AMIYA

サイバー攻撃自動検知パック

2 インフラを網羅するALog

社内インフラの「**証跡管理**」はお済みですか？

ALog

FW・UTM

ADサーバ

ファイルサーバ

ストレージ

データベース

Webプロキシ

PC

ミドルウェア

HCI

クラウドサービス

Microsoft 365

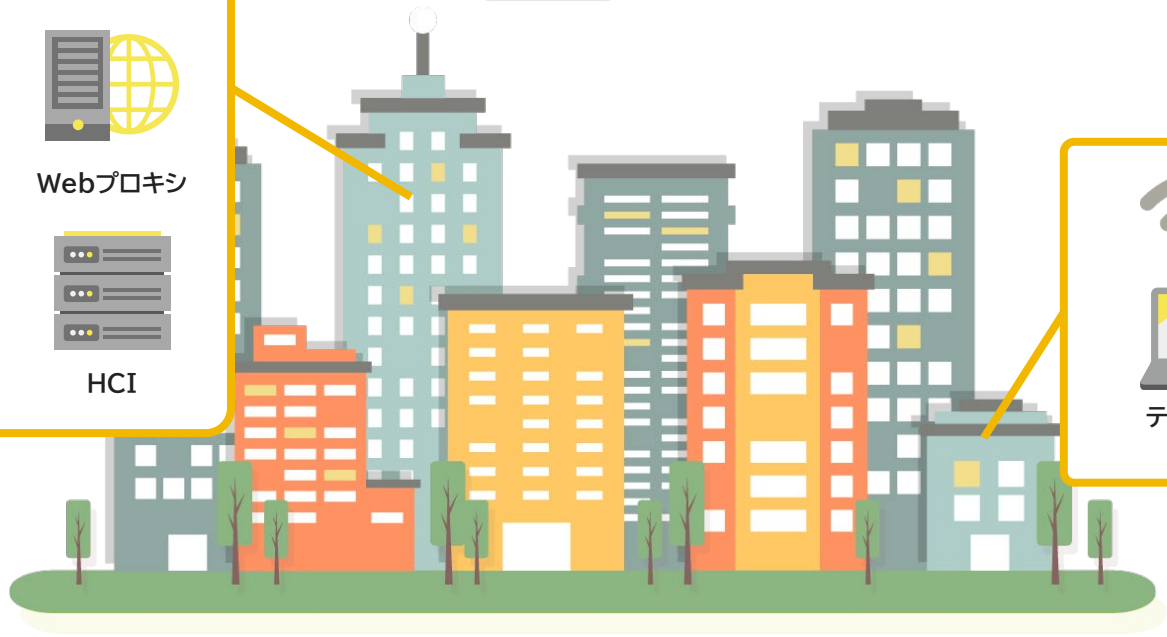
Google Workspace

aws

okta

Dropbox

box



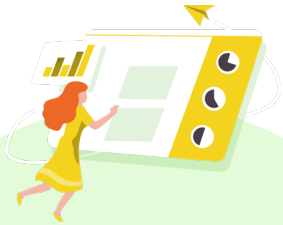
テレワーク用
PC

3 サイバー攻撃自動検知パック

専門知識不要！スグに始められる自動検知パック

最も効果のある監視項目を分析

典型的な攻撃パターンの証跡内容と最も効果的な監視項目を分析してパック化。



要件定義不要

機器ごとの取り込み/アラート/レポート、全てのテンプレートが事前定義済み。
難しい要件定義と設定は不要。

IPA(※)やJPCERT(※)ガイドラインに対応

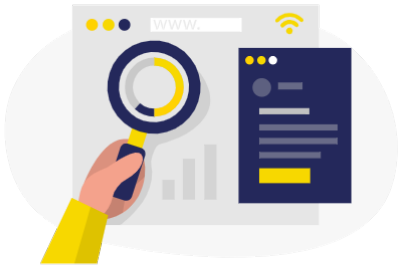
サイバーセキュリティに特化したガイドラインに沿った定義と対処を実施。

※ IPA： 独立行政法人 情報処理推進機構
※ JPCERT ：Japan Computer Emergency Response Team

サイバー攻撃 3つのフェーズ

「侵入」「情報取得」「持ち出し」

素早い検知が攻撃の被害を最小限に食い止める



侵入

攻撃者が企業の内部ネットワークに侵入を試みるフェーズ。フィッシングメール等でマルウェアを配布し、認証サーバへ必要な権限取得を試みる。

情報取得

権限を取得した攻撃者は、目的とする情報の捜索を開始。ファイルサーバ等の重要データの保管先を見つけ、目当ての情報を取得。

持ち出し

目的の情報を取得した後、攻撃者は外部へデータを持ち出す。インターネット上のサーバへデータを送信。

- ☑ 対策が難しそう？
- ☑ 効果的な監視方法を探している？
- ☑ 具体的に何から始めたら良いか分からない？

5 侵入フェーズ

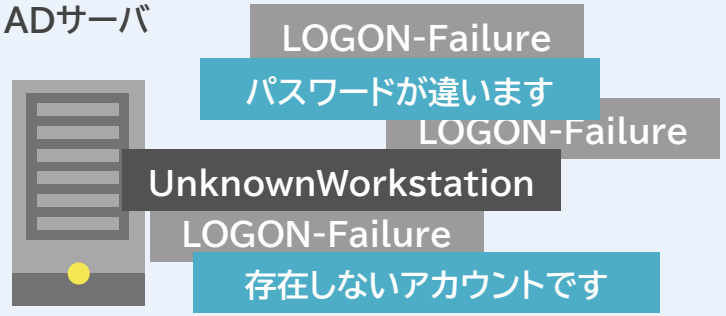
攻撃の最初のステップは企業の内部ネットワークに侵入し、必要なユーザ権限を入手すること。

ALog

ログオンチャレンジ

感染PCを踏み台に
社内アクセスを試みる

大量のログオン失敗



不審なログオン失敗をALogが自動検知

自動化パックで自動アラート

- ✓ 大量のログオン失敗
- ✓ 機械的なログオン試行
- ✓ 存在しないアカウントからのログオン失敗

6 情報取得フェーズ

手に入れた権限を用いて目的の情報捜索を開始。
通常は起こりえないファイルアクセスが発生することも。

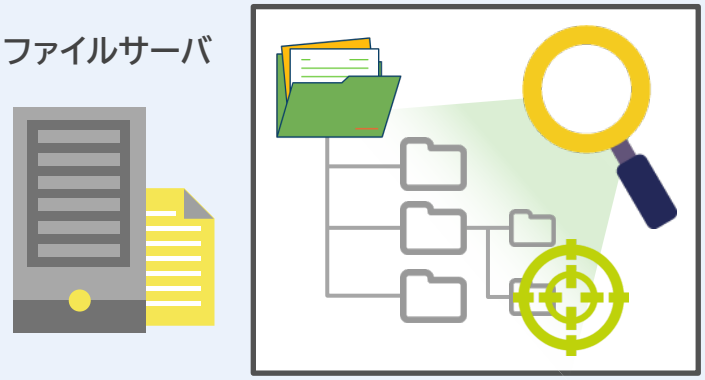
ALog

情報の検索

攻撃者による重要情報の検索

不審なアクセス

ファイルサーバ



いつもと違うファイルアクセスや
短時間での大量アクセスを検知

自動化パックで自動アラート

- ✓ 大量のファイル読み込み
- ✓ AIファイルパス検知
- ✓ 特権IDでのファイル操作
- ✓ 大量のファイル名変更

7 持ち出しフェーズ

サイバー攻撃は、手に入れた情報を外部サーバに送信することで完了する。
インターネット出入口の通信ログを監視することがポイントに。

ALog

情報の持ち出し

取得した情報の
アップロードを試みる

大量通信

ファイアウォール

プロキシサーバ

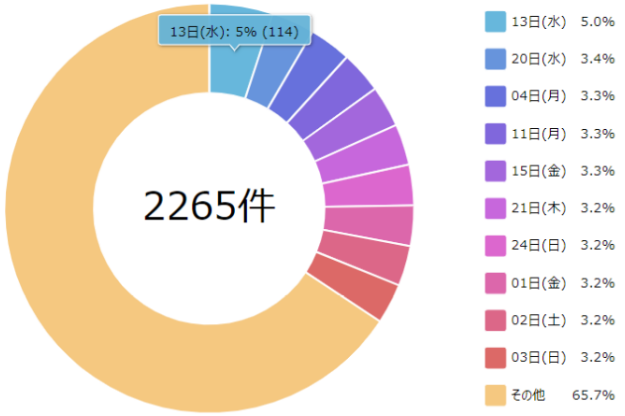
特定のIPが大量にデータを
アップロードしているのを検知

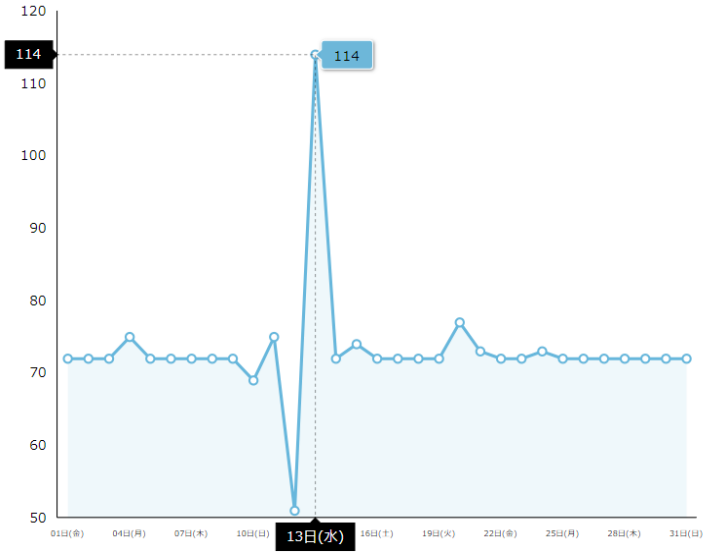
自動化パックで自動アラート

- ✓ 未許可ポートの利用
- ✓ WEB利用状況の監視
- ✓ IP別の大量アップロード/ダウンロード

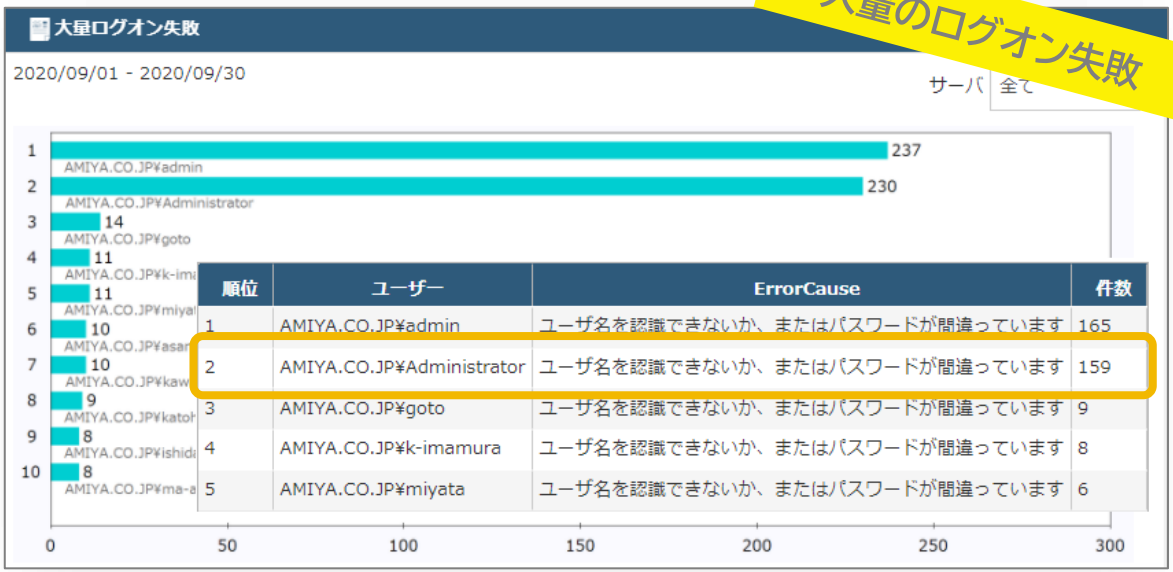
8 レポートイメージ

アラート/レポートを自動化





大量のログオン失敗



順位	ユーザー	ErrorCause	件数
1	AMIYA.CO.JP¥admin	ユーザ名を認識できないか、またはパスワードが間違っています	165
2	AMIYA.CO.JP¥Administrator	ユーザ名を認識できないか、またはパスワードが間違っています	159
3	AMIYA.CO.JP¥goto	ユーザ名を認識できないか、またはパスワードが間違っています	9
4	AMIYA.CO.JP¥k-imamura	ユーザ名を認識できないか、またはパスワードが間違っています	8
5	AMIYA.CO.JP¥miyata	ユーザ名を認識できないか、またはパスワードが間違っています	6

総合スコア

1	網屋 太郎	AMIYA\taro	72.4
2	網屋 次郎	AMIYA\Jiro	21.7
3	網屋 花子	AMIYA\Hanako	5.1
4	マイケル	AMIYA\Michael	4.2
5	Yutori	AMIYA\Yutori	1.0

頻度スコア

1	網屋 次郎	AMIYA\Jiro	21.7
2	網屋 太郎	AMIYA\taro	7.2
3	Yutori	AMIYA\Yutori	1.0
4	マイケル	AMIYA\Michael	0.6
5	網屋 花子	AMIYA\Hanako	0.0

パススコア

1	網屋 太郎	AMIYA\taro	65.2
2	網屋 花子	AMIYA\Hanako	5.1
3	マイケル	AMIYA\Michael	3.6
4	網屋 次郎	AMIYA\Jiro	0.0
5	Yutori	AMIYA\Yutori	0.0

監視項目お品書き

ALog

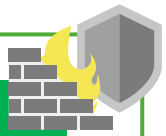
Windows ActiveDirectory

- 短時間に大量に行われたログオンチャレンジ
- 存在しないアカウントでのログオンチャレンジ
- 無効なアカウントによるログオンチャレンジ
- イベントログ削除
- システム監査ポリシーの変更
- ユーザーアカウントの作成/削除
- 特権ユーザのログオン

i-Filter Webプロキシ

- ファイル共有サービスへのアップロードサイズ
- ファイル共有サービスへのアップロード回数
- 業務時間外のアクセス監視
- 不正アクセスの把握

Fortigate FireWall



- ファイル共有サービスへのアップロードサイズ
- 業務時間外のアクセス監視

SQL/Oracle データベース

- 規定外ツールによるDB操作

Windows/NAS ファイルサーバ

- ランサムウェア感染の監視
- サーバへの直接的なログオンチャレンジ

自動化パック提供中

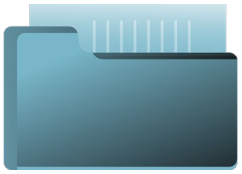
自動化までの3STEP

1
パックをダウンロード

- サポートサイトより
  利用したいパックを選択

2
インポートする

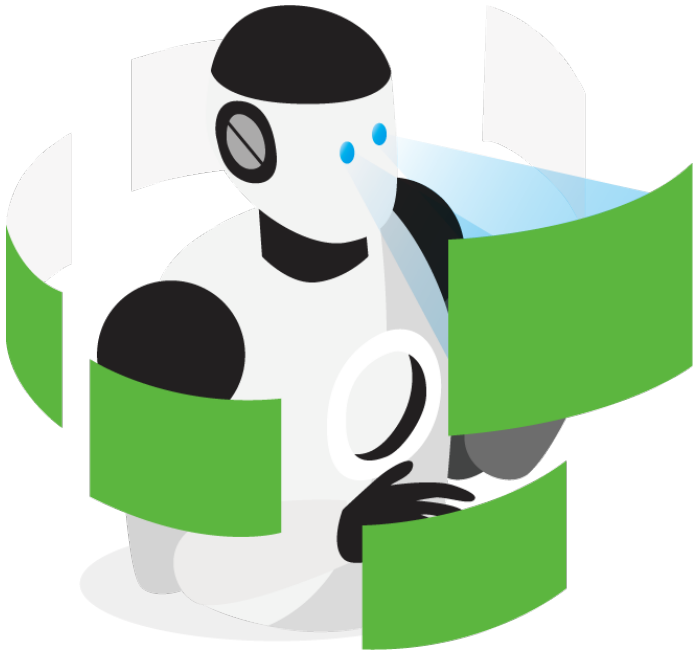
インポートファイルは1つだけ



- ダウンロードしたパックを
  ALog環境にインポート

3
機器名を登録したら完了

- インポートしたレポート/アラート
  より検知対象の機器名やドメイン
  情報を入力



お問い合わせ先

株式会社網屋

データセキュリティ事業部

TEL: 03-6822-9996（ダイヤルイン）

Mail: bv-sales@amiya.co.jp

AMIYA