SOLUTION BRIEF

FortiRecon EASM による 外部攻撃対象領域の セキュリティ問題の迅速な発見と修復

概要

ネットワークのコンバージェンス、サプライチェーンの拡大、クラウド、サードパーティベンダーの利用などに対応するため、すべての CISO とセキュリティチームが継続的な可視性を必要としています。これらの変化がもたらす組織のデジタル環境への影響を理解することが極めて重要になっています。リスクとなるすべての対象領域を可視化できれば、ネットワークに追加されるすべての新しい資産、ソフトウェア、アカウントとそれぞれのセキュリティステータスを理解できます。

フォーティネットの DRP（Digital Risk Protection：デジタルリスク保護）ソリューションの一部である FortiRecon EASM（External Attack Surface Management：外部攻撃対象領域管理）は、組織のデジタル対象領域を継続的に評価することで、新たな弱点や脆弱性に加えて、新たなデジタル資産も検出して特定し、警告します。EASM は、新たに検出した資産、脆弱性、リスクを直ちに可視化し、修復アクションを提示します。

「障害や変更の管理、シャドー IT、クラウドテクノロジーの拡大、新しく発表される脆弱性など、あらゆる組織の攻撃対象領域が常に変化している。」[1]

今日の変化する環境で複雑化するリスク評価と資産管理

クラウドや SaaS（Software-as-a-Service）ソリューションの採用や拡大、新しいサードパーティソフトウェアのライセンス管理、企業買収、新しい資産やサービスの追加などにより、ネットワークは常に流動的です。ネットワーク環境が変化すれば、リスク対象領域は拡大します。高度な脅威の急速な進化に伴い、デバイス、ソフトウェア、アプリケーション、サービスの構成ミス、保護されていないシステム、パッチが適用されていないシステム、外部に公開されているサービスを迅速に検出することがますます重要になっています。

さらには、オンプレミス、仮想化、クラウド、リモートの新しい資産が加わることで、企業資産の管理がこれまで以上に困難になっています。承認されていない資産やサービス（シャドー IT）、その他のポリシー違反、承認されているものの侵害された企業資産などの存在により、今日の資産管理は複雑化しています。新たに追加したデバイス、ソフトウェア、アプリケーション、サービスのナレッジを直ちに取得できることは、今日のセキュリティ戦略において極めて重要です。

FortiRecon EASM（外部攻撃対象領域管理）が環境に存在するリスクと新しい資産を特定

FortiRecon EASM は、オンプレミス、仮想、クラウドの資産、関連会社や新たに買収した会社の資産を評価することで、包括的なデジタル資産の検出と管理を可能にします。

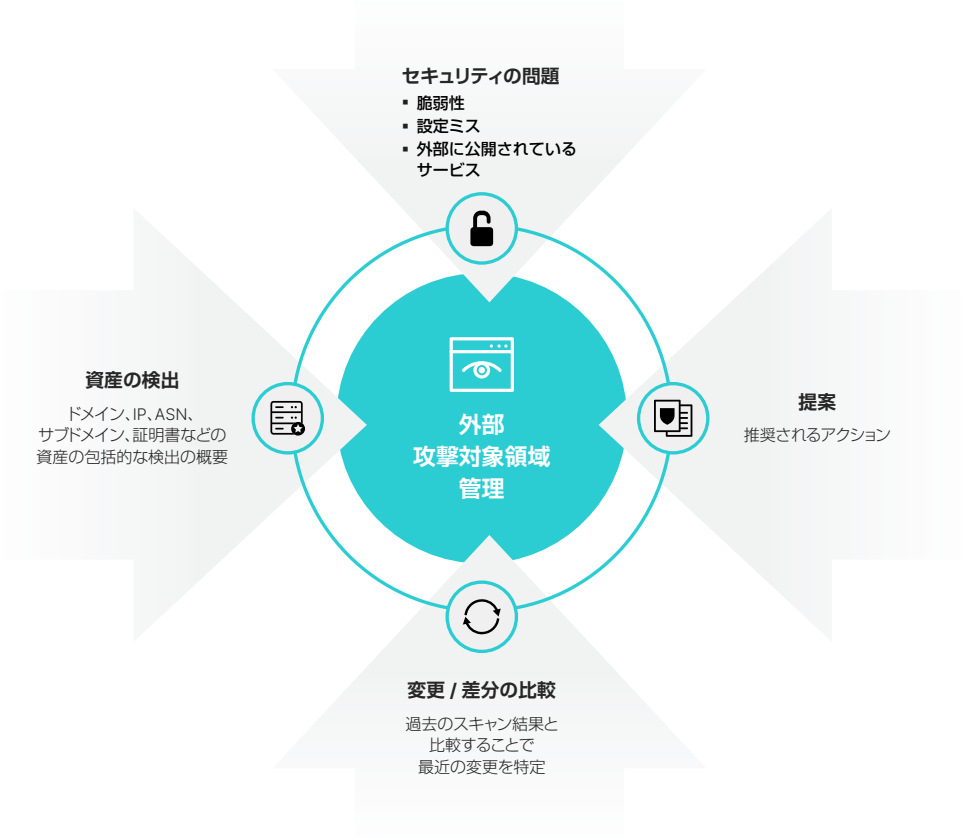
EASM は、デジタル資産を検出するだけでなく、セキュリティや GRC（ガバナンス、リスク管理、コンプライアンス）などの企業のリスクに責任を負うチームに、強力かつ実用的なインテリジェンスを継続的に提供します。何が変更され、何が修復され、何が未解決なのかを把握することで、コンプライアンスに対する説明責任を確実に果たすことができます。弱点のパターンや教育を強化すべき領域を特定し、それ以外の実用的インテリジェンスの活用により、リスク要因を理解し、それをプログラムで解決することができます。

EASM は、以下を特定することで、潜在的な弱点の迅速な解決を可能にします。

- 以下の手段で新たに検出された資産やサービス（シャドー IT を含む）
  - ASN（AS 番号）
  - IP アドレス
  - ドメイン
  - サブドメイン
  - ポート

- 以下のようなセキュリティの問題（パブリッククラウドにおける問題を含む）
  - SSL 証明書の問題
  - 脆弱性
  - 設定ミス
- 第三者による認証情報の流出

EASM の履歴ビューは、時系列的な変更のパターン、ポリシー違反、改善の領域、その他の潜在的なリスク領域の特定に役立ちます。セキュリティチームは、現在と過去の観点から問題の領域を解決すると同時に、精査が必要なリスクを正しく理解することができます。EASM の修復ガイダンスを利用することで、優先度を決めて貴重なリソースを最優先のリスクに集中させ、それ以外のリスクの減災計画をセキュリティチームが策定することができます。



FortiRecon によるデジタルリスクからの保護

FortiRecon EASM は、単独、FortiRecon Brand Protection と同梱、または FortiRecon Brand Protection と FortiRecon ACI の両方との同梱のライセンスでご利用いただけます。FortiRecon Brand Protection、EASM、ACI が付属する FortiRecon の完全ソリューションには、以下の機能が含まれます。

- デジタル資産の検出、アンダーグラウンドや公開フォーラムでの情報漏洩の検知、ブランド攻撃などへの迅速なアクション
- アカウント、Web サイト、不正モバイルアプリケーションのテイクダウンサービス
- 必要に応じて「外部から内部の」可視性を利用できる柔軟なライセンス
- 直感的 GUI（グラフィカルユーザーインタフェース）によるエグゼクティブからテクニカルレベルまでのビュー
- 脅威とインシデントに関する専門知識の提供（FortiRecon アナリストの付加解析からインシデントのレスポンス / 評価サービスまで）

フォーティネットによる包括的なセキュリティとサービスの提供

フォーティネット セキュリティ ファブリックは、FortiGuard 脅威インテリジェンスによる最新の保護を活用することで、攻撃ライフサイクルのあらゆる段階でエンドツーエンドのセキュリティを実現します。FortiGuard Labs 脅威リサーチチームは、オンデマンドの分析、評価、対策サービス、訓練も提供しており、豊富な知識と経験を活用して、世界中の数十億の脅威イベントを収集して分析し、関連性を特定します。これらの豊富な専門知識、経験あるダークウェブの研究者、多言語のインテリジェンス収集、HUMINT（ヒューマンインテリジェンス）のスペシャリストが協力してサービスを提供することにより、限定フォーラムや招待制フォーラムを含む最新の脅威活動に関する脅威インテリジェンスやデータへの比類ないアクセスが可能になります。生成される FortiRecon レポートのほぼ 4 分の 1 は、このサービスで収集されたヒューマンインテリジェンスのみに基づくものであり、リスクの最も現実的なビューを提供します。

終わりに

FortiRecon EASM は、フォーティネット セキュリティ ファブリックの拡張機能として、攻撃ライフサイクルの初期段階の保護を可能にし、ネットワークにすでに採用されているセキュリティ対策の上位に、デジタル資産のリスクプロファイルと修復のステップを追加します。FortiRecon のすべての機能の詳細については、Web サイトをご覧ください。

FortiRecon EASM のメリット

- サードパーティアプリケーションへの信頼性
- 新しく購入した資産の安全な追加
- 新たな脆弱性や外部への公開の迅速な修復
- 新たに追加された資産の迅速な検出
- 容易な変更管理
- 修復されたリスクの優れた可視性

[1] 「Maximizing Security Value Through External Attack Surface Management（外部攻撃対象領域管理によるセキュリティ価値の最大化）」、Jake Williams、Jim Wachhaus共著、SANS、2021年9月（英語）：https://www.sans.org/webcasts/maximizing-security-value-through-external-attack-surface-management/

フォーティネットジャパン合同会社
〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-FortiRecon-EASM-202208-R1