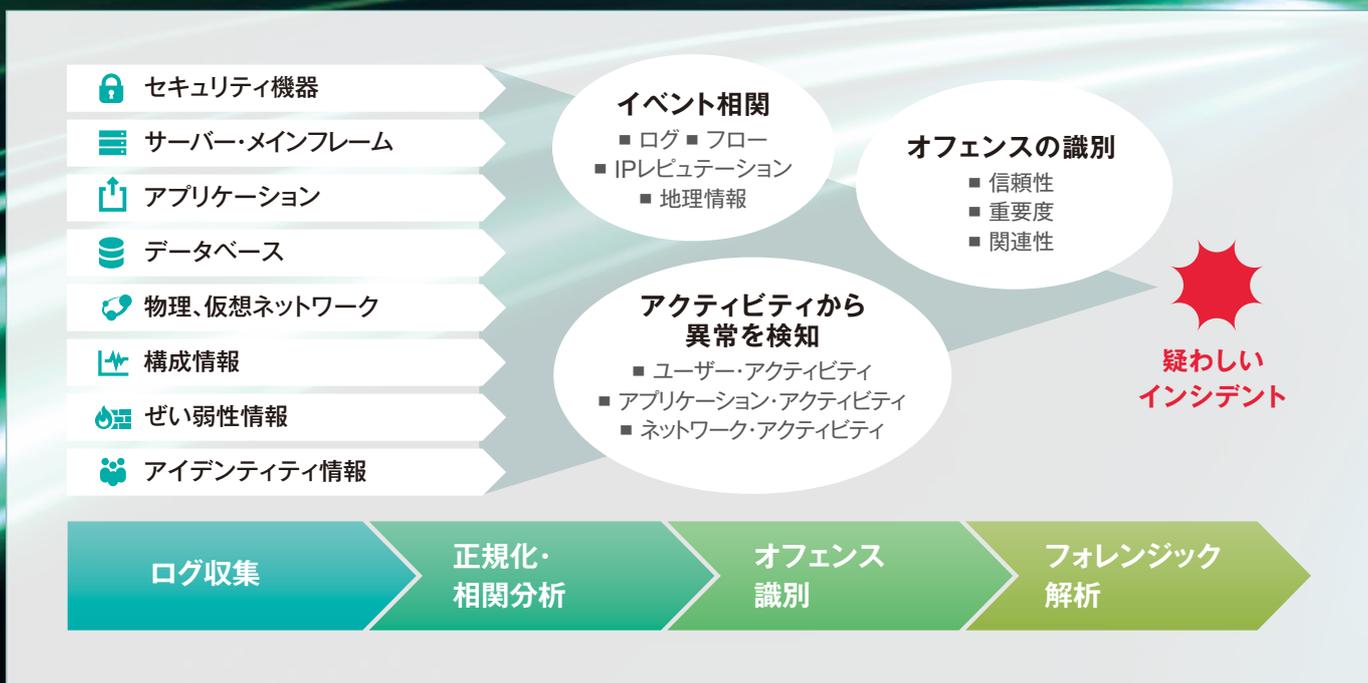


IBM® QRadar

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



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



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

製品ラインアップ

QRadar セキュリティ・インテリジェンス

(QRadar 製品体系)



	QRadar Apps	<ul style="list-style-type: none"> さまざまなベンダーセキュリティソリューションを効果的に活用 	Security App Exchange
	インシデントフォレンジックス	<ul style="list-style-type: none"> PCAPからのネットワークセッションの復元 データビジュアライズと可視化ツール 誰が/何を/何時の明確化を提供 	QRadar Incident Forensics
	リスク&ぜい弱性管理	<ul style="list-style-type: none"> ネットワークセキュリティの構成管理モニタリング ぜい弱性スキャンニング&優先順位付け 予測された脅威モデリングとシミュレーション 	QRadar Vulnerability Manager QRadar Risk Manager
	フロー収集	<ul style="list-style-type: none"> Layer7アプリケーション・モニタリング 物理および仮想環境に対応 	QRadar Network Insight
	相関分析 (SIEM)	<ul style="list-style-type: none"> ログ、フロー、ぜい弱性、相関分析 洗練されたアセット・プロファイリング オフense管理とワークフロー 	ベース製品
	ログマネージャー	<ul style="list-style-type: none"> ログ管理とレポート機能 小規模から大規模まで対応 SIEMにアップグレード可能 正規化とログエントリ 	

Cognitive Security

セキュリティアナリスト

- セキュリティ・イベントと異常調査
- アクティビティとぜい弱性の評価
- ツールのパラメーターやしきい値の設定

セキュリティアナリスト



Watson for Cyber Security

- セキュリティ知識を持つ
- 脅威の識別を行う
- 追加指標を明らかにする
- 関係を浮かび上がらせる
- 証拠をつかむ

QRadar

- データ相関
- 異常検出
- 優先順位付け



QRadar Advisor with Watson

- サイバー・セキュリティに関する Watsonを使用した脅威の調査を行う
- 調査した脅威とセキュリティ・インシデントを適切に関連付ける
- 所見を提供する

エイチ・シー・ネットワークス株式会社

〒111-0053 東京都台東区浅草橋1-22-16 ヒューリック浅草橋ビル4階
TEL 03-6381-8856 <https://www.hcnet.co.jp/>

CAT.NO.HCNET-045 Printed in Japan 201804

本カタログに記載の製品名および会社名は各社の商標または登録商標です。本カタログに記載の内容は、改良のため予告なしに変更する場合があります。本カタログに記載の製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、弊社担当営業にお問い合わせください。

