NTT AT

外部に漏洩・公開された情報資産を自動探索する可視化ツール

XCockpit EASM

自社のみならず、サプライチェーン全体のデジタル資産を守る、最新のAI監視システムです。

XCOCKPIT EASM

昨今、外部に漏洩した認証情報やセキュリティ設定が不十分なサーバー等の外部露出した資産からの侵入が増加し、リスク管理の重要性が高まっています。多様なサービスやサプライチェーンにまたがる外部資産のセキュリティ状況をリアルタイムで把握するのは難しく、認証情報の漏えいや攻撃につながるリスクを見逃しがちです。NTT-ATが提供するCuCraft社の「XCockpit EASM」は非侵入型の継続的なスキャン、ダークウェブにて販売されているIDや機密情報の調査を組み合わせ、企業の外部資産を自動検出・可視化することで、自社のみならずサプライチェーン全体のセキュリティを強化します。

POINT 1

高度な専門知識を必要とせずにリスクを洗い出し

自社で把握できていないネット上からアクセス可能な脆弱性やドメイン情報、ダークWeb漏洩情報を攻撃者の視点で洗い出し、自社だけでなくサプライチェーンに適用することで、関連企業のリスクを一元管理し連鎖的な被害を未然に防ぐことができます。

POINT 2

AIがリスクを分析してレベル判定し、対策案まで提示

洗い出したリスクはハッカー観点の攻撃の容易さや影響の大きさなど、さまざまな角度からAIが分析してリスクレベル判定します。また、AIが自然言語を用いて対策案まで自動で提示することで、対処の負担を軽減します。

POINT 3

検出したリスクをチケット化して対処までサポート

検出し評価されたリスクは「XCockpit EASM」のダッシュボード画面で一元化されて確認可能であり、対処状況を入力することで対処完了までの進捗管理ができる事から、効率的な対策実施が可能になります。

セキュリティ Security

https://www.ntt-at.co.jp/product/xcockpit_easm/

XCockpit EASMの特長

● 外部への資産漏えい管理

外部に公開されているデジタル資産をハッカーの視点で自動探索し、可視化します。システムの構成要素や個々のコンポーネントを分析し、リスク評価モデルを作成し、攻撃者に標的とされる可能性のある情報を特定します。企業は把握していない資産を認識し、潜在的な脆弱点を早期に発見できます。

● AIによるセキュリティ・コンプライアンス評価

・15種類の情報セキュリティ・リスク評価指標を備え、多様な情報セキュリティ管理システムや法規制に対応しています。

● デジタル証明書漏洩追跡システム

・インターネット上のオープンウェブやダークウェブにおいて、企業の正規デジタル証明書の公開または販売状況を検知します。

● 企業情報漏えいリスクの継続的管理

・企業の外部資産の変化に関する情報を提供し、リスクチケットの過去から現在にかけての改善実績を継続的に追跡可能です。

想定ユーザー

● このような方に最適です。

・サプライチェーンを含む外部露出資産とリスクの全容を把握したい
・ダークWebに漏洩した認証情報がないか確認したい
・外部露出資産のリスク対策を効率的に実施したい

お問い合わせ

https://www.ntt-at.co.jp/product/xcockpit_easm/

※記載された社名、各製品名等は、各社の商標または登録商標です。※本カタログ記載の内容は予告なく変更することがあります。※カタログ記載内容 2025年11月現在

NTTアドバンステクノロジ株式会社

NTT AT

ADアカウント等の悪用による攻撃パスをAIで予測し防御を強化

XCockpit IASM

ActiveDirectoryに関する高度な専門知識を必要とすることなく、AIがリスクの洗い出しと対策案を提示します。

XCOCKPIT IASM

現在、多くの企業においては、ActiveDirectoryやEntra IDの権限構造が複雑化しており、誤った権限付与や設定ミスといったセキュリティ上の問題が発生しやすくなっています。これにより、低権限アカウントからでも重要資産へのアクセスが可能となるようなリスクを抱えてしまうことから、その攻撃経路（AttackPath）を悪用した内部不正を防ぐため早急な対策が必要です。
NTT-ATでは、台湾で防衛・警察・政府機関で培った豊富なサイバーセキュリティ知見とAI技術を提供するCyCraft社のサービスを活用し、ADやEntra IDのリスク分析を自動化し、普段の運用にてリスク対策を実施できるサービスをご提供します。

POINT 1

高度な専門知識を必要とせずにリスクを洗い出し

アカウント管理の不備、グループ等への過大な権限の割り当て、各種設定に関する脆弱性、ActiveDirectory特有の攻撃に対する防御策の不備などを自動的に洗い出せるため、担当者の負荷を軽減し、効率的な管理が可能です。

POINT 2

AIがリスクを分析してレベル判定し、対策案まで提示

Windowsの管理機能で確認可能な設定を分析し、システムの侵害を可能とするAttack Pathを探し出します。また、これらのリスクを低減するための対策案をAIが提示するため、攻撃経路を事前に遮断可能となり、情報漏洩や内部侵害のリスクを大幅に軽減します。

POINT 3

検出したリスクをチケット化して対処までサポート

検出されたリスクはダッシュボード画面で確認可能であり、対処完了までの進捗が一元管理できます。また、リスク検出から対処までワンストップで管理できるため、リスク残存防止や今後の類似リスクへの対応の迅速化が期待できます。

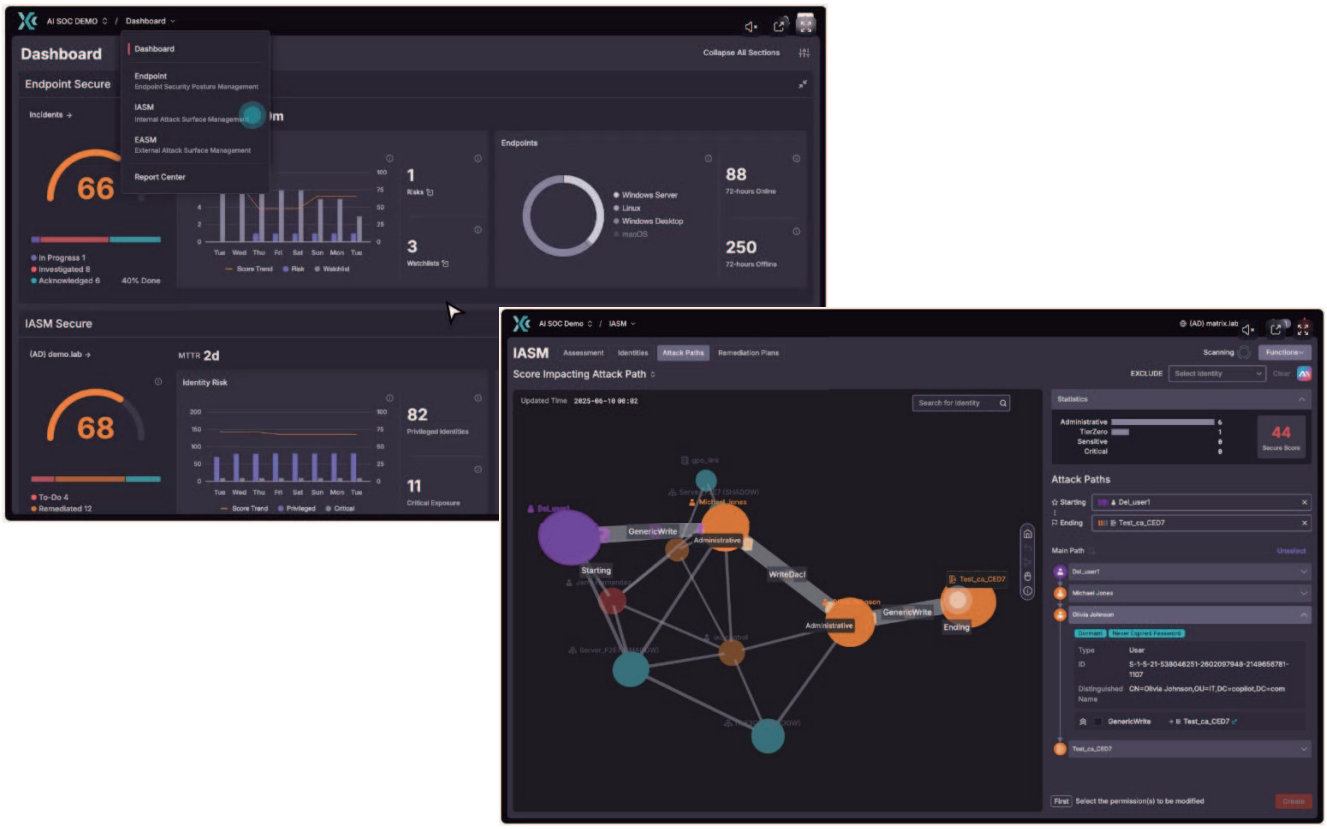
セキュリティ Security

https://www.ntt-at.co.jp/product/xcockpit_iasm/

XCockpit IASMの特長

● アカウントを悪用した攻撃パスの可視化やシャドー特権アカウントの検出により、セキュリティ体制を強化

ActiveDirectoryに参加しているPCにてスキャンを実行し、そのデータをクラウドのサイトへアップロードすることで、AIが自動でデータを分析してリスクアセスメントを実施し、結果がダッシュボード画面に表示されます。
お客様はダッシュボード画面でActiveDirectoryの設定に関するリスクと対処案を確認できるほか、AIが生成したレポート概要なども参照可能です。またこれらのリスクについてはチケット化し、対応完了までを一元的に管理できます。



● アカウント影響度分析

・AIによる特権アカウントの影響度分析、攻撃者による攻撃パスの予測、企業内アカウントの特権境界の調査結果を提供します。

● 脅威の前兆監視

・特権アカウントのアクティビティを監視し、アカウントを悪用する攻撃手法を検出し、攻撃の前兆を即座に特定します。

● 可視化によるアカウント管理

・組織のADアカウント管理におけるセキュリティ指標の定量化で、企業全体のセキュリティポスチャーの向上を実現します。

想定ユーザー

● このような方に最適です。

・企業等の情報システム部門やセキュリティ部門で、ActiveDirectoryやEntra IDの管理担当者
・内部ネットワークの権限設定ミスや攻撃経路の可視化・対策に課題を抱える組織
・複雑なID管理と高度なサイバー攻撃リスクに対応が求められる担当者

お問い合わせ https://www.ntt-at.co.jp/product/xcockpit_iasm/

※記載された社名、各製品名等は、各社の商標または登録商標です。※本カタログ記載の内容は予告なく変更することがあります。※カタログ記載内容 2025年11月現在

NTTアドバンステクノロジ株式会社