導入事例

株式会社NTTデータ グローバルソリューションズ

NTTデータ グローバルソリューションズは、Stellar Cyber Open XDR プラットフォームを利用して、セキュリティ運用の生産性を向上させます

NTTデータの国内グループ会社におけるSAP事業の中核会社の株式会社NTTデータ グローバルソリューションズは、 Stellar Cyber Open XDR プラットフォームを活用してセキュリティ運用の生産性を大幅に向上させました。同社は、基幹ネットワークのデータを分析できるNDRを探しておりましたが、XDRであるStellar Cyberに同社で使用しているさまざまな製品のログデータをStellar Cyberに送信し、何が分析できるか見てみて、次の対策を考えるという観点でStellar Cyberの導入が決まりました。
Stellar Cyber導入後は、リアルタイムでの検知が実現され、誤検知も減少しました。1日に何件の検知が発生したかなど全体を簡単に把握できるようなりました。少人数でのセキュリティ運用を効率的に実現しております。

株式会社NTTデータ グローバルソリューションズ

“Stellar Cyberは、ネットワーク、PCの操作、アンチウイルス、EDR、それぞれの製品のログを一箇所に収集し、何かが怪しいかもしれない、何かが起こるかもしれない、などの予兆や傾向をリアルタイムに検知し把握ができます。”

– (株)NTTデータ グローバルソリューションズ 事業戦略推進部

IT戦略&マネジメントグループ マネージャー　馬場 順一郎氏

導入前

視認性の欠如

脅威がどこで、どのように環境に影響を与えているかを確認することはほぼ不可能でした。

専門知識

脅威の特定には専門家のスキルと経験が重要であり、使用方法や管理方法を習得することは容易ではありませんでした。

STELLAR CYBER 導入後

Open XDR

複数の脅威ベクトルからの情報を1つの画面に集約、脅威を素早く認識できるようになりました。

オートメーション

脅威の自動ハンティングや対応アクションの適用が可能になり、作業効率が向上しました。

使い易さ

Stellar Cyberは、直感的で使いやすく、経験の浅い担当者でも迅速に対応することができるようになりました。

“Stellar Cyber導入後は、リアルタイムでの検知が実現され、誤検知も減少しました。1日に何件の検知が発生したかなど全体を簡単に把握できるようなりました。アクティビティなどの活動状態が一目で分かるのも良い点です。”

同社は2022年3月からStellar Cyberの運用を開始、2023年3月にはStellar Cyberのデータ量を拡張し、活用範囲を広げております。

同社の基幹システムのセキュリティ運用にStellar Cyber Open XDRプラットフォームを活用しております。基幹ネットワーク上に流れるパケット情報、クライアントからの操作情報、各種サーバ上で動いているログ情報などをStellar Cyberで分析しております。

現状の導入構成は、Microsoft Azure上にStellar Cyberを展開し、統合NW-F/W、NG-SWG、端末資産管理ツール、NG-マルウエア、EDR、業務SaaSなどのログデータをStellar Cyber Open XDRプラットフォームに送信し、リアルタイムでの検知・分析を行っております。

> “Stellar Cyberは、連携できる製品数が多いので、企業が新しい３rdパーティー製品の導入を検討する際、Stellar Cyberが対応している連携製品リストから製品を選ぶようになっていくと思います。”

Stellar Cyber導入前は、同社は、基幹ネットワークのIaaSからSaaSへの間のデータ量が非常に大きく、そのデータを分析できるNDRを探しておりました。NDRの代わりとしてStellar Cyberが使えるとの考えで、導入の検討が始まりました。他社のネットワーク監視製品も検討しましたが、XDRであるStellar Cyberに同社で使用しているさまざまな製品のログデータをStellar Cyberに送信し、何が分析できるか見てみて、次の対策を考えるという観点でStellar Cyberの導入が決まりました。

また、同社は既に使用しているSIEM製品で基幹システムの複数製品の分析を試したことがありましたが、ログデータが膨大すぎて、不足している人手で監視するのは不可能だと分かりました。Stellar Cyberは横断的に複数製品の分析がリアルタイムに行え、数名でも監視が行え、リアルタイムでの24時間365日対応の要件を満たした点も導入の大きな決め手でした。リアルタイム性は、インシデントが発生した場合の汚染リスクを最小限にする観点からも同社にとって非常に重要でした。

株式会社NTTデータ グローバルソリューションズ 事業戦略推進部 IT戦略&マネジメントグループ マネージャーの馬場 順一郎氏は、Stellar Cyberのメリットを次のように語っています。

「ファイアウォール製品なども人間が決めた閾値ベースのアラートは出せますが、怪しいかもしれないを判断する基準が難しいです。 Stellar Cyberは、ネットワーク、PCの操作、アンチウイルス、EDR、それぞれの製品のログを一箇所に収集し、何かが怪しいかもしれない、何かが起こるかもしれない、などの予兆や傾向をリアルタイムに検知し把握ができます。」

更に、馬場氏は「当社では端末資産管理ツールをPCの操作ログ取得ツールとして利用しています。以前は、何か発生したらとりあえずは端末資産管理ツールのログを見ていました。端末資産管理ツールも閾値を決めてアラートを通知する機能はありますが、リアルタイム性の問題やチューニングが非常に大変でした。Stellar Cyber導入後は、リアルタイムでの検知が実現され、誤検知も減少しました。1日に何件の検知が発生したかなど全体を簡単に把握できるようなりました。アクティビティなどの活動状態が一目で分かるのも良い点です。」と述べています。

同社は、Stellar Cyberのダッシュボードも積極的に活用しております。馬場氏は「Stellar Cyberのダッシュボードは、非常にわかりやすいです。送信元および送信先はどこか、何が起こっているか、などが一目で分かります。知りたい情報（IPアドレス、端末名、ドメイン名、経路、プロトコルなど）をビジュアルに分かりやすく表示してくれます。危険度を示すリスクスコアも自動的に計算し、検知した理由も表示してくれます。ダッシュボードを見ていれば、必要な情報は把握できます。」と述べております。

今後は、セキュリティ意識を高める啓蒙活動として一般社員へのダッシュボードの公開も検討されております。