内容

■ 検知までのステップ

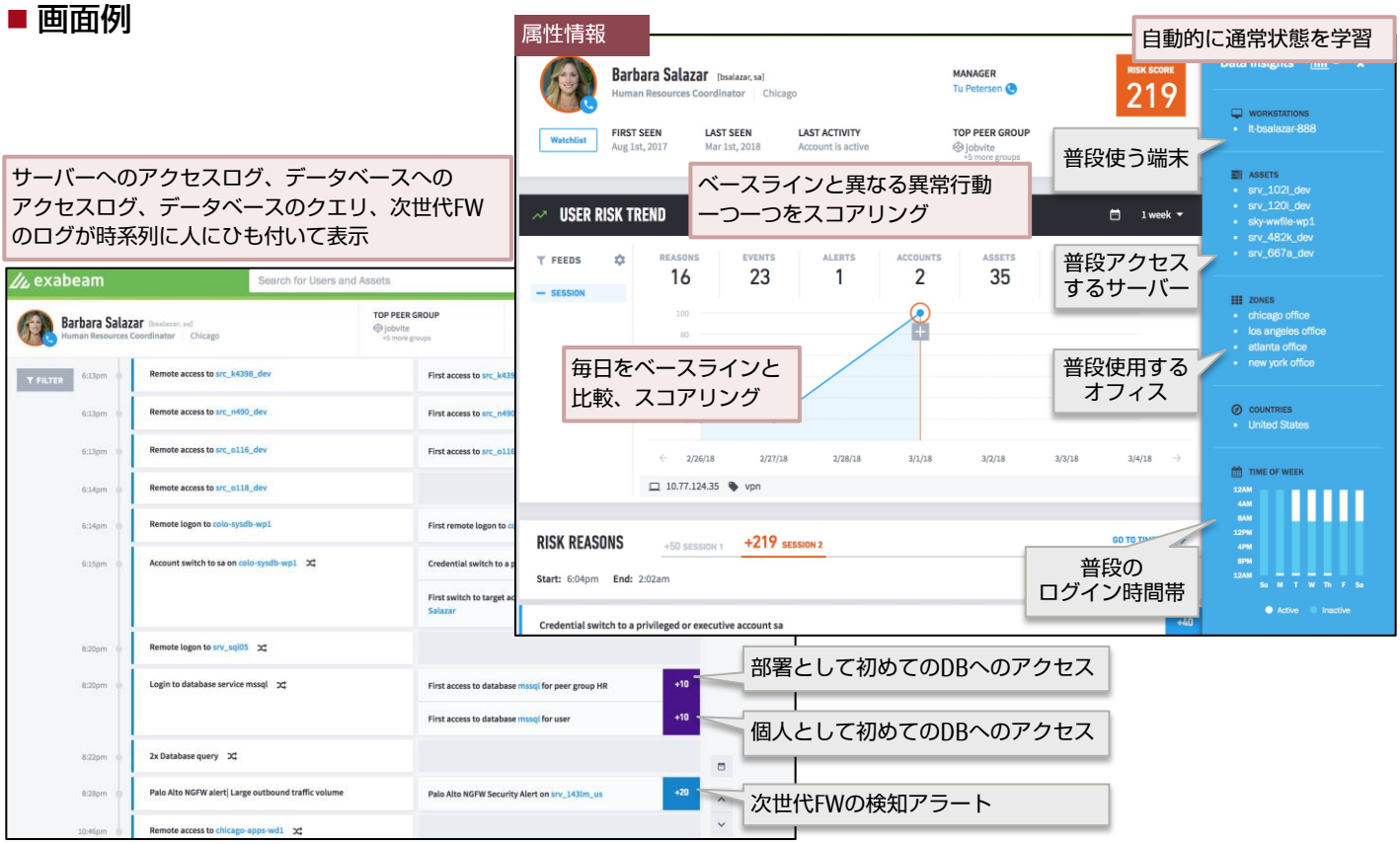
1.ログ収集
ログ管理サーバーにログを収集
(ログ管理サーバー例)
Splunk, IBM Qradar, ArcSight
McAfee SIEM,Exabeam Data
Lake など

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



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。