UNLV：SOCへの学生参加とSplunkで成功を収める

主な課題

サイバーセキュリティの人材とリソースが限られる中で、キャンパス全体のセキュリティを維持しながら学生に優れた実践的教育を提供できる創造的なソリューションを必要としていました。

主な成果

大学のSOCに参加する学生は、Splunkアカデミックアライアンスが提供するトレーニングを受け、構内のデジタル環境で見つかる重大な脆弱性を修正しながらセキュリティを実地で学んでいます。

UNLV

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 Cloud Platform、Splunk Enterprise Security、Splunkアカデミックアライアンス

UNLVでの実践的教育を通じたセキュリティ強化

ネバダ大学ラスベガス校(UNLV)は、米国屈指の研究機関であり、モハーベ砂漠の中心部に位置する知のオアシスです。UNLVのセキュリティチームは、わずか4名の専任のSOC (セキュリティオペレーションセンター)アナリストで構成されており、3万5,000人の学生と教職員が利用する複雑なデジタル環境を守るには、追加のサポートが必要でした。

「大学のセキュリティを維持するためにできる限りのことをしたいと思っています」と、UNLVのIT担当シニア情報セキュリティアナリストであるJason Griffin氏は言います。「また、教育の観点から、サイバーセキュリティを学ぶ学生に、社会に出てから必要になる知識と経験をここで身に付ける機会を提供したいとも考えています」。UNLVは、Splunk Enterprise Security、Splunk Cloud Platform、Splunkアカデミックアライアンスを活用して、その目的の達成を目指しています。

成果

600件以上
最初の6カ月間で修正した脆弱性の件数

大幅に向上
ハイブリッド環境の可視性

100%
卒業後の就職率

SIEMで築くサイバーセキュリティの拠点

2022年に開始されたUNLVのSOCプログラムでは、サイバーセキュリティを学ぶ学生に、アラートへの対応、チケットの相関付け、インシデントの優先順位付け、重大なセキュリティ脆弱性の解決といったSOC業務を実地で体験してもらい、セキュリティ人材に不可欠なスキルを育成しています。そして、その努力は実を結びつつあります。「Splunkのダッシュボードやアラート機能を利用することで、脆弱性管理プログラムの可視性が大幅に向上しました」とGriffin氏は評価します。「2024年5月以降、学生たちは600件以上の脆弱性を修正しており、そのうち約100件が重大な脆弱性でした」。こうして、学生のスキルが高まるとともに、キャンパスのセキュリティも向上しています。

「当初は、複数のプラットフォームへのログインから、データやスキャン結果の検証、チケットの作成まで、すべてのプロセスを手動で行い、重複やエラーがないことをただ祈るだけでした」とGriffin氏は説明します。現在では、Splunk Enterprise Securityを活用して、各種の運用ユースケースに応じたデータを取り込み、相関付けしています。ネットワーク内で不審なアクティビティが検出されると重要イベントが生成されるので、そこから詳細調査を開始します。Griffin氏とそのチームは現在、Splunkを使って複数のソースからデータを取り込み、相関付け、ワークフローアクションによってチケットシステムに接続することで、このプロセスを自動化することに取り組んでいます。「脆弱性の修正にかかる時間は以前に比べて半減しました。プロセスを完全に自動化すれば10分の1まで短縮できると見込んでいます」とGriffin氏は期待を寄せます。

アダプティブレスポンスなどの組み込みの機能も大きな効果を発揮しました。学生アナリストは、この機能を活用してドリルダウン検索を行うことで、より詳細な調査が可能になりました。さらに、事前設定されたオプションや、外部サイトへのアクセス機能も、プロセスの効率化に役立っています。

「Splunk Enterprise Securityのおかげで可視性が大幅に向上しました」とGriffin氏は言います。「以前は環境内で問題が起きていることを把握するのがやっとでしたが、今では環境全体を可視化して、問題の発生と同時に対処できるようになりました。ついに、リアルタイムの検出を実現したのです」

「Splunk Enterprise Securityは、大学のセキュリティ態勢の向上だけでなく、実践的教育の強化にも役立っています」と、UNLVの最高情報セキュリティ責任者(CISO)であるVito Rocco氏は評価します。「学生にSOCで実際の業務を経験してもらうことで、卒業後の視野と機会を広げることができます」

UNLVの最高情報責任者(CIO)であり、Rocco氏と協力して州からの助成金や承認の獲得に尽力しているKivanc Oner氏もこれに同意し、次のように付け加えます。「このプログラムは、学生に最先端のスキルを身に付けてもらうだけでなく、ネバダ州全体のサイバーセキュリティを強化することにもつながります。次世代のサイバーセキュリティリーダーを育成することで、州のデジタル環境の未来を有能な人材に託すことができます。Splunkはこのミッションにおいて重要なパートナーであり、教育と実践の橋渡しに貢献してくれています」

> Splunk Enterprise Securityは、大学のセキュリティ態勢の向上だけでなく、実践的教育の強化にも役立っています。学生にSOCで実際の業務を経験してもらうことで、卒業後の視野と機会を広げることができます。
>
> **UNLV最高情報セキュリティ責任者(CISO)、Vito Rocco氏**

学生たちはもちろん、このプログラムに熱心に取り組んでおり、SOCでの実践経験は1年間で最大1,000時間にも達します。それを思えば、このプログラムに参加した学生の就職率が100%であるのも驚くことではありません。Griffin氏によると、学生のほとんどが卒業後も大手小売企業や米軍などでサイバーセキュリティ関連の職に就き、全員が卒業前にSplunk Core Certified Power User認定を取得しています。「このプログラムに参加する学生たちの意欲と、Splunkを活用し、この優れたツールについて理解したいという強い思いが、こうしたすばらしい成果につながっているのです」と同氏は称賛します。

トレーニングで成功を掴む

Griffin氏は、UNLVでSplunk Enterprise Securityを運用してキャンパス全体のセキュリティを監視するほかに、Splunkアカデミックアライアンスを通じて大学院レベルのセキュリティデータ分析を教えるコースで講師も務めています。「.conf 2021で、このプログラムと、Splunkが学生に提供している機会について知りました」とGriffin氏は言います。当初は、同氏のカリキュラムを補強するための選択科目としてアカデミックアライアンスのトレーニングを提供していましたが、翌年からシラバスで必修科目としました。「月曜日は分析、水曜日はSplunkを教えています。いつも、分析の講義で議論した内容からいくつかのコンセプトを抽出し、Splunkの講義に引き継いでいます」

UNLVでアカデミックアライアンスプログラムの恩恵を受けているのは学生だけではありません。大学職員もSplunkに関する研修を受けています。「現在、大学のサイバーセキュリティチームがこのプログラムを通じて実際にトレーニングを行っています」とGriffin氏は説明します。「私自身も、後れを取りたくないので、教材を読んで最新の状況を学んでいます。まさに一石二鳥です」

クラウドで新たなレベルへ

Splunkのメリットは、UNLVのサイバーセキュリティチーム以外にも及びます。UNLVのIT担当シニア2 IT運用アナリスト兼スーパーバイザーであるJeremiah McClain氏は、2010年からSplunkのオンプレミス版を使用してきました。その間、UNLVのネットワークは単一サーバーからサーバークラスター構成へと拡大し、それに合わせて容易に拡張できるソリューションが必要になりました。そこで最近、オンプレミス版からSplunk Cloud Platformに移行しました。

> Splunkで私たちは火を発見しました。
>
> **UNLV IT担当シニア2 IT運用アナリスト兼スーパーバイザー、Jeremiah McClain氏**

「Splunk Cloud Platformでは、ユースケース、アクセス要件、保持期間に基づいてデータを簡単に分類できます」とMcClain氏は説明します。「基本的なダッシュボードであれば、ユーザーがほんの数分で利用できるようになることもあります」。メリットはほかにもあります。

UNLVのIT担当ITオペレーションセンターディレクターであり、Splunkのビジネス面の推進役を務めるPaul Trinidad氏は、次のように述べています。「クラウドへの移行は、長期的にコストの大幅な削減になるだけではありません。管理作業にかかる時間も大幅に節約してくれるため、チームは組織に付加価値をもたらす業務により集中できるようになります」

McClain氏もこれに同意し、メリットとして、ダッシュボードの構築とGriffin氏のサイバーセキュリティ業務のサポートも付け加えます。「環境全体を包括的に可視化できるようになり、チーム間の連携が深まりました」

クラウドに移行して以来、稼働率も大幅に向上しています。「信頼性が格段に高まりました」とMcClain氏は評価します。「また、皆が利用するサービス、特にセキュリティチームが利用するサービスの運用が以前よりも楽になりました。プラットフォームの堅牢性とレジリエンスは高いに越したことはありません」

UNLVが果たす役割

Griffin氏とMcClain氏は、UNLVのSOCプログラムをネバダ州全体に拡大して、他の大学を支援したいと考えています。同時に、キャンパス内でのSplunkのユースケースの拡大にも取り組んでいます。ウェルネスセンターのライン管理から、保守依頼の優先順位付け、ラボ機器からの研究データの取り込みまで、2人はほぼあらゆる領域でSplunkを活用することを目指しています。

「Splunkで私たちは火を発見しました」とMcClain氏は言います。「次はどうしますか?」

Griffin氏は答えます。「車輪を発明しましょう」

Splunkを無料でダウンロードするか、Splunk Cloudの無料トライアルをお試しください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわりなく、お客様のニーズに最適な展開モデルでご利用いただけます。