LSUの学生主体のSOC、18の大学で24時間365日のセキュリティ対応を実現

主な課題

サイバーセキュリティ教育の実施機関として名高いLSUは、学生にセキュリティオペレーションセンター (SOC)の実践的な経験を積む機会を用意し、ルイジアナ州すべての高等教育機関のセキュリティ態勢を強化したいと考えていました。

主な成果

LSUの学生主体のSOCでは、SplunkおよびTekStream社との提携により、ルイジアナ州全体で18の大学をサイバー攻撃から保護しており、学生たちは毎年最大1,000時間のセキュリティ経験を現場で積み重ねています。

業種：大学・研究機関(行政・公共機関)

ソリューション：セキュリティ、プラットフォーム

製品：Splunkプラットフォーム、Splunk Enterprise Security、Splunkアカデミックアライアンス、Splunk SOAR

LSUの学生はサイバーセキュリティに関してトラのように鋭い目を持つ

ルイジアナ州立大学(LSU)は164年間にわたり、学生たちが生涯にわたり成功を収め、ルイジアナ州のより良い未来に貢献できるよう導いてきました。2023年には米国家安全保障局によってCenter of Academic Excellence in Cyber Operations (サイバーオペレーションの中核的研究拠点)に指定されており、パープルとゴールドの大学旗のもと、最も優れたサイバーセキュリティ教育を提供する機関としての地位を確立しています。LSUの学長、William Tate氏によるサイバーセキュリティ指令を受け、LSUのCISOを務めるSumit Jain氏はCIOのCraig Woolley氏に対し、学生たちにSOCの現場経験を積ませながらLSUのサイバーセキュリティ態勢を強化するという大胆な構想を持ち掛けました。それだけではありません。ルイジアナ州高等教育機関理事会と共同で、州のすべての高等教育機関を保護する取り組みにも乗り出しました。

成果

18
保護対象の大学

最大1,000時間
学生が毎年積むことが可能なSOC経験

24時間365日
セキュリティ対応

LSUは、この大胆な構想を形にするために、適切なテクノロジーパートナーを必要としていました。そこで選ばれたのが、Splunkとマネージドセキュリティプロバイダーの TekStream社です。現在、LSUの学生主体のSOCプログラムはルイジアナ州の18の大学に対応しており、その数は増え続けています。導入は急速に広がっており、対象となる大学は2025年までに38校に達する見込みです。この取り組みは州全体の学術機関のサイバーセキュリティを強化するとともに人材育成に着実に貢献しており、全国的な模範となるサイバーセキュリティカリキュラムの基盤になっています。

(パープルと)ゴールドを目指して

LSUの学生主体のSOCプログラムは18の大学に対応するまでに成長しており、さらに20校が加わる見込みです。オンボーディングと学生のトレーニングを効率的に実施できるようになったことで、LSUはこのプログラムを当初の見込みよりもさらに多くの大学へと展開することができました。「Splunk、TekStream社、LSUの提携により、人材、プロセス、テクノロジーの完璧な組み合わせが実現しています」とJain氏は述べています。

このプログラムの最大の特長は、大学全体を挙げての包括的な取り組みである点です。学生主体のSOCは、IT、サイバーセキュリティ、コンピューターサイエンス専攻の学生を参加対象とするのが一般的です。Woolley氏は次のように述べています。「当校の執行部および高等教育機関理事会は、全員を対象とした機会とすることを望んでいました。よって、このプログラムはあらゆる学科の学生に開かれています。唯一求める条件は、批判的思考力です。それさえあれば、後はどんなことでも学んでいけます」

この戦略は奏功しています。「サイバーセキュリティは非常に専門的な分野なので、目新しいことばかりです」と、学部生時代に人事学を専攻していたJain氏は語ります。「とはいえ、将来に通用する実践力のあるサイバーセキュリティ人材を育成し、拡大する脅威に対抗するには、さまざまな背景を持つ学生と共に取り組むことが極めて重要です」

> Splunkは効率性と使いやすさの点で当校にぴったりの製品でした。Splunkは最も優れたソリューションです。
>
> **Craig Woolley氏**、LSU、CIO

LSUの学生がSplunkユーザーに

学生主体のSOCプログラムの実現にあたり、LSUは複数のSIEMソリューションを検討しました。「結果として、Splunkは効率性と使いやすさの点で当校にぴったりの製品でした。Splunkは最も優れたソリューションです」とWoolley氏は語ります。

わずか1年の間に、参加している各学生は最大1,000時間のSOC経験を現場で積み重ねています。参加期間中、学生たちはTekStream社のサポートを受けながら実際の従業員さながらの研修を受けます。Splunkアカデミックアライアンスのコースを受講し、Splunk SOARにTekStream社が構築したプレイブックを教材に、さまざまなユースケースと収集する必要のある証拠について学びます。TekStream社と共同で、参加者は22種類の検出結果を調査する力を身につけます。2024年初頭にSplunk SOARの使用を開始して以来、学生たちはSOCのサイバーセキュリティインシデント全体のおよそ33%に対応してきました。

参加する各大学がSplunk Cloud PlatformおよびSplunk Enterprise Security (ES)のインスタンスを運用し、さまざまなダッシュボードを活用してSplunk SOARの統合環境で状況を確認することで、分析の効率化を図っています。「かつて、LSUでは手動で対応していました」とJain氏は話します。しかし現在は、Splunk SOARプラットフォームの自動化機能であるプレイブックを活用し、インシデントを自動で修復することで対応を効率化しており、特に終業後のメリットは顕著です。

「LSUでは、インシデントが夜の6時、7時、8時といった時間帯に発生したときには、翌朝まで確認されないのが当たり前でした」とJain氏は続けます。「今では、SOCプログラムによって24時間365日の対応が実現しており、LSU、さらに州全体の総合的なセキュリティ態勢が向上しています」

Jain氏にとって学生主体のSOCプログラムでSplunkを使用することの大きなメリットは、重要なセキュリティイベントを特定して、わかりやすく報告できる点です。「すべてのインシデントを単一の環境にまとめる機能は、このプログラムの効率化および参加大学のセキュリティ確保に大いに役立っています」とJain氏は述べます。そうでなければ、各大学がそれぞれの環境を自主的にチェックして重要イベントを把握しなければなりません。Jain氏はこう続けます。「そうする代わりに、我々は各大学の状況を単一画面で包括的に確認しながら対応しています。Splunkなしでは、この学生主体のSOCプログラムは成功していなかったでしょう」

「さあ行け、タイガース!」

学生主体のSOCの1期生の参加者が2024年12月に卒業を控える中、LSUでは彼らの就職に向けて、可能な限りの差別化要因を生み出したいと考えています。その一環として、TekStream社と共同で、各学生にSOCの経験を総合的に記載した成績証明書を発行し、学生たちが就職面接で提示できるようにしようと計画しています。「取り組んだすべての重要インシデントと対応件数に加え、どのような複雑な状況を乗り切ったかが明記されます」とJain氏は述べています。

Woolley氏は次のように語っています。「この経験を就職先に証明できれば、学生たちの卒業後の成功を後押しできるはずです。これは、LSUのプログラムならではの特長です」

25_CMP_cust_LSU_v3-JA-202506

2025年6月までに、LSUはプログラムの参加大学を38校まで増やし、同州の高等教育機関の大半に対応することを目指しています。Woolley氏は次のように述べています。「オンボーディングプロセスは最適化している最中ですが、目標達成への取り組みは順調そのものです」

しかし、これで終わりではありません。Woolley氏はこう締めくくりました。「今回の成功を受けて、学生主体のSOCをもうひとつ設立し、全国の大学が利用できるようにしたいと考えています。プログラムの利用をルイジアナ州の大学に限定する必要はないのですから」

> Splunkなしでは、この学生主体のSOCプログラムは成功していなかったでしょう。
>
> **Sumit Jain氏、**LSU、CISO

25_CMP_cust_LSU_v3-JA-202506