導入事例

DEEPTREE

Deeptreeは、Stellar Cyber Open XDRで包括的なセキュリティサービスを提供します

Stellar Cyberを使用すると、Deeptreeは”もっと見る、もっと知る、より速く行動する”ことができます

アラスカに本社を置き、モンタナとプエルトリコにオフィスを構えるDeeptreeは、米国全土の顧客にサイバー防御、回復、および回復力のサービスを提供するマネージド検出および応答（MDR）プロバイダーです。Deeptreeは、金融、ヘルスケア、教育、製造、その他のセクターの企業に、総合的でカスタマイズされたセキュリティサービスを提供することに誇りを持っています。 エンタープライズクラスのセキュリティプレーヤーの専門知識とサービスへの献身と敏捷性を組み合わせて、あらゆる規模の企業がホワイトグローブサービスを利用できるようにします。Deeptreeは、セキュリティパッケージの中心であり、Stellar Cyber Open XDR（拡張検出および応答）プラットフォームを使用して、集中的なアナリストチームとともに世界クラスのサイバーセキュリティサービスをクライアントに提供します。

STELLAR CYBER®

DEEPTREE

アメリカではサイバー攻撃が他の場所の2倍発生する可能性があり、顧客は攻撃対象領域全体を保護し、どこにいても自分の場所に派遣できる専門知識を備えたセキュリティパートナーを必要としています。

導入前

散在するセキュリティ

サイロ化されたツールは、相関する検出を妨げました

制限

新しい機能を統合するのは難しい

高コスト

石畳のソリューションは高価でした

STELLAR CYBER 導入後

スケーラブル

小規模から大規模の顧客アカウントに簡単に拡張できます

機械学習

インシデントを自動的に関連付けて、潜在的な脅威を特定して評価します

合理化

単一画面ですべてを見て、すばやく反応します

応答性

ライバルよりも速く行動する

“Open XDRを使用しているため、拡張ツールを構築し、それらをStellar Cyberに統合して、新しいニーズを満たすことができると確信しています...”

STELLAR CYBER

https://jp.stellarcyber.ai

課題：すべての人に合わせたサービスを提供する

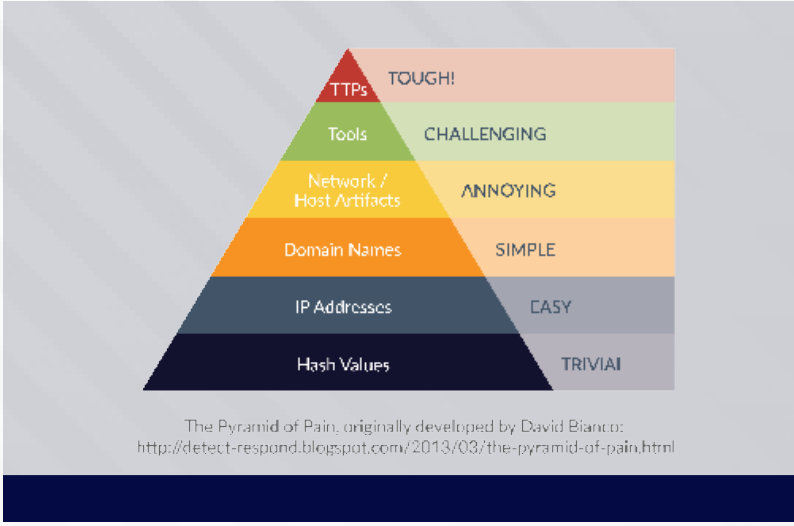
COVID-19のパンデミックの間、企業は仕事を成し遂げるために遠隔地の労働力にもっと目を向けてきました。 そして予想通り、これにより企業のサイバー攻撃対象領域が広がりました。 スタッフは主に企業VPNを使用しているため、防御には、標準の防御に加えて、ネットワークアクセス制御とユーザー/エンティティの動作分析が不可欠です。 労働者はもはや企業システムだけで保護されているわけではなく、家庭でのセキュリティのレベルは大きく変動します。 ネットワークの包括的なビューを実現することは、パンデミック時に組織の資産と価値の流れを守るのに役立ちます。 これは、オフィスの規模に関係なく当てはまります。

“サイバー攻撃は他のどこよりもアメリカで2倍発生する可能性があり、顧客は攻撃対象領域全体を保護し、どこにいても自分の場所に派遣できる専門知識を備えたセキュリティパートナーを必要としています”とDeeptreeのCEO ピーター・ハウス氏は述べています。 “私たちは、カスタマイズされたエンタープライズクラスのセキュリティサービスをすべての人に提供します。 これがStellarと提携することの利点です。スケーラビリティとはスケールアップまたはスケールダウンを意味します。 また、エンタープライズクラスのセキュリティを企業とその小規模なパートナーに提供することは、完全なカバレッジを意味します。 私たちの製品を設計する際、あるオペレーターに寄せられた批判は、一部のクライアントは小さすぎて問題にならないというものでした。 私たちのクライアントにとって、私たちはあなたがクライアントである限り、白い手袋は白い手袋であるように運営しています。違いは質ではなく量にあります。”

ソリューションの選択

セキュリティオペレーションセンターの中央ツールの選択プロセスは、現在のソリューションの悪徳を回避する必要があることを意味しました。ハウスによると、”サイロ化されたセキュリティツールを大量に入手するだけでは、ツール間で検出を相互に関

> “サイロ化されたセキュリティツールを大量に入手するだけで、ツール間で検出を相互に関連付けるという問題が発生することはわかっていました...”



連付けるという問題が発生することはわかっていました。 これにより、運用コストが上昇し、プロセスが遅くなり、応答時間が遅くなります。 そのため、重要なツールをすべて統合し、特定の顧客のニーズを満たすために必要に応じて他のツールを統合できる、包括的でクラス最高のセキュリティプラットフォームが必要でした。 ヘルスケアと金融は2つの非常に異なる業界であるため、異なるツールセットが必要です。 Stellarは、これらのさまざまなニーズに対応しながら、単一画面で使用できるようにします。”

主要なSOCベンダーを評価し、機能が不足しているか、新しい機能の統合に関して制限が厳しすぎることを発見した後、DeeptreeチームはStellar Cyberを発見しました。 Stellar Cyber Open XDRプラットフォームは、UEBA、EDR、NDR、SIEMなどの主要なセキュリティ機能を1つのインターフェイスに統合し、サードパーティのファイアウォール、IDS、SIEMおよびその他のシステムと簡単に統合できるオープンAPIを備えているため、Deeptreeに最適でした。

さらに、Stellar Cyberプラットフォームは、AIと機械学習テクノロジーを活用して、インシデントを自動的に関連付け、潜在的な脅威を特定して評価します。 誤検知がはるかに少なくなるため、Deeptreeのアナリストチームは、複雑な攻撃を見つけて修正する際に、はるかに高速で生産性を高めることができます。 Stellarを使用すると、Deeptreeは、対処が非常に困難であることが証明されているPyramid of Pain（痛みのピラミッド）のトップレベルで動作できます。

Open XDR：仮想バウンサー

“インターネットは浸透性です”とハウスは言います。 “ファイアウォールがあれば、城壁の後ろにいないわけではありません。 それは、千のドアがあるバーを操作するようなものです。 警備員のチームがいて、彼らはみんなと彼らの側近をチェックしなければなりません。 これは特にCOVIDとリモートワーカーに当てはまります。 すべてを見て迅速に反応できる仮想用心棒が必要です。 マルウェアを嘘で捕まえるには、視点からマルウェアを見る必要があります。複数の視点、 単一画面、それが Stellarの違いです。”

UEBAは、このタイプの脅威検出の基礎であり、ネットワークトラフィックが他のシステムが見逃している攻撃を明らかにするため、NDRに関連付けられています。 Stellar CyberのNDRおよびUEBA機能は、ログを分析するだけのSIEMではアナリストが見ることができない洞察を提供します。 たとえば、あるスピアフィッシング攻撃では、悪意のある人物が教師とその生徒の名前を知っており、おそらく別の教師からメールを送信していました。 DeeptreeはStellar Cyberを使用してこの策略を検出し、すぐに対応しました。

“検出のフットプリントが小さいため、応答がはるかに速く、より良くなります”とハウス氏は言います。 “アイラ・ウィンクラーは、”何があっても、保護は最終的に失敗する”と最もよく言っていました。そのため、対応する能力は非常に重要です。 それがアマチュアとプロを区別するものです。”

Stellarの機械学習がログ処理の大幅な増加を促進することで、Deeptreeの専門家は価値の差別化に集中することができます。 そのような例の1つは、メモリフォレンジックです。

“Deeptreeではボラティリティを誇らしげに使用しています。 また、Tier I技術者を含むすべての運用スタッフは、メモリフォレンジックトレーニングを受けます。 あるケースでは、Stellarは、クライアントホストで生成された一連のイベントID4656について警告しました。 ご存知のように、これはMimikatzが生成するクラスター内のEIDの1つです。 1時間足らずで、アラートから実行中のプロセスを正当なものとしてクリアするように移行することができました。”

今後の展望

Stellar CyberのOpen XDRプラットフォームとそのオープンAPIのおかげで、ハウスは、特定のタイプの顧客向けにカスタマイズされたセキュリティサービスを構築できる中心的なコアとして使用できると感じています。 これにより、Deeptreeの市場も拡大します。これは、新しいツールセットをコスト効率よく統合することで、新しいセグメントを特定し、それらに付加価値を与えることができるためです。“Open XDRを使用しているため、拡張ツールを構築し、それらをStellar Cyberに統合して、新しいニーズを満たすことができると確信しています。 これにより、サイバーセキュリティである進化し続けるスペースの観点からだけでなく、変化する市場ニーズの観点からも、将来を見据えた自信が得られます” とハウス氏は述べています。

ハウスは、Stellar Cyberを、新しいツールを統合し、他のシステムには見られない攻撃を発見して阻止する能力があるため、彼の成長と成功の鍵と見なしています。 “Stellar CyberのOpen XDRは、競合他社よりも多くのことを知り、より多くのことを知り、より速く行動できるため、競合他社の主要な差別化要因になると予測しています。”

“Stellar CyberのOpenXDRは、競合他社よりも多くのことを知り、より多くのことを知り、より速く行動できるため、競合他社の主要な差別化要因になると予測しています。”