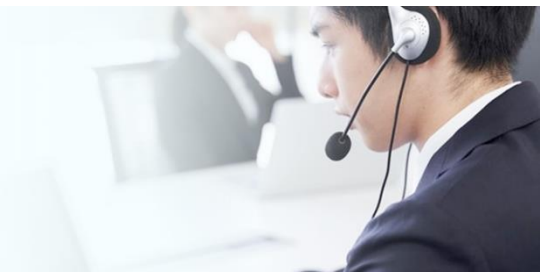
エクシオグループ 株式会社

自社内で実践中 クラウドツール等を活用したセキュリティ監視サービス

Endpoint セキュリティ監視サービス



昨今のサイバー攻撃は巧妙化しており、全ての攻撃を水際で完全に防御することは難しく、このため感染を前提とした対策が主流の考え方となっています。また、エンドポイント端末の挙動を監視し、不審な動作の兆候から不審なプログラムやプロセスを検知し、解析/分析/調査を行い、感染端末や侵入経路、被害状況などを可視化することを本サービスにて実現し、お客様の資産を脅威からお守りする支援をします。

特徴

- 24時間365日お客様のシステムを監視
- 設定や運用を代行
- マルチベンダーサポート

導入効果

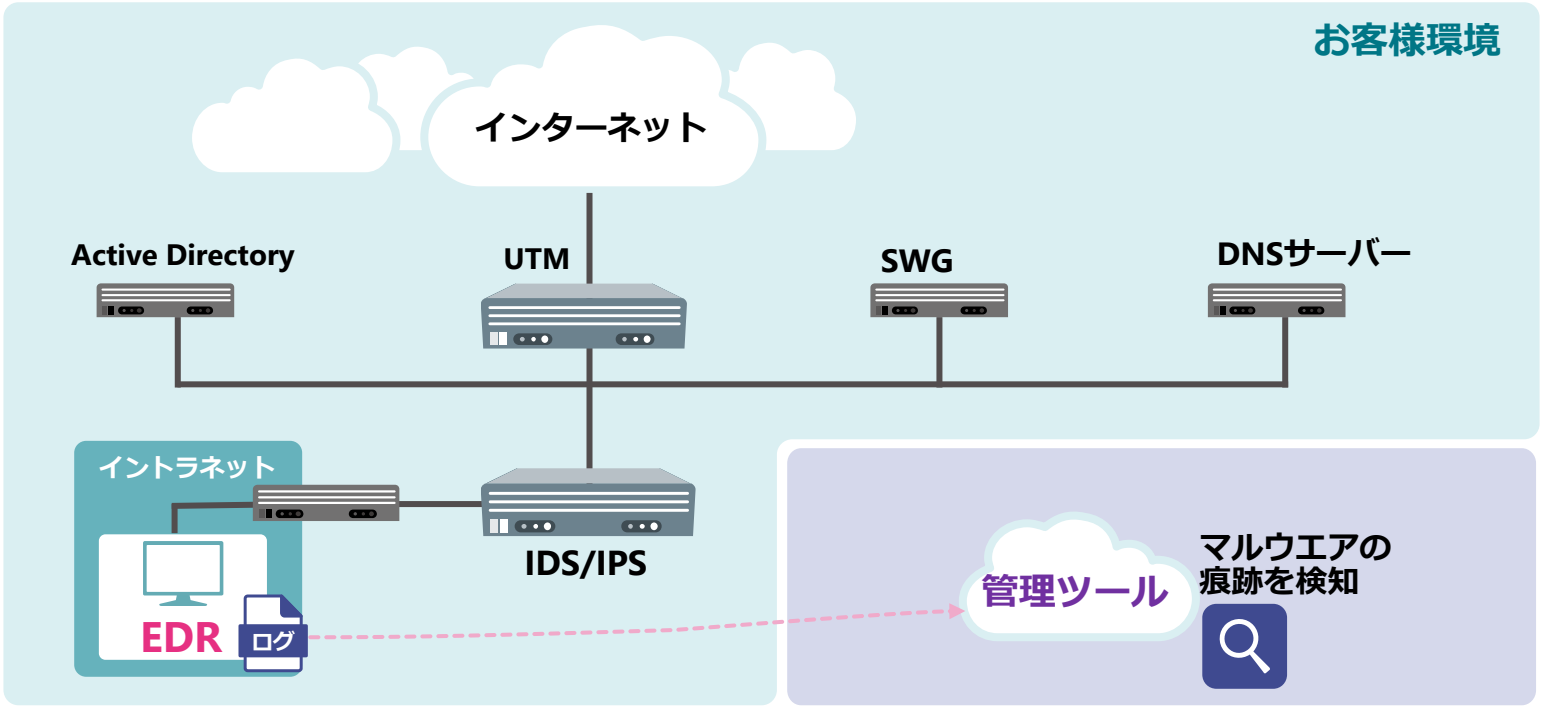
- お客様の運用コスト削減
- 危険性の高いセキュリティ事案をリアルタイムで分析/報告
- 稼働状況/対応内容を月次で報告

◆サービスイメージ

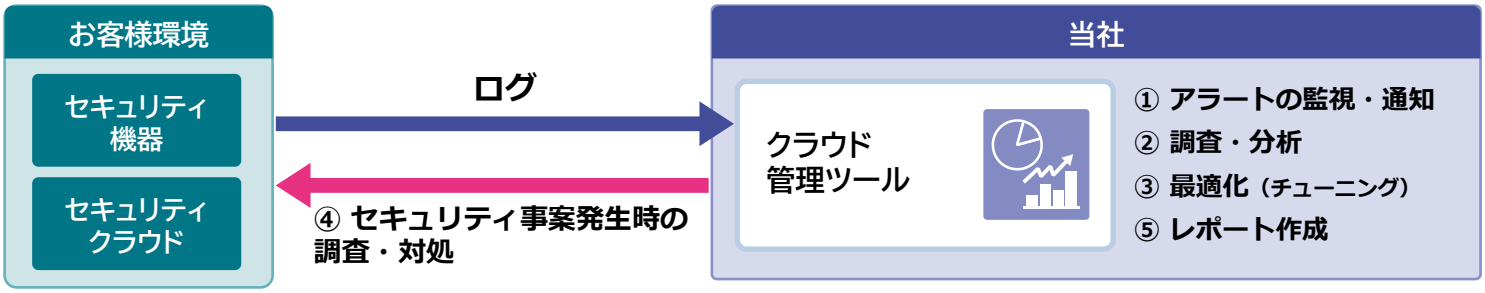
- 当社のエンジニアやアナリストが24時間365日運用監視
- イベントと発生時には、当社のエンジニアやアナリストがリアルタイムでログ解析と対応検討

Point

- ログの管理
- リアルタイム分析
- セキュリティインシデントの早期発見



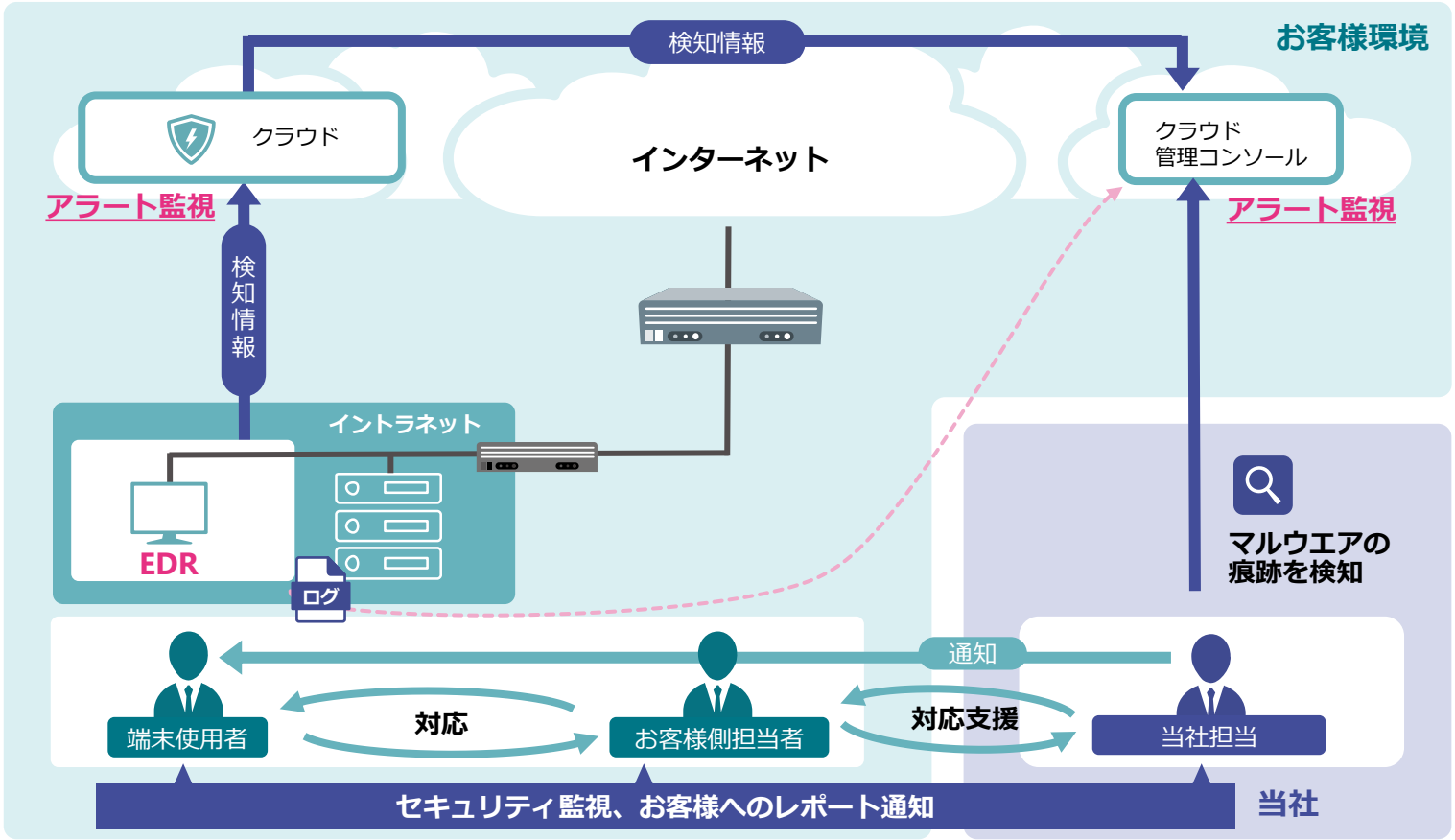
◆サービスメニュー　設計・構築に加えてお任せください！



No.	提供サービス概要	備考
①	アラート監視、アラート発生時の内容の通知	
②	アラート発生時の調査・分析	
③	アラート誤検知、大量検知時の検知ロジックの最適化	チューニング
④	セキュリティ事案発生時の調査・対処	端末隔離・復旧
⑤	お客様向け専用レポートの作成（アラート分析結果・傾向・兆候・インシデントなど）	QA対応

◆対策強化のご提案例

EDR（Endpoint Detection and Response）により端末の監視が可能になります。
※エクシオグループのEDRは、Microsoft Defender for Endpointを提供しております。



※料金等、詳しくはお問い合わせください

EXEO エクシオグループ 株式会社
https://www.exeo.co.jp/

お問合せ窓口
ソリューション事業本部デジタルコンサルティング本部
E-Mail：**degicon-network@hqs.exeo.co.jp**