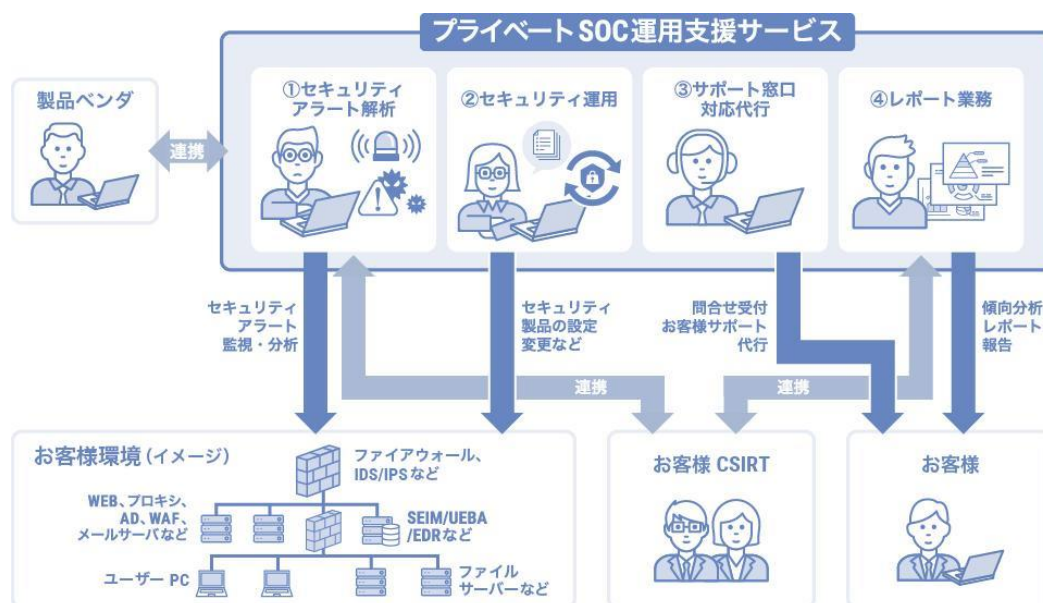


「Elastic Security」を組み合わせたプライベート SOC 運用支援サービス ～生成 AI を活用し、大量のデータから高精度のセキュリティ分析が可能に～

昨今、企業へのサイバー攻撃はますます高度化・巧妙化し、発生件数も増加傾向にあります。一方で、企業のセキュリティ人材は依然として不足しています。このような中、NTT データ ニューソンでは、企業の情報システムへの脅威の監視を行う専門組織 SOC の活動を支援する、プライベート SOC 運用支援サービスを提供しています。このたび、Elasticsearch 株式会社とサイオステクノロジー株式会社と協業し、セキュリティソリューション「Elastic Security」とプライベート SOC 運用支援サービスと組み合わせた提案が可能になりました。本協業により、3 社で「Elastic Security」の活用支援をおこなうほか、販売促進活動もおこなっていきます。



生成 AI 活用で高精度なセキュリティ分析・回答が可能な Elastic Security

Elastic Security は、オープンソースのデータ検索・分析エンジンである Elasticsearch に、SIEM 機能をはじめとしたセキュリティ機能を統合したプラットフォームです。SIEM に加え、エンドポイントセキュリティやクラウドセキュリティまで広範囲なセキュリティ対策を行えます。SIEM は、コスト面が障壁となり導入をためらうケースもありますが、「Elastic Security」はリソース使用量に基づいた課金体系で、ニーズに応じた無駄のない費用設計が可能です（一部の機能では追加ライセンスが必要な場合があります）。NTT データ ニューソンの経験豊富なセキュリティアナリストのノウハウと Elastic Security の生成 AI のセキュリティ分析等の機能を組み合わせることで、更なる解析速度短縮や品質向上、コスト削減を実現していきます。

機能面での特長は以下の通りです。

■ 柔軟性の高さ

パブリッククラウド、プライベートクラウド、オンプレミスなど様々な環境のサービスを組み合わせて利用できるため、導入先企業の運用環境にあわせた構築が可能です。また、分散型アーキテクチャを採用しているため、大規模なデータ処理に適しています。さらに、リアルタイム性が高く、データの追加や更新がすぐに反映されます。様々なデータ形式に対応しているため、構造化データのみならず、非構造化データも柔軟に扱うことができます。

■ 生成 AI を活用したセキュリティ分析

生成 AI アシスタントの「Elastic AI Assistant」を活用することで、セキュリティアラートの調査や対処方法の検討をチャット形式で支援します。ここでは、検索拡張生成（RAG : Retrieval-Augmented Generation）と呼ばれる技術を採用しています。これは、蓄積された業務文書や規定などのデータベースを検索し、その情報を大規模言語モデル（LLM）の出力に反映させる仕組みです。RAG を活用することで、関連情報を文脈として大規模言語モデルに提供し、より精度の高い回答を得ることが可能になります。これにより、過去のインシデント対応記録などをもとに、分析や対応方針の候補を瞬時に提示することや、社内文書の検索に時間がかかり、サポート対応が遅れるといった問題の解消にもつながります。RAG の活用では正確なコンテキストデータを迅速かつ効率的に取得することが重要で、そこで要になるのが、Elasticsearch が長年培ってきた、大量のデータの中から最適な情報を探す仕組みです。Elasticsearch では、ベクトル検索と従来の全文検索を組み合わせたハイブリッド検索にも対応可能であり、あいまいな表現や多義語にも柔軟に対応できます。

Elastic Security 導入に向けて 3 社の知見やノウハウを活かす

NTT データ ニューソンは、プライベート SOC 運用支援サービスを提供し、お客様の予算に合わせてアラートの検知・分析や製品運用などセキュリティ面における課題解決に向けた支援してまいりました。当社のプライベート SOC 運用支援サービスのセールスポイントの一つは、お客様がすでに導入されている製品を活用し、特定の製品に依存しない柔軟な SOC 運用を実現できるという点にあります。さらに、このたびの 3 社の協業により、製品選定からご検討されているお客様に対しても、各社の専門性と豊富な実績を活かし、柔軟性に優れ、コストパフォーマンスの高いセキュリティソリューションをご提案できる体制が整いました。製品に精通している Elasticsearch 社、セキュリティコンサル力の高い SIOS 社、セキュリティ運用に長けた当社のシナジーにより、品質の高いセキュリティソリューションを提供することが出来ます。特に運用面では Elasticsearch 社とのコラボレーションにより、SOC 運用に必要なパーサ開発力やパーサを活用したアラート解析力といった当社の強みをより活かした対応が可能となり、高品質のサービス提供に繋げることができます。NTT データ ニューソンは、今後もお客様のサイバーレジリエンスの実現に向け、セキュリティサービスの対応製品の拡充やより高度な分析やツールの利活用を進めてまいります。

※Elastic および関連するマークは、Elastic B.V.およびその子会社の商標または登録商標です。他のすべての会社名および製品名は、該当する所有者の商標である場合があります。

【参考情報】

・プライベート SOC 運用支援サービス

<https://www.newson.co.jp/services/ITInfra/P-SOCservice/>

・Elastic Security

<https://www.elastic.co/jp/security>

■ NTT データ ニューソンについて

株式会社 NTT データ ニューソンは、情報システムの企画、設計、開発、保守をしています。1974 年に設立以来、システムインテグレータとしてソフトウェアとハードウェアの融合を行っております。2017 年に NTT データグループの一員となり、2024 年に創立 50 周年を迎えました。

NTT データ ニューソンは、NTT データグループの各社と連携し、“情報技術で、新しい「しくみ」や「価値」を創造し、より豊かで調和のとれた社会の実現に貢献すること”を目指しています。

NTT データ ニューソンに関する詳細な情報については、<https://www.newson.co.jp/> をご覧ください。

< 本件に関するお問い合わせ先 >

株式会社NTTデータ ニューソン 経営企画部 アライアンス推進担当

E-mail : pr_newson@newson.co.jp