Qualys

エッセンシャルズガイド

必須事項: 攻撃対象領域の管理

ランサムウェア攻撃、データ侵害、フィッシング詐欺は、その量と複雑さを増し続けています。同時に、企業の攻撃対象領域は拡大し続けており、今日の脅威環境の要求に追いついていない旧来のサイバーセキュリティ対策や脆弱性管理（VM）プログラムを悪用しようとする脅威アクターに対し、組織はますます危険にさらされています。

ESG の調査によると、**組織の 69%が「インターネットに接続された未知の、管理されていない、または適切に管理されていない資産」を標的とした攻撃を経験しています。**その結果、攻撃対象領域管理（ASM）の人気が高まり、セキュリティ担当者は既存の VM プログラムをより高度なサイバーセキュリティで強化できるようになりました。しかし、これほど多くの選択肢がある中で、ASM の重要な要件は何でしょうか？

次の 5 つの必須要素に基づいて適切な ASM 戦略を構築します。

1 外部攻撃面管理 (EASM)

外部攻撃面管理（EASM）はセキュリティベンダーの間で流行語になりつつありますが、今日の多くの ASM ソリューションは依然としてネットワークの包括的な「外部」ビューを提供していません。そのため、セキュリティ担当者は、休眠状態の外部デバイスを利用して防御を突破しようとする悪意のある攻撃者に対して不利な立場に置かれます。ベンダーの ASM 機能を評価する際には、EASM 機能をテストしてください。外部スキャンのコストが法外に高くないこと、そして宣伝されている EASM 機能が実際にドメインとサブドメインをカバーできることを確認してください。包括的な EASM により、セキュリティ担当者は外部の悪意のある攻撃者の視点から洞察と資産インテリジェンスを獲得し、より詳細な脅威コンテキストと、VM を補完するプロアクティブな脅威ハンティングを提供できます。

How we do it

Qualys CSAM は、真に強力なネイティブ統合 EASM 機能を提供し、攻撃対象領域全体における継続的な検出、リスク評価、優先順位付け、そして修復を実現します。Qualys CSAM は、ドメインとサブドメインを含むあらゆる資産タイプに対する無制限のネットワークスキャンを含む単一プラットフォームから、社内の既知および社外の未知のインターネット接続資産（オンプレミス、マルチクラウド、子会社）の両方を網羅します。Qualys CSAM は、外部資産データマッピングと社内資産データを組み合わせることで、外部に公開されているデバイスの爆発半径を特定できる唯一の ASM ソリューションです。さらに、Qualys CSAM は Qualys Vulnerability Management, Detection and Response（VMDR）とネイティブに統合・導入されており、脆弱性管理、資産の可視性、そしてリスクベースの攻撃対象領域管理の最高の機能を組み合わせます。

2 資産のインベントリと検出

ASM は常に包括的なセキュリティスタックの一部です。そのため、選択した ASM ソリューションが既存のセキュリティスタック内の関連ツールとどの程度統合され、活用されるかをテストすることは不可欠です。例えば、ASM ソリューションが VM プログラムとシームレスに統合されていない場合、ASM はターゲットを絞ったポリシー適用や修復パスウェイに必要な主要な資産分析を活用できません。ASM への投資を最大限に活用し、ASM が VM プログラムを補完することを確実にするために、ASM が資産インベントリおよび検出プラットフォームと適切に連携することをテストしてください。

How we do it

Qualys Qualys CSAM は、統合された資産インベントリと可視性に加え、リスクベースの脅威の優先順位付けにより、コンテナ、データセンター、マルチクラウド資産を含む攻撃対象領域全体を網羅します。Qualys クラウドプラットフォームの一部として、Qualys CSAM は VMDR、ITSM、パッチ管理、SecOps 製品にネイティブに統合されたワークフローを備えており、資産メタデータの容易な運用化を支援します。その結果、オーケストレーションされ、シームレスに統合されたサイバーセキュリティツールスタックが実現します。

3 高度な分析

ほとんどのハイブリッドネットワークでは、エンドポイントエージェントを持たないデバイスが見つかることは珍しくありません。しかし、エージェントレスエンドポイントを容易に見つけ出し、修復することは重要です。エンドポイントエージェントを持たないデバイスは、環境にとって深刻なセキュリティ上の影響を及ぼすからです。エンドポイントの可視化と資産レベルまでの分析が円滑に行われなければ、セキュリティ担当者は、広大なネットワーク全体におけるエンドポイントポリシーの遵守状況や脅威のコンテキストについて、推測するしかありません。エンドポイントセキュリティと高度な分析においては、このようなモグラ叩きのような推測作業を避けるよう努めてください。ASM 戦略を構築する際には、ASM がサイバーセキュリティ分析に対するリスクベースのアプローチをサポートし、すべてのエンドポイントが考慮されていることを確認してください。

How we do it

業界で最も包括的な資産インベントリおよび VM ソリューションの一つである Qualys CSAM は、比類のない資産可視性と、資産レベルおよびエンドポイントレベルまでのリスクベースの脅威分析を提供します。また、25 以上の脅威ソースから 18 万件以上の脆弱性情報を蓄積し、常に拡大を続ける Qualys 脅威データベースにより、セキュリティ担当者は Qualys CSAM が常に最高かつ最新の脅威インテリジェンスを提供し、ASM 戦略を導くことを確信できます。

4 脆弱性、パッチ適用、ITSM サポート

多様化する物理資産と仮想資産のネットワークが拡大する中、多くの従来型資産管理ソリューションはゼロデイ脅威の特定能力に限界があります。IT チームとセキュリティチーム間のパッチ適用と、何よりも迅速な修復活動を促進することが重要です。脆弱性が特定された場合、その脅威の修復には業界平均で 8 日以上かかることが多く、48 時間以内に完了する攻撃を阻止し、エクスプロイトに対応するには遅すぎます。平均対応時間（MTTR）を短縮するには、IT 部門とセキュリティ部門の両方の関係者が、脅威の検出と対応をより迅速かつ的確に行うことができる、資産管理への新たなアプローチを必要としています。

How we do it

Qualys CSAM は、ServiceNow などの ITSM ツールとの統合に重点を置き、リスクベースの資産管理アプローチを提供するだけでなく、IT とセキュリティの連携を強化します。Qualys CSAM では、脅威は資産の重要度に基づいて優先順位付けされ、Qualys VMDR およびパッチ管理とネイティブに統合されています。これにより、組織はアラートから即座にアクティブなインシデント調査へと移行し、同じエクスプロイトの影響を受ける可能性のあるすべての資産を特定し、Qualys Patch Management を使用してパッチを適用できます。

5 クラウドの誤った構成の特定

企業はワークロードをデータセンターからクラウドに移行し、生産性と柔軟性の向上に貢献してきました。しかし、この「マルチクラウド」環境は、攻撃対象領域の拡大によりサイバーセキュリティリスクも増大させています。セキュリティ担当者は、クラウド資産とその構成状況を追跡できる正確な資産インベントリを維持するという課題に直面しています。この能力がなければ、クラウドの設定ミスがセキュリティ侵害につながるか、あるいは侵害が既に発生したことを示す兆候となる可能性があります。今日のマルチクラウド環境に適した適切な ASM 戦略を維持するには、クラウドの設定ミスをリアルタイムで特定することが不可欠です。

How we do it

Qualys CSAM は、Qualys VMDR と TruRisk を活用し、マルチクラウド環境全体の設定ミスを瞬時に特定し、侵害指標にリスクコンテキストを適用します。Qualys CSAM を活用することで、セキュリティ担当者はクラウドインスタンスや設定ミスが見逃されることがなく、対処も万全であると確信できます。

Essential Must-Haves: Attack Surface Management

CyberSecurity Asset Management（CSAM）は、お客様が脅威を継続的に発見、分類、修復することを可能にするクラウドサービスです。攻撃者が使用するのと同じ実用的なインテリジェンスを活用し、攻撃者が脆弱性を発見する前に、社内外の IT 資産のサイバーセキュリティ体制を目に見える形で強化します。既知および未知のインターネット接続資産をすべて検出し、リスクを 100%可視化・追跡します。

Qualys CSAM と外部攻撃サーフェス管理の詳細については、次の Web サイトをご覧ください。

www.qualys.com/csam

v240228