Splunk Services Japan 合同会社 × 株式会社ラック

セキュリティ製品を増やしても、なぜ企業は守り切れないのか

Splunkとラックが語る、「統合SOC」xPDR Advanced

EDR やネットワークセキュリティ、クラウドセキュリティなど、企業ではさまざまなセキュリティ製品の導入が進んでいます。しかし、製品を増やせば、それだけ組織全体の防御力が高まるとは限りません。個々の製品が検知したアラートを確認できても、異なるシステムのログや情報が分断されていれば、攻撃の全体像を把握できず、適切な対応が遅れる恐れがあります。

攻撃の動きが自動化するなか、個別のアラートを人が一つずつ確認する従来の運用にも限界が見え始めています。いま求められているのは、散在するデータを集約し、検知から調査、初動対応までを一連の流れとしてつなぐ「統合 SOC」です。

では、統合 SOC によって企業のセキュリティ運用はどう変わるのでしょうか。大規模な組織でなければ実現できないものなのか、そして AI の進化によって SOC アナリストの役割はどう変わるのでしょうか。セキュリティ統合基盤を提供する Splunk Services Japan 合同会社と、長年にわたり SOC サービスを提供してきたラック。両社の専門家に、企業が抱えるセキュリティ運用の課題や統合 SOC の必要性、そして「JSOC xPDR Advanced」を通じて目指すセキュリティ運用の姿を聞きました。

PROFILE



Splunk Services Japan 合同会社
技術統括本部パートナー技術本部兼
ソリューション技術本部 部長
横田 聡



株式会社ラック
MSS プロダクトインテグレーション部
副部長
田原 祐介



Splunk Services Japan 合同会社
Splunk パートナー・ソリューションズ
エンジニアリング本部
シニア·パートナー·ソリューションズ
エンジニア
長島 広隆



株式会社ラック
MSS プロダクトインテグレーション部
中井 恵子

セキュリティ製品を導入しても、企業全体を守り切れないのはなぜか

――近年、企業から寄せられるセキュリティ運用や AI 活用に関する相談には、どのようなものがありますか。

長島氏

以前、Splunk に相談されるお客様は、セキュリティや SOC に精通している方が多かったと思います。しかし最近は、セキュリティに関するニュースを受けて、会社として対応する必要性は感じているものの、具体的に何を守り、何をすればよいのかまでは整理できていないケースが増えています。そうしたお客様に対しては、要望を聞いてから製品を提案するだけでは十分ではありません。われわれからベストプラクティスを示す提案が、これまで以上に求められていると感じています。

田原

SOC に関しては、複数の製品やログを横断して監視したいというニーズが高まっています。これまで個々のセキュリティ製品が部分最適で導入されていることが多く、担当部門が分かれていることもあります。そのため、統合的なセキュリティ運用を検討する以前に、「どのようなログがあるのか」「どの程度保存されているのか」を整理するところから、ご相談が始まることも多いのが現状です。



横田氏

加えて、お客様からのご相談には、AI をめぐり大きく三つの傾向があります。一つ目は、AI の進化を受け、これまで難しいと考えていた SOC の内製化を改めて検討し始めていることです。二つ目は、フロンティア AI の登場によって脅威が変化する中、脆弱性管理の対応にどのように優先順位を付けるかという課題です。三つ目は、社内で AI や AI エージェントを開発・活用する際に、新たに生じるリスクへの対応を模索していることです。

――セキュリティ製品がすでに導入されていても、なぜ十分に守れないのでしょうか。

田原

特定のセキュリティ製品を監視していても、インシデントが発生したときに、関連するほかのシステムのログが手元にない場合があります。例

© 2026 LAC Co., Ltd.

えば、ある製品で不審な挙動を検知できたとしても、どこまで影響が広がっているのかまでは分かりません。その機器で検知した事象は特定できても、その先で何が起きたのかは分からず、攻撃の全体像を捉えられないといった状態は企業にとって大きなリスクです。そのため、まずは IT 資産から必要なログを収集し、一元的に確認、分析できる環境に集約する提案をしています。

横田氏

多くのお客様は、自社にどのようなリスクがあり、何を守るべきかを整理したうえで、対策の道筋を描ける状態にはなっていません。また、すでに多くの製品を導入している企業でも、日々発生するアラートへの対応だけで疲弊しています。本来であれば、対策を見直したり、新しい脅威に備えたりする必要がありますが、そのためのリソースを確保できていないのです。

お客様が、セキュリティに関する知識やスキルを持つ専任者を自社内に置くことは簡単ではありません。そのため、製品やテクノロジーを提供するだけではなく、何を優先し、どのように段階を踏んで対策を進めるのかという支援も必要と感じます。

長島氏

製品を導入したことで、「この対策をしているから大丈夫」と考えてしまうケースにも注意が必要です。一つの対策を行っても、その周辺にはまだ対応できていないリスクが残っている可能性があります。そのリスクを受容するのか、時間をかけて対応するのかを整理し、ロードマップを作っていく必要があります。

データと運用をつなぐ「統合SOC」という考え方

――これまでの SOC に加えて、なぜ調査や初動対応までを一連の運用として考える必要があるのでしょうか。統合 SOC はどのような役割を果たすのでしょうか。



田原

お客様が求めているのは、SIEM にログを集めて監視することだけではなくなっています。例えば認証基盤への侵害を検知した場合には、すぐにアカウントを無効化するなど、その後の対応まで行ってほしいというニーズがあります。攻撃側の動きも自動化され、高速になっているいま、侵害の検知後に、人が一つずつ確認して対応していたのでは間に合わなくなってきています。

そのため、検知だけでなく、その後の調査や初動対応までを一連のオペレーションとして考える必要が出てきました。最近のセキュリティ製品は API を備えているものも多いため、技術的には製品同士を連携させることができます。しかし、API を使ってロジックを組み、自動化の仕組みを構築し、継続的に運用することは簡単ではありません。製品に関するノウハウも必要です。大規模な企業の中には自社で対応できるところもありますが、そこまでの人材や運用体制を持たない企業が多いのが現状です。

横田氏

従来は、アラートの監視をセキュリティの専門会社へ任せればよいという考え方が中心でした。しかし今、お客様は、アラートが発生した後の初動対応まで踏み込んでほしい、さらには一緒に対応してほしいと考えています。また、SIEM による検知や SOAR による対応といった機能を個別に使うのではなく、製品やデータをつなぎ、お客様とサービス提供者が一緒に運用できる形を整えることが重要です。

長島氏

機能面で見ると、多様なログを扱い、関連する事象を結び付けられることが最低限必要になります。統合 SOC とは、分散している製品、データ、担当者、運用を横断的につなぎ、検知から調査、対応までの流れを一体として捉える考え方ですね。

――統合 SOC を検討する企業は、何から始めればよいのでしょうか。

田原

統合 SOC や SIEM に関するニーズは高まっていますが、自社がどのような IT 資産を持ち、何を使って何を保護しているのかが整理されていないケースがあります。さらに、「どのログを取得し、監視すべきか」という問いに対する答えを、お客様自身が持っていないこともあります。その場合、ラックではネットワーク構成やシステムの概要を確認し、攻撃を受けた場合にどこに痕跡が残る可能性があるのかを考えながら、取得すべきログを一緒に整理するところから始めます。

攻撃は外部から行われるものだけではありません。すでに内部へ侵入されていた場合に何が起きるのかまで想定していき、お客様が何を守るべきかを整理する支援も、ラックの役割だと考えています。

中井

漠然とした不安を抱えている状態ですと、具体的に何をすればよいのかまでは決めきれず、「SIEM を導入しなければならない」「AI を搭載した製品を入れなければならない」と、解決手段の導入が先行しがちです。しかし、何か一つを導入すれば、すべての問題を解決できるわけではありません。まずはお客様の環境の中で何を守る必要があるのかを整理し、そのために必要な対策や運用を考えることが重要です。

――企業が統合 SOC や Splunk の検討を始めるきっかけにはどのようなものがありますか。

横田氏

統合 SOC を検討するきっかけは、お客様の中で EDR/SASE などの様々なゼロトラストアーキテクチャ導入を経て、日々のアラート管理が増えていき、それぞれのコンソールを見ながら対応するスピードが追いつかなくなってきた時に統合 SOC 基盤の相談をいただくことが多いです。そこから予算が確保され、導入検討が進む場合があります。これから始めるお客様にとっては統合 SOC の製品選定だけでなく、運用体制も含めてアドバイスを求められることは多く、「同業他社はどのような対策をしているのか」「自社は何から始めるべきか」という話になり、Splunk では、海外の先行事例や取り組みに関する情報も踏まえて、日本のお客様へアドバイスし、導入をご検討いただいています。

――これまで SOC は、大規模な組織が導入するものという印象もありました。中堅企業にも必要なのでしょうか。

中井

従来のプライベート SOC は、官公庁や規模の大きなお客様による利用が中心でした。お客様ごとの環境に合わせて監視や分析を設計し、導入や運用にも相応の体制が必要なため、非常に高コストとなるケースが多いのが現状です。

同様に、EDR をはじめとするセキュリティ製品の導入が進んでいる中堅企業で同じようにプライベート SOC を立ち上げようとすると、コス

© 2026 LAC Co., Ltd.

トの壁に当たってしまいます。ラックが提供する統合 SOC は、企業の規模やリスク、現在のセキュリティ対策状況に合わせて必要なところから SOC を始めていく、という進め方が可能です。

長島氏

大規模な SIEM 運用を行っている企業も、最初から現在の形を完成させたわけではありません。担当者が一人しかいない企業に、最初から高度な SOC 運用を求めても、それを運用できる体制が整っていません。まず必要なログを集めるところから始め、組織や役割を整備しながら、検知や対応を段階的に高度化していくことは可能です。

お客様の目的が明確であれば、それに必要なログや機能から始められます。目的がまだ具体化していなければ、ベストプラクティスをもとに、最初の一歩を提示します。

Splunkとラックで、統合基盤から運用・対応までをつなぐ

――ラックの「JSOC xPDR Advanced」は、こうした課題にどのように応えるのでしょうか。

中井



相関分析を行うためにログを集めようとすると、お客様からは「できるだけ多くの製品のログを取り込みたい」という要望が出てきます。Splunk は、さまざまな製品のログを取り込みやすいプラットフォームです。この点が、新サービスの JSOC xPDR Advanced で Splunk を採用した一番の理由です。

JSOC xPDR Advanced では、複数のセキュリティ製品やサービスから得られるログを Splunk に集約し、ラックのアナリストが出てきたアラートを横断的に分析します。今後対応する製品は 50 製品を目標に拡張していき、より多くのお客様の取り込みニーズに対応していきたいと考えています。

田原

JSOC xPDR Advanced の特徴の一つは、お客様が保有するさまざまな IT 資産のログを取り込み、横断的な分析に活用できることです。個別の製品によっては追加開発が必要になる場合もありますが、Splunk を統合基盤とすることで、幅広いログを扱うことができます。

また、インシデントが発生した場合には、SIEM に集約されたログをもとに、ラックのアナリストが調査を支援します。さらに詳細な調査が必要な場合には、ラックのサイバー救急センターでインシデントレスポンス支援やフォレンジック調査を一貫して提供することができることも特徴です。異常を検知して通知するだけでは、被害の全容を把握できるとは限りません。何が起きたのかを詳しく調査し、その結果を踏まえて対策を講じることが重要です。

また、お客様の状況によっては、すぐに統合的なログ分析を始めるのではなく、まず EDR など特定の対策から始める方が適する場合もあります。ラックは複数のセキュリティサービスを提供しているため、お客様の現在の状況や目的に応じた提案ができます。

Splunkの技術とラックの運用知見が生み出す価値

――両社が協業することには、どのような意味がありますか。

長島氏

お客様が最終的に求めているのは、Splunk というプラットフォームそのものではなく、SOC やセキュリティ運用です。Splunk は、そのために必要なデータ分析やセキュリティ運用の基盤を提供します。しかし、プラットフォームだけでお客様の SOC 運用を完結させることはできません。

特にセキュリティ人材が不足する中では、Splunk のプラットフォームと、セキュリティに関する知見を持つパートナーのサービスを組み合わせることが重要になります。ラックのように、Splunk を使った監視・分析を具体的な SOC サービスとして提供し、お客様の運用まで支援できるパートナーの存在は不可欠です。

横田氏

昨今は、AI を利用すると、もっともらしい回答が返ってくるようになりましたが、その回答が本当に正しいのか、そのまま対応を進めてよいのかを、セキュリティの文脈で判断しなければなりません。AI の判断を受け入れ、実際の対応につなげるためには、お客様と一緒に考え、判断を支援できる存在が必要です。セキュリティビジネスを長く経験し、運用の実態を理解しているラックのようなパートナーには、AI SOC の時代においても大きな役割があると考えています。

田原

ラックから Splunk に期待しているのは、セキュリティコンテンツのさらなる充実です。これまでラックでは、プライベート SOC などの運用を通じて、分析ルールを独自に作ってきました。しかし、扱う製品やログが増える中で、すべての製品に対してあらゆるインシデントを捉える分析ルールを作り続けることには限界があります。

JSOC xPDR Advanced では、Splunk が提供するセキュリティコンテンツも活用しています。Splunk が提供する分析ルールや、各製品のログを取り込むための Apps が充実すれば、ラックのサービスの品質も、さらに高めることができます。Splunk の技術と、ラックが培ってきた運用・分析の知見を組み合わせることが重要です。

長島氏



Splunk が提供するルールは、原則として、実際に検知できることを確認してから公開しています。外部の知見や公開ルールを取り込むことも重要ですが、それが実際の環境で期待どおりに動作するかという品質は欠かせません。信頼できるコンテンツを提供することで、パートナーのサービス品質向上にも貢献していきたいと考えています。

© 2026 LAC Co., Ltd.

AIはSOCアナリストに取って代わるのか

――AI の進化によって、SOC やアナリストの仕事はどのように変わるでしょうか。

横田氏

反復的な処理や、一定の基準で判断できる作業は、AI によって担われていくと思います。これまでアナリストが繰り返し行ってきた確認業務や一次的な分析も、AI が支援できる領域が広がっていくでしょう。

ただし、AI は学習に必要な情報がないものについて、誤った推論を行う可能性があります。既知の脅威や、一定のパターンで処理できるものには AI を活用できても、未知の脅威への対応や、責任を伴う判断を全面的に任せることは簡単ではありません。AI が自律的にインシデントをクローズするなど、判断と対応まで行うようになると、「その判断に誰が責任を持つのか」という問題も生じます。AI を活用しながらも、運用者が合意した範囲や方法で動かし、人が必要な判断に関与できる形にすることが重要です。

田原

はい、アナリストの仕事は、AI と協働する形へ変わっていくと考えています。影響が限定的で、一定のルールに沿って処理できるものは AI へ任せ、人間はより高度な判断が必要な業務へ移っていくでしょう。

一方で、AI を適切に動かすには、トリガーとなる分析ルールを作成・チューニングして、セキュリティに関するコンテキストを与えて、AI が分析・調査ができる基盤を用意する必要があります。AI によってアナリストが不要になるのではなく、アナリストの役割が、一件ずつアラートを確認することから、AI の判断を支え、分析や運用の品質を高めることへ変わっていくのだと思います。

分断をつなぎ、検知から対応までを行う統合SOCへ

統合 SOC の出発点は、新しいセキュリティ製品を導入することではありません。まず、自社が何を守るべきかを整理し、必要なデータや、判断・対応を担う体制を明確にすることが大切です。ただし、必要な情報が個々のセキュリティ製品や部門に分散したままでは、インシデント発生時に全体像を把握し、対応方針を速やかに決めることは困難です。こうした分断を解消し、検知した事象の調査から対応までを切れ目なく進めるために、統合 SOC が求められています。

AI による自動化が進めば、アラートの確認や定型的な調査に費やしていた時間を、より高度な分析や判断に振り向けられるようになります。しかし、AI の判断が妥当かを見極め、対応に責任を持つ人の役割はなくなりません。むしろ、AI を適切に活用するための運用設計や分析の知見が、これまで以上に問われることになります。

Splunk が提供するデータ分析とセキュリティ運用の統合基盤と、ラックが長年の SOC 運用で培ってきた分析・対応の知見を組み合わせた JSOC xPDR Advanced は、企業の規模や対策状況に応じて、ログの集約から横断的な分析、インシデント対応までをつなぐサービスです。セキュリティ製品を増やすだけでは見えてこない攻撃の全体像を捉え、検知した後の対応まで確実につなげる統合 SOC は、自社に合ったセキュリティ運用を実現するための選択肢となります。



［お問い合わせ］
株式会社ラック
サービス紹介ページ　https://www.lac.co.jp/operation/jsocxpdr_advanced.html

● ラックおよびLACは株式会社ラックの登録商標です。　● 記載されている会社名、サービス名、製品名は、一般に各社の登録商標または商標です。

© 2026 LAC Co., Ltd.