株式会社JSP 様

EPP製品では検知が困難な脅威に対応するためSophosのEDR製品を導入
重要なインシデントの調査・解析はCEC SOC のEDR原因解析サービスで対応

CEC
Computer Engineering & Consulting

Sophos Intercept X Advanced with EDR

導入事例

Sophos Intercept X Advanced with EDRがゼロデイ攻撃やマルウェアなどの脅威をクラウドから自動で監視・検知・駆除。セキュリティ管理の工数が削減され、リモートワークでも威力を発揮

課 題

- EPP製品だけでは、攻撃パターンを把握できない未知のゼロデイ攻撃やマルウェアなどへの対応が困難
- EDR製品の導入にあたり、静的解析やウイルスチェックといったEPP部分を事前に評価する時間やコストはない
- 社内に重要なインシデントに対応するための知見を蓄積できるシステムを構築したい

効 果

- EDR製品のSophos Intercept X Advanced with EDRで、未知のゼロデイ攻撃やマルウェアをクラウドから監視・検知・駆除
- 開発元のSophosは企業に最適なセキュリティソリューションを提供する世界最大規模のセキュリティベンダー
- 重要なインシデントの調査・解析はCEC SOC のEDR原因解析サービスが対応

導入の背景・課題

EPP製品だけでは対応できない

株式会社JSPは、自動車の軽量化部材、高機能断熱材、食品容器、各種緩衝材、梱包材など世界最高水準の発泡技術で持続可能な社会づくりに貢献しているワールドワイドなサプライヤーだ。その情報システム部は、社内のITインフラ基盤の運用・保守を担う部門。「メーカーの情報システム部門なので、システムの企画から社内開発、導入ツールの検証・運用、セキュリティまで幅広く携わっています。」と情報システム部 システム企画・開発グループ 主査の今 直人氏は語る。

近年、同社のセキュリティ対策で頭を悩ませていたのが、ゼロデイ攻撃やマルウェアといったEPP（Endpoint Protection Platform）製品では検知が困難な脅威。「当社はこれまでEPP製品のアンチウイルスソフトで検知対応してきました。しかし、最新の脅威に対応するには、常にシグネチャをアップデートする必要があるため、攻撃パターンを把握できない未知のゼロデイ攻撃やマルウェアなどへの対応は困難でした。」と語るのは情報システム部 システム企画・開発グループ 主査の八木 貫志氏。

EDR製品での出口対策が必要

実際、同社のサーバーと通信許可されているアジア方面から攻撃を受けたインシデント事例もあった。その際は情報漏えいなどの被害はなかったが、原因究明は困難を極めた。「外部ベンダーも使って残っているログを調査しましたが、非常に工数を要してしまいました。このとき、現状のEPPだけではインシデントが発生した際に対応しきれないと実感しました。」（今氏）

そこで同社は侵入防止の入口対策だけでなく、侵入後の出口対策も行う必要があると考えた。行き着いたのは、エンドポイント上での不審な動きを常時監視し、マルウェアやランサムウェアの存在をいち早く検知・除去するEDR（Endpoint Detection and Response）製品の導入。「親会社の三菱ガス化学株式会社からも、セキュリティ対策としてEDR製品の導入要望があり、本格的にEDR製品の比較・検討を行うことになりました。」（八木氏）

ベンダーの選定

Sophosの情報量を評価

取引会社からの紹介や自社の検索などによって選定したEDR製品は6社。その後の絞り込みではEPPでの実績を重視した。「行うのはEDRの評価ですが、EPPでの実績がないベンダーの製品は静的解析やウイルスチェックといったEPPの部分も評価しなければなりません。そうなると、時間もコストもかかります。それならば、もともとEPPで実績のあるベンダーをベースに検討した方が得策と判断しました。」（今氏）

そこで残ったのは2製品。そのひとつがシーイーシーが提案したSophos Intercept X

株式会社JSP 様

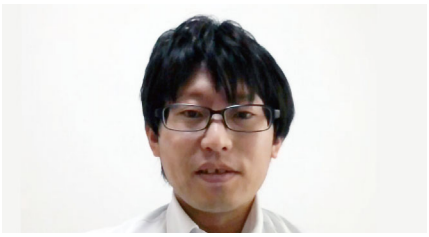
EPP製品では検知が困難な脅威に対応するためSophosのEDR製品を導入
重要なインシデントの調査・解析はCEC SOC のEDR原因解析サービスで対応

CEC Computer Engineering & Consulting

Sophos Intercept X Advanced with EDR

導入事例

情報システム部 システム企画・開発グループ 主査 八木 貴志氏



情報システム部 システム企画・開発グループ 主査 今 直人氏

Advanced with EDR（以下、Intercept X）だった。同社は2製品を比較・検討するためPoC（Proof of Concept）を実施し、最終的にIntercept Xの導入を決定した。選定理由については「管理コンソールから確認できる情報の多さが決め手でした。情報量が多ければ、自分たちで追跡・調査する際に役立ちます。さらに、コスト面でのメリットもありました。」（八木氏）と語る。

EDR原因解析サービスも依頼

Intercept Xを導入するにあたって懸念もあった。通常、EDR製品を導入するとエンドポイントを監視・検知するSOC（Security Operation Center）のサービスが含まれるが、Intercept Xの場合は対処（駆除）まで行うフルオートメーション。運用において情報システム部の手を煩わせることはほとんどない。半面、どういったインシデントが発生したのか社内で詳細に確認することもできない。

そこで、Intercept Xとともに導入することにしたのが、CEC SOCが提供するEDR原因解析サービス。「フルオートメーションはありがたいのですが、簡単な事後報告だけでは知見を蓄積できませんから、重大なインシデントがあった際、我々が対応できなくなってしまいます。そこで、我々が調査すべきと判断したインシデントについて解析を行い、詳細な脅威情報や対処方法を報告してくれるCEC SOCのEDR原因解析サービスを利用することにしました。」（八木氏）

導入の効果

端末のフルスキャンは不要に

Intercept Xの導入は2020年の5月からスタート。国内および国内関連会社の端末分に相当する1500ライセンスを導入した。すべての端末を把握するのが困難だったが、無事2020年末には導入作業を終えた。現在、Intercept Xの運用に携わるなか、今氏はIntercept Xを以下ように評価している。

＜セキュリティ工数の削減＞

EPP時は対処が不完全なところもあって、端末に対する作業が結構ありましたが、Intercept X導入後は通知を確認したときには対処が終わっています、事後処理の作業は少なくなりました。また、以前は対処後に端末のフルスキャン実行を従業員に促していましたが、Intercept Xはそれも不要。インシデントに関する作業工数は大きく減ったと思います。

＜リモートワークに対応＞

新型コロナウイルス対策の影響で当社もリモートワークが増えました。そういった状況のなか、クラウド製品のIntercept Xは自宅のネットワーク環境でも、社内と変わらない機能を享受することができます。今後、新型コロナウイルスが収束したとしても、働き方改革などと相まってリモートワークは残っていくと思われますから、この効果は大きいと感じています。

今後の展開と期待

運用コストの削減に取り組む

現在、同社が行っているのはインシデントに対する精度向上。「Intercept Xは検知力が高いせいか、既存アプリケーションの挙動を誤検知してしまうことがあります。そのため、ホワイトリストを作成するなどの対処を行い、インシデントの精度向上に努めています。これを続けていけば、セキュリティに関する運用コストも下がってくると考えています。」（八木氏）

国内にいくつもの工場をかかえる同社は、シーイーシーのデジタルインダストリー事業にも注目しているという。「IoTの導入や制御系システムのセキュリティ部分の見直しなど、工場において生産プロセスの変革による生産性の向上は、常に取り組んでいく必要があります。当社としてはその方面でも良い提案を期待しています。引き続きよろしくお願いします。」（八木氏）

お客様プロフィール

株式会社JSP 様

1962年にポリスチレンペーパー事業にて創業。その後、世界に先駆けて無架橋発泡ポリエチレンシートやビーズ法発泡ポリプロピレンなどの独自製品、さらに住宅用断熱材ポリスチレン押出ボードおよびビーズ法ポリスチレン事業を加えて業容を拡大。発泡プラスチック製造の国内大手となった現在は、バンパーなどの自動車用資材から精密機器運搬用の緩衝容器、食品容器、住宅用資材、高機能断熱材、梱包材など幅広く手掛けている。2003年に三菱化学系列の三菱化学フォームプラスティック株式会社と合併。2014年には三菱ガス化学の連結子会社となる。

本　社	〒100-0005 東京都千代田区丸の内三丁目4番2号 新日石ビル
代表者	代表取締役社長　酒井 幸男
従業員数	単独 782名（出向者除く）、 連結 3,074名（2020年3月31日現在）
事業内容	発泡プラスチック、その他合成樹脂製品の製造販売および輸出、土木・建築工事の設計・請負および管理
URL	https://www.co-jsp.co.jp/

お問い合わせ

CEC 株式会社シーイーシー
Computer Engineering & Consulting

〒150-0022　東京都渋谷区恵比寿南1-5-5　JR恵比寿ビル
TEL：03-5789-2442 FAX：03-5789-2585
Email：marketing@cec-ltd.co.jp
URL：https://www.cec-ltd.co.jp/

販売代理店

202102-003-022CI