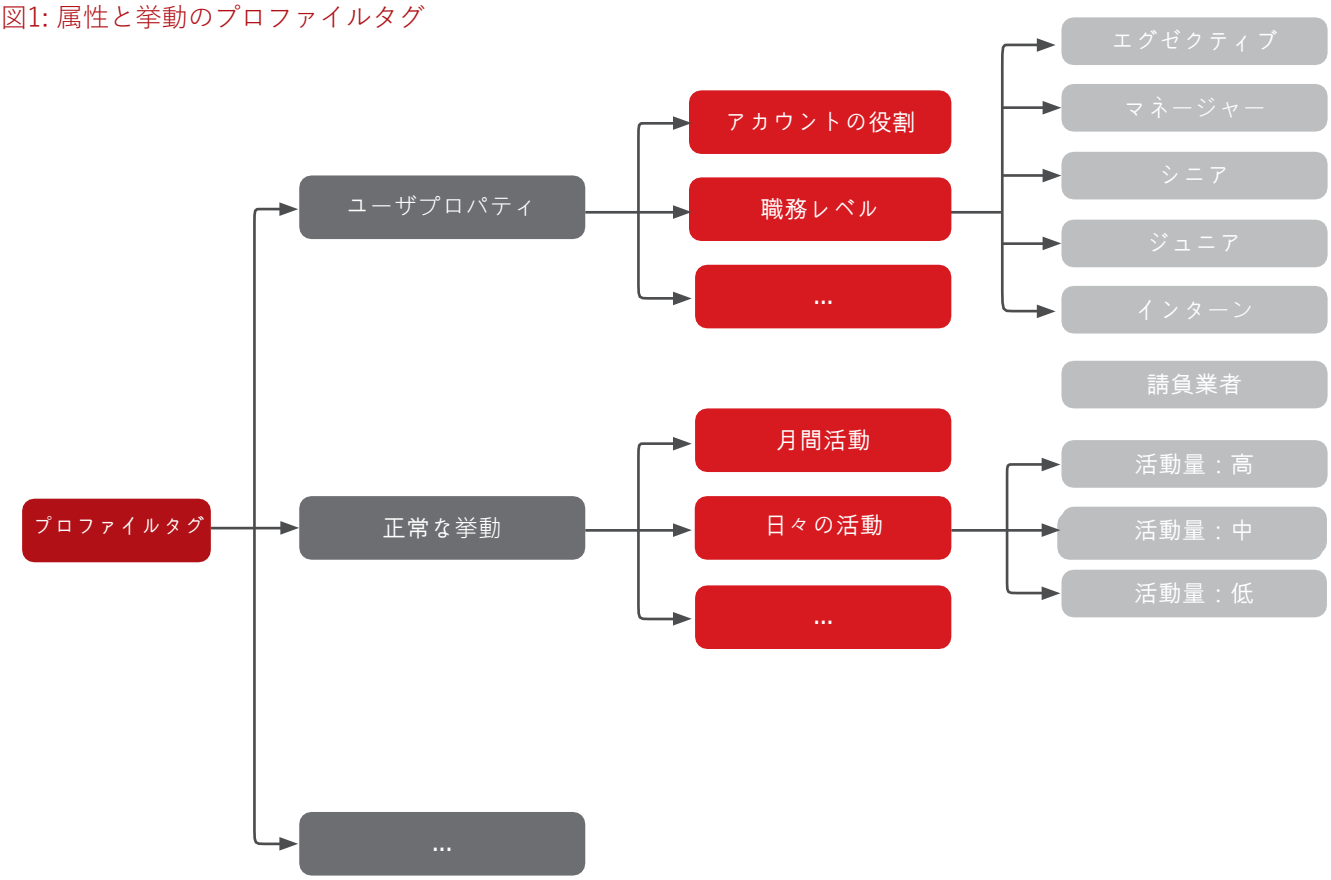
影響度とは、ビジネス価値によって決定される資産の重要度です。 この値は、NISTのマッピングガイドに記載されているCIAトライアドに基づいています。 *Guide for Mapping Types of Information and Information Systems to Security Categories* (NIST SP 800-60, Volume One, Revision One):

- **機密性(Confidentiality): データ、オブジェクト、およびリソースが不正アクセスから保護されること**
- **完全性(Integrity): データが不正な変更から保護され、信頼性と正確性を確保すること**
- **可用性(Availability): 承認されたユーザのみが、必要なシステムやリソースにアクセスできること**

Trend Vision Oneは、これらの3つの要因に影響を及ぼす属性と行動パターンを監視してビジネス価値を評価し、プロファイルタグで表現します。 たとえば、ユーザの職務レベルを考慮します。 エグゼクティブチームメンバーのアカウントの重要度は、エントリーレベルの従業員のアカウントよりも高くなる可能性があります。 職務、アカウントステータス、アカウント特権、資産タイプ、およびデバイス所有権は、CIAトライアド値に影響を与えるその他の資産属性です。

同様に、ユーザの挙動も影響します。 月間活動、日々の活動、アクセス履歴などの一般的な挙動はすべて、任意の資産のCIAトライアド値を評価および導出する際の考慮事項です。

図1: 属性と挙動のプロファイルタグ



機密性の評価の定義

評価	危険度	説明
5	非常に高い	将来の開発および/または基本的な利益に影響を及ぼす可能性のある機密情報を含む。データが漏えいすると、組織に壊滅的な損害を与える可能性がある。
4	高い	機密性の高い情報が含まれ、その漏洩は組織のセキュリティと利益に重大な損害を与える可能性がある。
3	中	漏洩した場合、組織のセキュリティと利益を損ないかねない機密情報。
2	低い	機密性は低いものの、内部でのみ開示すべき情報。あるいは、この情報の拡散により、組織の利益にわずかな損害を与える可能性がある。
1	極めて低い	公開されている情報処理ツールとシステムリソースを含む、公開されている情報。

完全性の評価の定義

評価	危険度	説明
5	非常に高い	不正な変更や中断が、組織やビジネスに深刻な修復不可能な影響を与える可能性がある。
4	高い	不正な変更や中断が、組織に重大な影響を与えるだけでなく、深刻なビジネス影響を及ぼす可能性があり、修復がより困難。
3	中	不正な変更や中断が、組織に重大な影響を与える可能性があり、ビジネスにある程度の影響を及ぼす。ただし、前述の影響を修復できる場合もある。
2	低い	不正な変更や中断が、組織に重大な影響を与えることはない。ビジネスへの影響は軽微であり、容易に修復できる可能性がある。
1	極めて低い	不正な変更や中断が、組織に与える影響はほとんどない。

可用性の評価の定義

評価	危険度	説明
5	非常に高い	正当なユーザに対する情報と情報システムの年間可用性が99.9%以上であるか、またはシステムの中断が許容されない。
4	高い	正当なユーザに対する情報と情報システムの可用性が、1日あたり90%以上であるか、またはシステムが最大10分の中断しか許容されない。
3	中	正当なユーザに対する情報と情報システムの可用性が通常の勤務時間中に少なくとも70%であるか、またはシステムが最大で30分の中断を許容する。
2	低い	正当なユーザに対する情報と情報システムの可用性が、通常の勤務時間中に少なくとも25%であるか、またはシステムが最大60分の中断を許容する。
1	極めて低い	正当なユーザに対する情報と情報システムの可用性が、通常の勤務時間中に25%未満という無視できる程度。

リスクスコアの算出

レベル	スコア
低	0-30
中	31-69
高	70-100

Trend Vision Oneは、セキュリティ制御の構成に関わる設定、資産の重要性、脆弱性、脅威活動など、リスクスコアにさまざまな要素を取り入れており、資産タイプごとおよび組織全体のリスクスコアを算出します。その結果は、0から100の間の整数で示され、右図のように3つのレベルのうちの1つに分類されます。資産への攻撃、エクスポージャ、およびセキュリティ設定に関するイベントのリスクスコア要因は、影響度で乗算します。

これは、ビジネスへの影響が少なく最小特権の資産では、攻撃対象領域が小さくなる可能性があることを意味します。
逆に、特権が広範囲に与えられた高価値の資産は、より大きな攻撃対象領域で構成されています。 リスクスコアは資産ごとに個別に算出され、各スコアは資産タイプと重要度を考慮して計算されます。リスクスコアの算出プロセスは複雑ですが、攻撃の可能性と影響度の幾何平均として要約できます。言い換えると、次のように攻撃の可能性に影響度を乗じた積の平方根を計算することです。

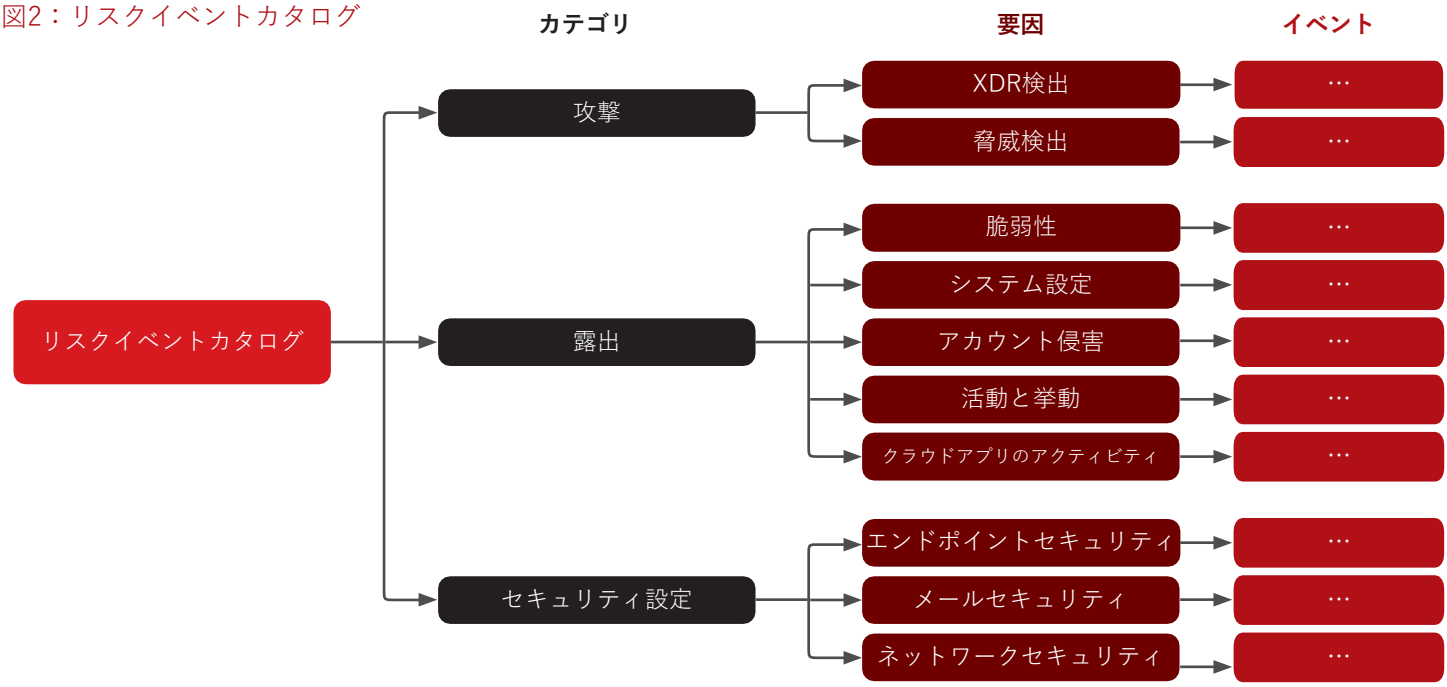
$$RiskScore = \sqrt{likelihood \times impact}$$

この公式は、機密性、完全性、可用性を測定して影響を受ける資産の重要度を評価することで、確率に基づいて加重されたリスクスコア要因として攻撃の可能性がどのように計算され、影響度がどのように計算されるかを示します。

リスクイベント、要因、およびカテゴリ

Trend Vision Oneを通じて実行されるリスク評価は、1,000を超えるリスクイベントに基づいています。 これらはそれぞれ、リスクを評価する基本的な単位です。 Trend Microおよびサードパーティのソリューションからのすべてのテレメトリデータ、検出、XDRアラート、脆弱性、およびその他のイベントが収集され、リスクイベントに変換されます。これらのリスクイベントは、3つのカテゴリと10の要因に分けられます。

図2：リスクイベントカタログ



このカタログ内の該当する3つのカテゴリは、次のように機能します。

攻撃カテゴリ(Attack)
セキュリティ分析エンジンを含むさまざまなセキュリティモジュールから脅威を検出することで、攻撃の可能性を判断するのに役立ちます。これにより、以前の脅威活動と既存の脅威活動、および関連するデータをとらえて、将来の悪意のある動きを予測するのに役立ちます。

露出カテゴリ(Exposure)
悪用される可能性がある環境内の弱点を表しています。 これには、共通脆弱性識別子(CVE)、セキュリティとクラウドの設定ミス、侵害されたアカウント、およびユーザ、デバイス、クラウドアプリからの異常な活動が含まれます。

セキュリティ設定カテゴリ(Security Configuration)
エンドポイント保護ソリューションや挙動監視などの特定の機能セットなど、環境内に導入済みおよび不足しているセキュリティコントロールが考慮されます。

組織が十分なセキュリティを構成している場合は、より適切に保護され、攻撃を受ける可能性が低いとみなされます。

これらの3つのカテゴリの加重和の計算は、さらに下の式で表されます。 図2のイベントは、組織の既存のセキュリティ製品やツールからのテレメトリを使用して生成されます。 これには、使用中のTrend Microソリューションのほか、SIEM(Security Information and Event Management)、SOAR(Security Orchestration, Automation and Response)、IDアクセス管理(IAM)、ファイアウォール、脅威インテリジェンス、ITサービス管理とのAPI統合が含まれます。

発生可能性

Trend Vision Oneのリスクイベントは、発生可能性と影響度の観点で評価されます。 発生可能性とは、リスクイベントが発生するか、特定の資産を悪用する確率を示します。一方、影響度とは、その資産にもたらされる損害の規模を示します。リスクイベントが直接または脆弱性の連鎖を通じてITインフラストラクチャの弱点を悪用する可能性は、確率に基づいて加重されたリスクカテゴリに変換されます。これは、個々の資産への攻撃、エクスポージャ、およびセキュリティ設定のカテゴリに基づいて、次の式で評価されます。

$$likelihood = P(attackEvents, exposureEvents, securityConfigurationEvents)$$

ここで、“P”は、これらのカテゴリで疑わしい資産に関連するすべての検出イベントからの可能性を考慮する機能です。各カテゴリで1から100までの間のスコアを受け取ります。スコアが高いほど、セキュリティの問題がより深刻であり、より最近のイベントが発生可能性の評価に大きな影響を与えることを示しています。

影響度

侵害が組織にもたらす被害の大きさを示します。資産の重要度を評価することで決定される攻撃対象領域が実質的に影響します。この評価は、前述のCIAトライアドに基づいており、対象の資産のビジネス関連のすべてのプロファイルタグの要件の要約を提供します。この影響度はこれらの要件から計算され、以下の式により1から5までの間のスコアで表現されます。

$$impact = Q(confidentiality,\ integrity,\ availability)$$

プロファイルタグの最大値は、各資産要件（機密性、完全性、可用性）に使用されます。次に、関数“Q”のマッピングを適用して、平均値を1から100の範囲の最終的な影響度として整数に変換します。影響度が大きいほど、組織内の資産がより重要になりますが、これは発生可能性の算出に似ています。

リスクスコア算出の例

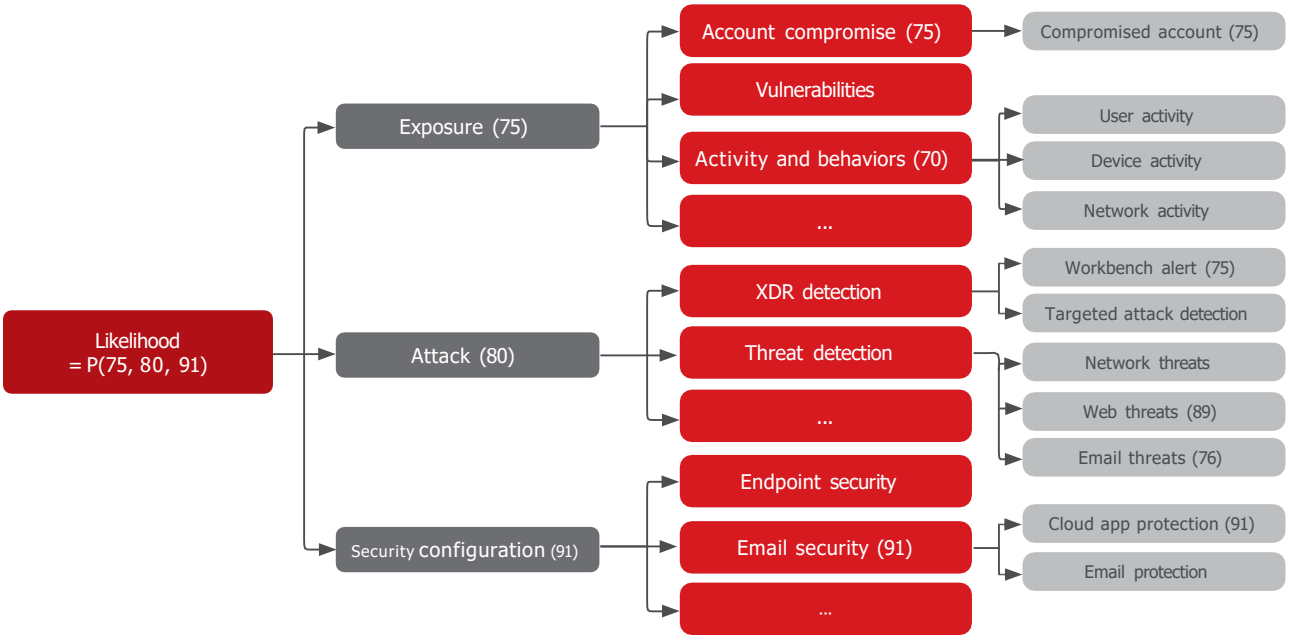
たとえば、リスクスコアが84のユーザー資産を考えてみましょう。リスクスコアは、攻撃、露出、およびセキュリティ設定のカテゴリイベントから計算される発生可能性スコアを評価することによって算出されます。

このユーザのアカウント漏洩によるアカウント識別イベントが73点、Microsoft Entra ID Protectionのリスク検出イベントが80点であったとします。これらの加重平均である75点が、イベントの上位レイヤーであるアカウントの侵害指標に集約されます。その他のイベントも、その加重平均を関連する指標に集約します。次に、指標からの加重平均は要因に集約され、攻撃、露出、およびセキュリティ設定のカテゴリに最終的に集約されます。

この3つのカテゴリの加重平均はそれぞれ75、80、91です。 ここから、この資産の発生可能性スコアを以下のように計算できます。

$$likelihood = P(75,\ 80,\ 91) = 82$$

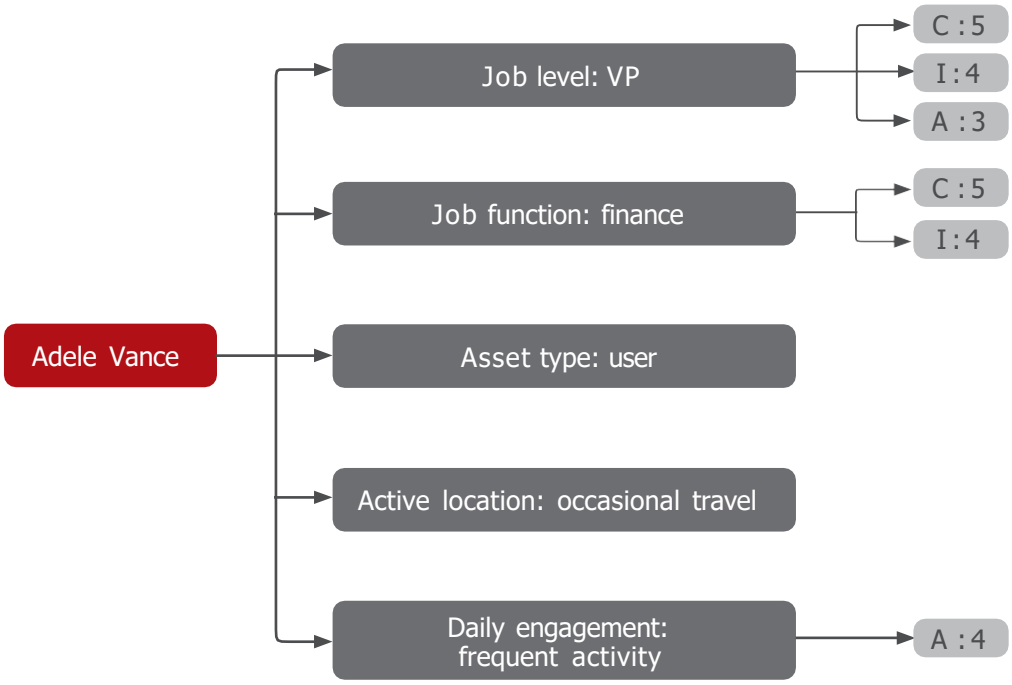
Figure 3：発生可能性スコアの算出例



影響度スコアは、機密性、完全性、可用性の要件の最も高い値とパーセントマッピングを使用して算出されます。以下の例では影響度を計算した結果が87となりました。

$$impact = Q(5, 4, 4) = 87$$

Figure 4：CIAトライアド要件から導き出される影響度



発生可能性と影響度が算出できたので、ユーザの全体的なリスクスコアを算出することができます。

$$RiskScore = \sqrt{likelihood \cdot impact} = \sqrt{82 \cdot 87} = 84$$

その結果、リスクスコアとして84が算出されます。新しいイベントが検出されると、同様の複雑な計算がすべての資産に対して継続的に実行され、リスクスコアが再計算されます。

リスク指標

数学的に公正な方法で組織の全体的なリスクを表すこの指標は、生成されたすべてのリスクイベントのリスクスコアを使用して、加重合計方法で計算されます。計算プロセスは、要因スコア(FactorScore)を従属するリスクイベントから直接取得します。 横展開または影響フェーズでの攻撃、ゼロデイ脆弱性などのイベントが発生した場合、以下に示す関数“F”で実装されたアルゴリズムに基づき、要因スコアが増幅されハイライトされます。これにより、以下に詳述するように、寄与要因の加重合計を計算することにより、カテゴリスコアを特定できます。

$$FactorScore = F(event_score_1, \ldots, event_score_n)$$
$$CategoryScore = sum(Wf_1 * FactorScore_1, \ \ldots \ , Wf_n * FactorScore_n)$$

(Factors = XDR detection/Threat detection/Vulnerabilities/System configuration/Account compromise/Activity and behaviors/Cloud app activity/Endpoint security/Email security/Network security)

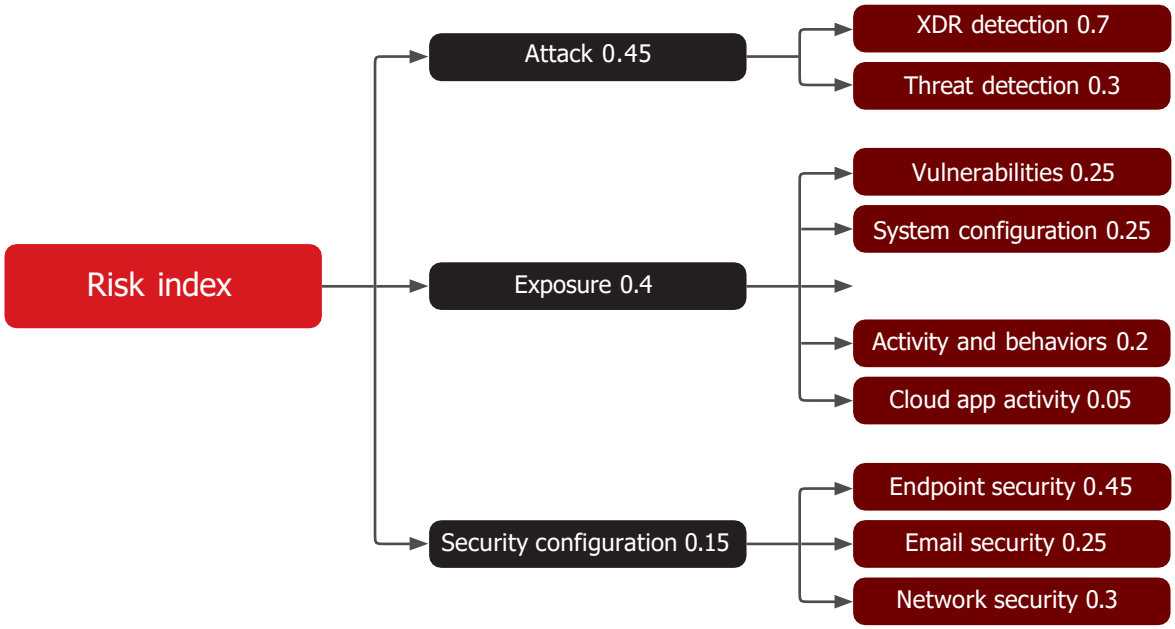
最後に、リスク指標は以下の3つのカテゴリの加重合計となります。

$$RiskIndex = sum(Wc_1 * CategoryScore_1, Wc_2 * CategoryScore_2, Wc_3 * CategoryScore_3)$$

(Categories = Attack/Exposure/Security configuration)

以下の図5に示すように、カテゴリスコアとリスク指標の加重は、Trend Microのセキュリティエキスパートによって事前に定義されています。これらの加重は、製品の研究開発のように、不定期または長期的に調整されます。一旦これらを環境に適用したら、加重の調整プロセスを完了する必要があります。これにより、リスクの現状とケーパビリティが明らかになります。このプロセスでは、ASRMソリューションから導き出される顧客が有効化したデータソースを利用します。事前に定義された加重と顧客が有効化したデータソースの組み合わせにより、関連する実際のシナリオに基づいて情報が生成および適用されます。

図5：リスク指標算出のための初期加重設定



攻撃指標

この継続的に監視されて更新される値は、過去24時間で検出されたすべてのサイバー脅威のうちの最大攻撃強度を示します。 攻撃指標の増加は、セキュリティ設定を確認および強化する必要がある可能性を示します。 攻撃指標は、既知の検出数、影響を受ける資産、およびそれぞれの固有の脅威タイプの重大度に基づいて計算されます。Trend Vision Oneは、エンドポイント、メール、ネットワーク、およびクラウドからXDRテレメトリを収集することで脅威検出を強化して、修復を迅速化します。

これらのレイヤー全体で関連付けられた脅威データを使用して、攻撃者の活動を識別し、複数の対応アクションを提案します。結果的に、XDRは攻撃指標の精度を向上させます。「攻撃の強度」は、以下の方程式によって、「影響を受ける資産数」に対する「脅威の総数」として、およそ計算されます。この値にMITRE ATT&CK™ framework.によって定義される影響度を乗じます。

$$attackIntensity \approx \frac{totalThreatCount}{impactedAssetCount} \times impact$$

攻撃指標は、以下に示すように、過去24時間以内のすべてのサイバー脅威の最大攻撃強度です。これは、新しい攻撃イベントが発生するたびに継続的に更新されます。

$$attackIndex_{today} = max(attackIntensity_1, \ldots, attackIntensity_n)$$

露出指標

この指標は、さまざまな要因によって組織がさらされるリスクを明らかにします。これには、パッチが適用されていない脆弱性の数と重大度、ソフトウェアの設定ミス、およびエクスプロイトへの影響の可能性が含まれます。

露出指標は、リスク指標の算出にも使用される事前に定義および調整された加重を使用して算出されます。ただし、露出指標では、露出カテゴリイベントに関連するイベントのみが方程式に組み込まれます。 ゼロデイエクスプロイトなど、タイムクリティカルな脆弱性のリスクイベントが発生した場合、関数「G」で実装されたアルゴリズムにより要因スコアが増幅されてハイライトされます。 露出指標の完全な方程式は以下に詳述します。ここまで完了したら、寄与要因の加重を合計して、露出カテゴリのスコアを取得します。

$$FactorScore = G(event_score_1, \ldots, event_score_n)$$

$$ExposureIndex = ExposureScore = sum(Wf_1 * FactorScore_1, \ \ldots, Wf_n * FactorScore_n)$$

(Factors = Vulnerabilities/System configuration/Account compromise/Activity and behaviors/Cloud app activity)

セキュリティ設定指標

セキュリティ設定指標は、さまざまなレイヤー、ソリューション、および機能にわたる組織のセキュリティコントロールのステータスを調査します。アナリストはシステム設定の傾向を時系列で表示および追跡できます。この指標は、リスク指標の算出でも使用されている事前に定義および調整された加重を使用して算出されますが、以下に示すように、セキュリティ設定カテゴリのイベントに関連するもののみを使用して算出されます。

$$FactorScore = H(event_score_1, \ldots, event_score_n)$$

次に、以下に示すように、寄与要因の加重を合計することで、セキュリティ設定カテゴリのスコアを取得します。

$$SecurityConfigurationIndex = SecurityConfigurationScore$$
$$= sum(Wf_1 * FactorScore_1, \ \ldots, Wf_n * FactorScore_n)$$

(Factors = Endpoint security/Email security/Network security)

リスクの概要

リスクの概要では、組織全体のリスク指標により組織のセキュリティ体制を一目で把握し、攻撃、露出、およびセキュリティ設定のリスクレベルを低、中、高のランキングによって補完表示します。

たとえば、露出指標は低いですが、攻撃指標は高いとします。 これは、組織に何らかの攻撃圧力があることを示していますが、露出が少ないため、適切に設定され保護されています。

このリスクの概要は、組織のセキュリティ体制に関するハイレベルな情報を表示する場所です。

リスクの概要の大まかな特長は、組織に対する全体的なリスクの一般的な概念を示しているということです。これには、どのコンポーネントが最も脆弱であるかも含まれます。

1つの画面上で、発生可能性と影響度によって決定される全体的なリスクスコアについて洞察を得ることができます。 それは、最大のリスク要因とスコア、傾向、および同業他社との比較などです。

リスクの概要には、リスクのある資産の優先順位付けされたリストも含まれます。これは、寄与要因の加重と算出により最もリスクの高いものに基づいています。継続的かつ自動化されたリスク分析により、組織に対する深い洞察が得られます。これは、セキュリティアナリストの作業負担を軽減し、経営陣に適切かつ迅速な脅威レスポンスのアクションを伝達します。

動的なリスク評価は、デジタル上の露出リスクを最小限に抑えるための最も重要な第一歩です

Trend Vision Oneは、意思決定に必要な情報を提供し、正確なリスク評価を可能にし、修復アクションに優先順位を付けるためのインテリジェントなガイダンスと推奨事項を提供します。リスクスコアに寄与する要因と算出方法を理解することで、リスクスコアを低減し、全体的なセキュリティ体制を強化するために必要な知識を身に付けることができます。

可視化と洞察を活用してセキュリティ運用を強化

セキュリティチームは、全社的なリスク指標を活用して、脅威の発生と潜在的な影響の高度なリスク評価を行うことができます。 これまでに説明したように、Trend Vision Oneのリスク評価では、運用に影響を及ぼす攻撃、露出、およびセキュリティ設定のイベントを考慮します。 組織内のリスクの包括的な可視化により、リスク要因を予測し、環境をプロアクティブに保護し、脅威を検出して防御し、その影響を軽減する機能が強化されます。 その後、このプロセスを洗練させることで、どんなに高度な攻撃に直面してもレジリエンスのあるゼロトラストアーキテクチャを展開できます。

リスクの洞察は、組織がゼロトラストアーキテクチャを実現するためのバックボーンとして機能しながら、このようなアーキテクチャが要求する継続的で厳しい監視要件を満たすことができます。

Trend Vision Oneによって特定されたセキュリティギャップを埋めることで、セキュリティ体制を時間をかけて是正することができ、ゼロトラストモデルに従ったアクションが可能になります。さらに、より安全な環境を広範囲にわたって確立する為に、ZTSAを活用している他組織から収集された膨大なインテリジェンスに貢献、あるいは使用することで、ますます増え続ける高度な脅威アクターと対峙することができるようになるでしょう。

TREND MICROは、トレンドマイクロ株式会社の登録商標です。本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。記載内容は2024年7月現在のものです。内容は予告なしに変更になる場合がございます。
Copyright © 2024 Trend Micro Incorporated. All rights reserved.