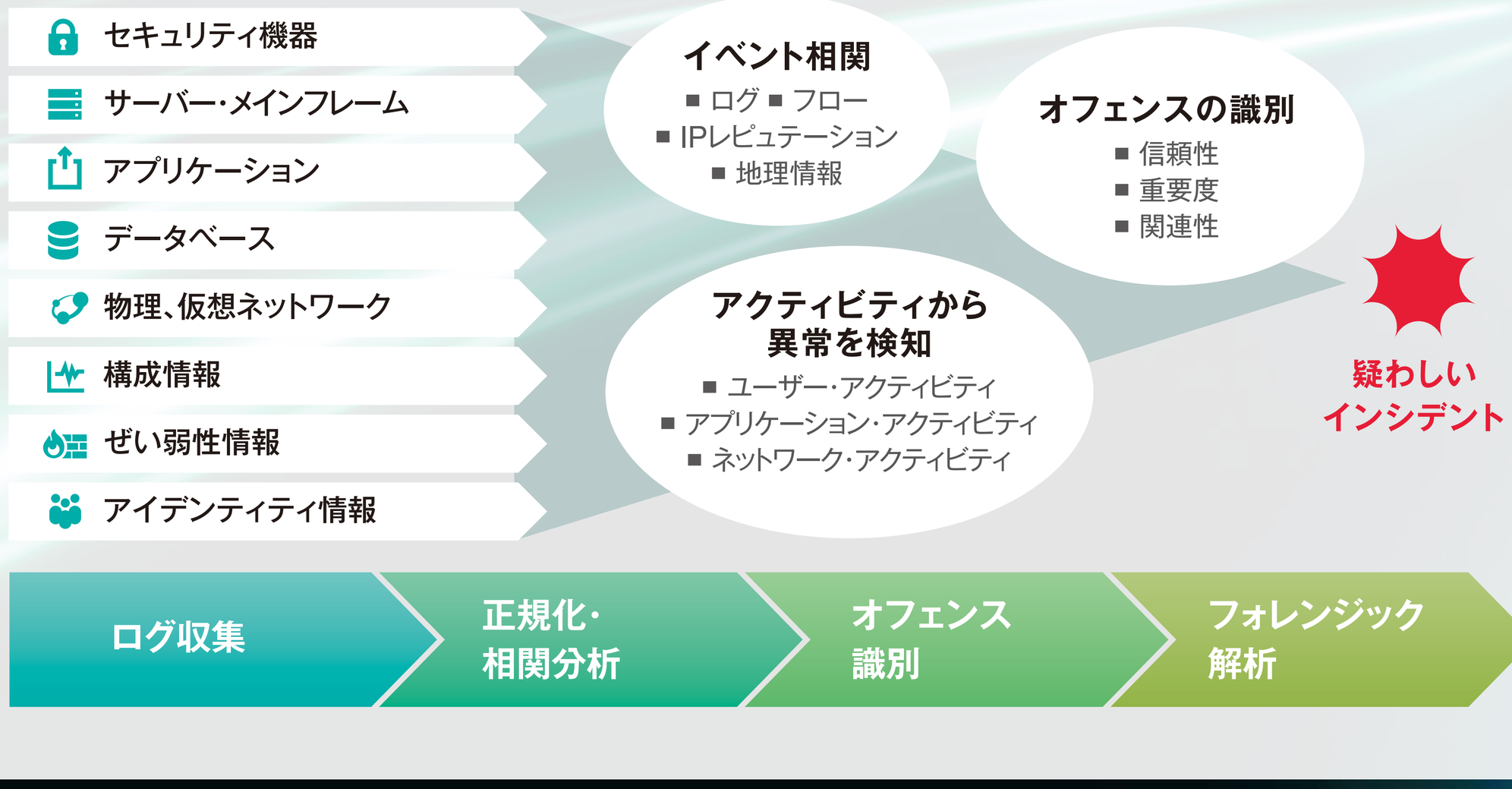
新時代のセキュリティ分析プラットフォーム

IBM® QRadar

キューレーダー

ネットワークに潜む脅威をリアルタイム検知



IBM QRadarの特長

解析ルール
（セキュリティを見える化）

- 350種類以上のデフォルトルールにより、構築を早期に実現
- 継続的なアップデートにより、最新の脅威にも対応可能

解析の自動化
（相関分析による異常検知）

- 1日に何十万件にもおよぶログデータを横断的に自動解析
- 人手では不可能な瞬時の解析とコスト削減
- DSM（標準で正規化をサポートするModule）により
  データの意味づけを行いログを正規化し解析

幅広い情報源
（X-Forceによる知見）

- X-Forceの知見を生かした350種類以上の相関ルールを標準提供
- 多頻度（毎時1回）のレピュテーション情報をUpdate

リアルタイム
（運用負荷の軽減）

- 脅威検出を即時にアラートすることで、素早い調査・対処が可能
- セキュリティログだけではなく、ネットワークトラフィックも
  相関対象とすることにより、未知なる脅威の早期発見を実現

コグニティブ技術と拡張性
（セキュリティ監視プラットフォーム としての拡張性）

- Watson（コグニティブ技術）のセキュリティ領域への活用
- QRadarはSIEMだけでなく、リスク管理、ぜい弱性管理、
  フォレンジックスなどに段階的な機能拡張が可能

エイチ・シー・ネットワークス株式会社