i-CYBERTECH アセスメントサービス

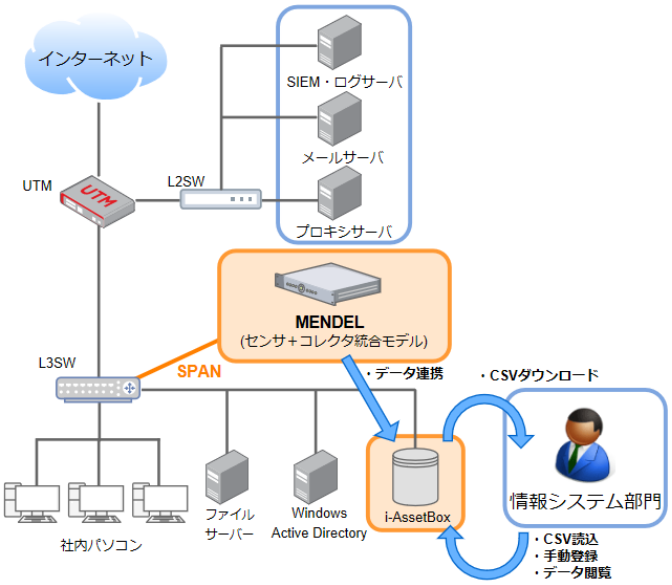
デバイスアセスメントとセキュリティアセスメントを一度に実現。未知のマルウェアによる脅威への備えを万全にします

組織のネットワーク上に存在する、あらゆるデバイスの管理・把握を行います。さらに、未知の脅威をもたらすマルウェアへの対策も強化することができます。

● i-Cybertech アセスメントサービスの特徴

1. アセスメントツールの導入時、既存のネットワークに影響を与えません。
2. 組織のネットワークに接続するあらゆるデバイスを詳細に調査し、把握することが可能です。
3. 今後、増加が予測されるIoTデバイスや、OT系の制御システムなど未対応デバイスも検知することができます。
4. 管理用ソフトウェア（i-AssetBox）を導入することで、自組織でのデバイスアセスメントが可能となります。

● 構成図



i-AssetBoxの機能

1. MENDELからデバイス・ネットワーク・セキュリティ情報が、i-AssetBox（自社製品）に定期的に書き込まれます。
2. i-AssetBoxにアクセスすると、書き込まれたデバイス情報を参照できます。さらに、CSV形式で一覧を取得することができます。
3. i-AssetBoxの情報は、データをCSVの読み込みや手動登録により、更新することができます。

● デバイスアセスメント

社内ネットワークに接続されている端末の棚卸しを行うことで、社内管理外（不正な端末）や管理漏れの端末、脆弱性のある端末を検出することができます。

【i-AssetBoxに格納される情報一覧】

番号	項目名	説明
デバイス		**端末に関連する情報を表示しています。**
①	デバイスの種類	端末がよく利用しているサービス、またはプロトコル（N/A：設定なし）
②	ホスト名	端末のホスト名（N/A：設定なし）
③	IP アドレス	端末の IP アドレス
④	Vlan	端末が所属している Vlan 名
⑤	MAC	端末の MAC アドレス
⑥	ベンダー	NIC のベンダー
⑦	イベントの種類の数	端末で発生したイベントの種類の数
⑧	リスク	端末の危険度（高、中、低） 高いものから優先に対応が必要
ネットワーク		**トラフィック量の多い通信の TOP5 をプロトコル別に表示します。**
⑨	全体トラフィック量	端末全体の受信トラフィック量と送信トラフィック量
⑩	プロトコル	通信で使用しているプロトコル名
⑪	ポート	通信で使用しているポート番号
⑫	IN	該当通信の受信トラフィック量
⑬	OUT	該当通信の送信トラフィック量
セキュリティ		**イベント発生数をカテゴリ別に表示します。**
⑭	マルウェア	マルウェアに関するイベント
⑮	脆弱性の利用	脆弱性を利用する攻撃パターンの通信に関するイベント
⑯	異常	異常な通信に関するイベント
⑰	偵察	資産のデータを収集する通信に関するイベント
⑱	ポリシー	MENDEL であらかじめ定義されたポリシーに違反している通信に関するイベント
⑲	通知	通知に関するイベント
⑳	状態	重大：深刻度 8 以上のイベントが発生 高：深刻度 7 以上のイベントが発生 中：深刻度 4 以上のイベントが発生 低：深刻度 1 以上のイベントが発生 正常：イベントが発生していない
㉑	件数	発生したイベントの種類数

・検出ホストの集計

有効MACアドレスとそのMACアドレスを使用する
IPアドレスの紐づけや、VLAN・セグメント別集計を行います。

・デバイス報告書

デバイス情報、プロトコル別トラフィック情報TOP3、
カテゴリ別イベント発生数、高深刻度イベントTOP3
等の情報を表示します。（CSVファイルでの提供も可能）

深刻度高イベント TOP3		端末で発生したイベントのうち、深刻度の高いもの TOP3 を表示します。
㉒	深刻度	イベントの深刻度 8～10：優先度高の調査が必要 4～7：優先度中の調査が必要 0～3：優先度低の調査が必要
㉓	イベントタイトル	イベントの概要説明
㉔	ID	イベントの ID
㉕	時刻	イベントの発生日
㉖	検出機能	イベントを検出した MENDEL の機能 ・ネットワークの振る舞い分析 ・IDS ・相関分析
㉗	送信元	イベントの送信元ホスト名、IP アドレス （ホスト名が未設定の場合は非表示）
㉘	宛先	イベントの宛先ホスト名、IP アドレス （ホスト名が未設定の場合は非表示）
㉙	プロトコル	イベントで使用しているプロトコルとポート番号
㉚	イベントカテゴリ	イベントに該当するカテゴリ ※セキュリティ⑭～⑲と一致

※セキュリティに関しては、
追加ライセンスが必要となります。

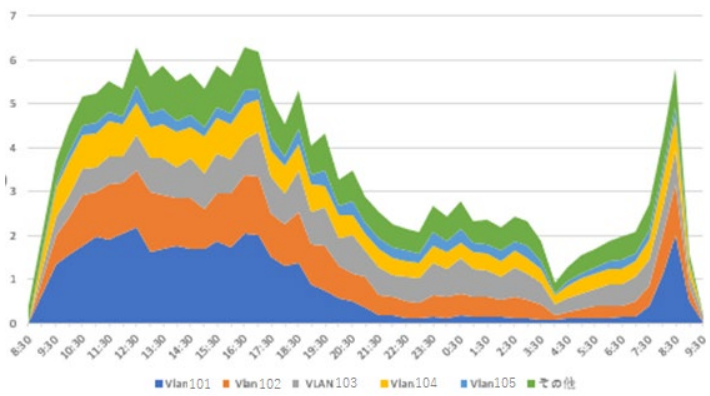
ネットワークアセスメント

ネットワークトラフィックやパフォーマンスの分析により、ネットワークのループやボトルネック等、
課題の原因を特定することができます。

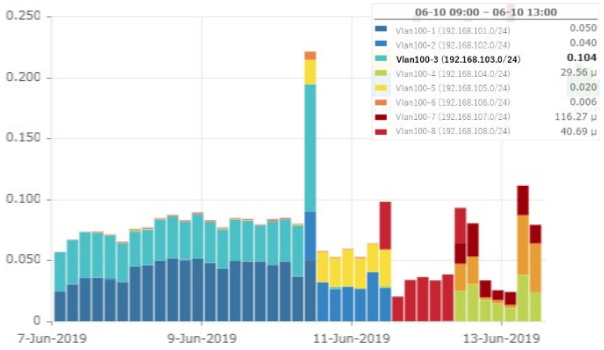
・トラフィック量の推移
　ミラーポート流入の全体トラフィック量（IN、OUT）の推移を確認が可能
　VLAN、セグメント単位でのトラフィック解析が可能

・各種パフォーマンス情報
　VLAN、セグメント単位、またサービス単位でのパフォーマンス（応答時間）変動の確認が可能

【VLAN別トラフィック量】



【VLAN/セグメント単位の応答時間推移】



セキュリティアセスメント

デバイスアセスメントにより検出したセキュリティイベント結果から、優先順位付けした対応方針のご提案が可能です。

深刻度: 10

内容：　SMBログオンの失敗
検知機能：　フロー分析

NBAとIDSを組み合わせて検出

イベントの概要：　10.1.1.2　がADサーバ　10.2.1.4　こ対して、複数のSMBログオンを試したが失敗しました。

危険性：SMBで複数のログオンを試したが失敗しました。ADサーバーは、Windows Server 2003 R2 3790 Service Pack2 が利用されていることが確認できました。また古いバージョンのSMB、NTLMも利用されていることが確認できました。この環境は脆弱性攻撃であるEternal Blueで実行できる環境です。そのため、Eternal Blueに対応するパッチがインストールされているかを確認する必要があります。

イベント例：
・SMBによる異常
・ネットワーク異常検知
・偵察(情報収集)
・脆弱性攻撃
・通知・異常な通信等

【検知されたイベント】▲

【課題および対策】▶

検知されたイベント、課題および推奨される対策は、画面上でわかりやすく表示されます。（図はサンプル）

危険　緊急対策が必要なセキュリティ課題一覧

結果・課題	ご提案内容
① 特定ホストから脆弱性検査コマンドが実行されました。（Apache Struts2の脆弱性を突く攻撃、リモートコマンドの実行など）	攻撃や不正アクセスが発生したときに、ネットワークふるまいを検知するシステム（MENDEL）やSIEMなど、ログ分析システムが導入されているか確認してください。 もし、導入されていない場合は、攻撃が成立する前に検出できる仕組み、該当端末をネットワークから排除できるような仕組みが必要です。
② ブラックリストに登録されているNTPサーバに接続が発生しました。	ブラックリストに登録されているアドレスに向けて接続できないように、FWもしくは、プロキシサーバにおいてフィルタリングを実施してください。タイムサーバを社内ネットワークに設置することによって外部にNTP通信を出さないようにする方法も有効です。タイムサーバはセキュリティの問題以外にも、高精度な時間設定が求められる場合にも効果的です。
③ SMB通信において多数ログインが失敗していることを検出しました。	フローの中身を確認によると、ADサーバのOSバージョンが古いことが判明しました（Windows2003 R2）。サーバをバージョンアップしてください。

導入実績

下記の企業・団体様に、弊社のアセスメントサービスを利用いただいています。（2020年1月現在）

大手通信会社、地方公共団体、独立行政法人、鉄道会社、インフラ系企業、
グローバル製造業、研究機関ほか

i-CYBERTECH
アセスメントサービス

iSEC information security inc.
情報セキュリティ株式会社
〒650-0012 神戸市中央区北長狭通 4 丁目 9-26 西北神ビル 3･7･8 階
TEL：078-381-8980（10:00~17:00 土・日・祝除く） FAX：078-381-8979
E-Mail：inquiry@isec.ne.jp URL：https://isec.ne.jp/