

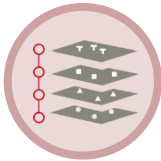
内容

■ 検知までのステップ



1. ログ収集

ログ管理サーバーにログを収集
(ログ管理サーバー例)
Splunk, IBM Qradar, ArcSight
McAfee SIEM, Exabeam Data
Lake など



2. ログの紐づけ・整理

ログを自動的にユーザー毎に
紐づけ・整理



3. ベースライン作成

機械学習を使い、ユーザー毎の
活動のベースライン(通常状態)
を作成



4. 検知・可視化

ユーザー毎のベースラインから
逸脱した行為を監視・検知
ユーザー毎にすべての活動を
タイムラインで可視化

■ 画面例

サーバーへのアクセスログ、データベースへのアクセスログ、データベースのクエリ、次世代FWのログが時系列に人にひも付いて表示

属性情報

Barbara Salazar [bsalazar.sa]
Human Resources Coordinator Chicago

RISK SCORE: 219

自動的に通常状態を学習

普段使う端末

普段アクセスするサーバー

普段使用するオフィス

普段のログイン時間帯

ベースラインと異なる異常行動一つ一つをスコアリング

毎日をベースラインと比較、スコアリング

部署として初めてのDBへのアクセス

個人として初めてのDBへのアクセス

次世代FWの検知アラート

参考費用

素材名 (開発元)	概要	動作環境
Exabeam(exabeam,Inc)	様々な機器のログを、「人軸」で管理し、機械学習を使って一人ひとりの通常業務を学習します。普段と異なる業務行動を可視化することで、標的型攻撃と内部不正を検知・追跡します。	アプライアンスで提供

※記載の会社名、商品名は、各社の商標または登録商標です。
 ※記載された情報は、予告なく変更することがあります。
 ※記載の内容は、2019年11月現在のものです。



% \$ #) & ~ \$ % # &
 8 z ` T \ _ ` - ` - ` f f _ z \ a Y b 3 V f !] c ! Y h] \ g f h ! \
 [g g c f - " " j j j ! Y h] \ g f h ! V b