導入事例

University of Zurich[UZH]

チューリッヒ大学の中央IT部門 Stellar Cyberでセキュリティを統合

Stellar Cyberは、AIと高度な相関関係を使用して、隠れた脅威を明らかにしアナリストの生産性を向上させます

チューリッヒ大学はスイス最大の大学で、25,000人以上の学生がいます。 チューリッヒ市に位置し、1833年に設立され、現在、哲学、人間医学、経済科学、法律、数学と自然科学、工学、コンピューターサイエンス、ロボット工学、神学、獣医学のプログラムを提供しています。国内の大学の中で最も幅広い科目とコースです。 大学には豊かな学術的伝統があります。2020年5月の時点で、13人のノーベル賞受賞者がチューリッヒ大学の卒業生、教員、または研究者として所属しています。

STELLAR CYBER®

限られた予算とセキュリティスタッフで大規模な学生と教職員に一元化されたITサービスを提供するという使命を持って、大学は既存のツールと統合しながら、必要なセキュリティアプリケーションを経済的に統合する新しいセキュリティプラットフォームを望んでいました。

導入前

無駄な時間
アナリストが脅威を見つけるのに数日または数週間かかる場合があります

誤検知
実際のセキュリティ問題から気をそらす

制限されたリソース
大学内のすべてのニーズをカバーする

限られたスタッフ
すべてのセキュリティをカバーする

ライセンス料
さまざまなセキュリティ機能の支払い

STELLAR CYBER 導入後

電光石火の速さ
アナリストが数日ではなく数分で脅威を見つけることができるようにします

50%少ない
誤検知 他のテストされた製品と比較

150以上をセキュア
大学および大学機関

24時間年中無休
自動化されたセキュリティカバレッジ

お金を節約
20以上のネイティブセキュリティアプリケーションを使用したライセンス料

“チューリッヒ大学の中央IT部門がサイバーセキュリティのための強固なプラットフォームを必要としていたとき、Stellar Cyberは、複数のソースからのデータを相互に関連付け、脅威ハンティング機能を改善し、実際の脅威を誤検知から分離することでアナリストの生産性を向上させるソリューションでした。”

既存のツールとの統合

チューリッヒ大学の中央IT部門のセキュリティチームは、別のSIEMを構築するだけでなく、セキュリティニーズに対応する最新のソリューションを見つけることを望んでいました。 チューリッヒ大学は他のソリューションを調査およびテストしましたが、Stellar Cyberは、単一の直感的なダッシュボードに約20のセキュリティアプリケーションを統合したため、最良の選択でした。

Stellar Cyberの導入は簡単でした。それはプラグアンドプレイのインストールであり、箱から出してすぐに結果を出し始めました。 Stellar Cyberの組み込みマルチテナンシーにより、セキュリティチームは大学ファミリー内の150を超える研究所や大学を効率的にサポートすることもできます。

“組み込みのマルチテナンシーに感銘を受けました”と、チューリッヒ大学の中央IT部門のITセキュリティ責任者は述べています。 “私たちは、それぞれ独自の問題を抱えている多くの異なる大学や大学の学部をサポートしており、それらを個別に追跡する必要があります。 私たちが見た他のすべての製品は、オプションとして提供されたとしても、マルチテナント操作をサポートするために非常に高価なアップグレードが必要でした。”

脅威の可視性の向上

Stellar Cyberの組み込みの検出により、セキュリティチームの可視性がすぐに向上しました。 “いくつかの基本的な設定で、私たちはすぐに多くの意味のある検出を行い、以前は見逃していたかもしれない多くのセキュリティイベントを発見しました”とITセキュリティ責任者は言いました。 “実際、使用の最初の1か月の間に、数日ではなく数時間以内に指摘することができたセキュリティケースがありました。 私たちが気付いたもう1つのことは、誤検知の割合が“トラフィック量は多くの誤検知アラートを引き起こし、実際の脅威をキャッチして対応する能力に大きな影響を与えました... Stellar Cyberは分析費用を削減し、脅威をはるかに迅速に殺すことができました。” テストした他の製品の半分であり、機械学習をトレーニングして以前の攻撃ベクトルを認識できるようにすることで、さらに効果的になります。”

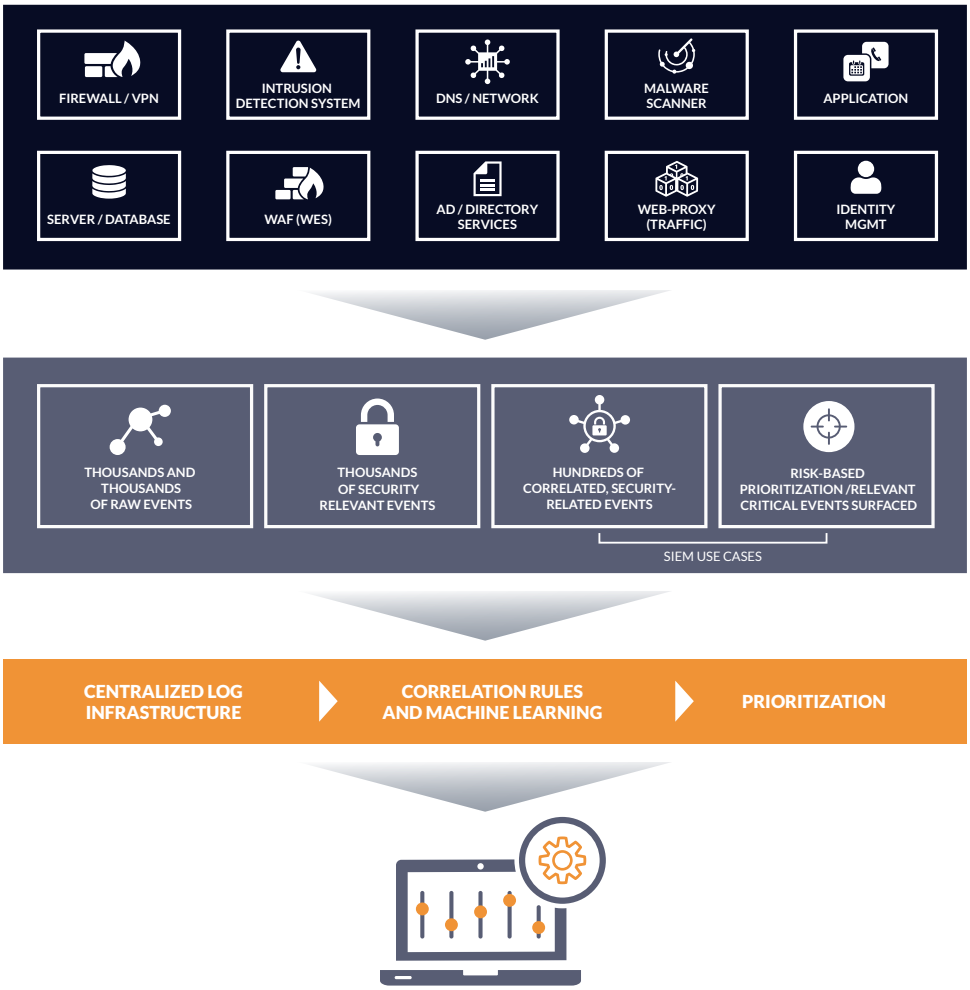
> “トラフィック量は多くの誤検知アラートを引き起こし、実際の脅威をキャッチして対応する能力に大きな影響を与えました... Stellar Cyberは分析費用を削減し、脅威をはるかに迅速に殺すことができました。”

“トラフィック量は多くの誤検知アラートを引き起こしており、実際の脅威をキャッチして対応する能力に大きな影響を与えていました”とITセキュリティ責任者は付け加えました。 Stellar Cyberは分析費用を削減し、脅威を迅速に消去することができました。”

Stellar Cyberは、攻撃対象領域のすべての領域からデータを収集し、無関係なインシデントと見なされる可能性のあるものを相互に関連付けて分析し、それらが実際の脅威であるか誤検知であるかを判断します。 大学のトラフィックが多い場合でも、他のシステムでは捕捉できない可能性のある脅威を発見します。 “以前は、多くの誤検知アラートが発生していましたが、実際の脅威をキャッチして対応する能力に大きな影響を与えていました”とITセキュリティ責任者は述べています。 “Stellar Cyberプラットフォームでの忠実度の高いアラートの自動優先順位付けにより、分析の生産性が大幅に向上し、実際の脅威をはるかに迅速に消去することができます。”

多くの教育機関で一般的であるように、チューリッヒ大学の中央IT部門は限られたスタッフで厳しい予算にありますが、さま

High Speed High Fidelity Detection & Automated Response



ざまな脅威からすべての独自のエンティティを保護するという大きな任務を負っています。
Stellar Cyberは、サイバーキルチェーン全体に沿って包括的なデータを相互に関連付け、直感的なダッシュボードに表示することで、ステージ1のアナリストタスク（複数のツールからのデータを手動で相互に関連付ける）の必要性を大幅に排除しました。 また、アナリストの努力をより生産的にすることで、時間とお金を節約できます。 そうでなければ脅威を追跡するのに数日または数週間を費やさなければならないアナリストは、Stellar Cyberインターフェースを介して数分でそれらを見つけることができます。

“重要な状況では、攻撃者のインフラストラクチャ（関与する外部IPアドレス）とすでに接続または接続されている内部エンドポイントの概要を把握するために、ドットを接続して攻撃状況をすばやく特定することができました”とチューリッヒ大学のITセキュリティオフィサーは述べています。”さらに、使いやすい”自動化”機能により、監視と対応を迅速に設定し、影響を受けるITマネージャーに、責任範囲内で新たに感染したエンドポイントについて自動的に通知することができました。 この種の自動化により、人的資源なしで24時間年中無休で対応できます。”ツールの削減によるもう1つの節約：Stellar Cyberには、マルウェア検出やIDSを含む20を超えるネイティブセキュリティアプリケーションが組み込まれているため、大学の中央IT部門は、現在使用しているスタンドアロンツールの一部を廃止できる可能性があるため、ライセンス料を節約できます。

チューリッヒ大学の中央IT部門がサイバーセキュリティのための強固なプラットフォームを必要としていたとき、Stellar Cyberは、複数のソースからのデータを相互に関連付け、脅威ハンティング機能を改善し、実際の脅威を誤検知から分離することでアナリストの生産性を向上させるソリューションでした。