Stellar Cyber(ステラサイバー)

https://jp.stellarcyber.ai

Stellar Cyber(ステラサイバー)は、2015年に米国シリコンバレーで創立されて以来、今日までOpen XDRの世界的リーダーとして業界を推進してまいりました。世界中の企業SOCおよびMSP・MSSP会社から高い信頼を得ております。Open XDRは、全ての検出と応答です。オープン(Open) で統一された、相関性のあるインテリジェントなセキュリティ運用プラットフォームを通じて、企業の攻撃対象領域全体を効果的かつ効率的に保護します。

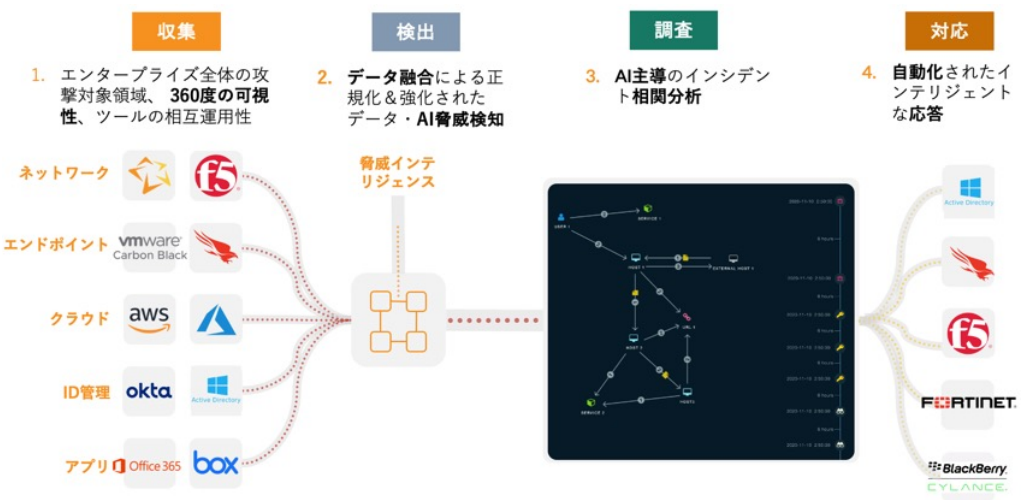
ステラサイバーはAI主導で未知の「脅威検知～脅威対処」を自動化、あなたの会社をサイバー攻撃から守ります。SOCの生産性を大幅に改善します。

AI次世代サイバー攻撃対策プラットフォーム

Stellar Cyber は、AI主導でサイバー攻撃の「脅威検知～脅威対処」を行い、SOCの生産性を劇的に改善します。レガシーな従来ツールは、EDR（エンドポイントデータ）、NDR（トラフィックデータ）、SIEM（ログデータ）などを個別に収集し分析していましたが、Stellar Cyberは全てのデータを１つに融合しAI主導で相関分析を行います。その結果、精度の高い相関分析が可能になり、脅威を素早く検出し、脅威に対して直ぐに対応することができます。

「収集～脅威検知～相関分析～応答」を自動化

Stellar Cyberは、４つのステージ「①収集 ②検出 ③調査 ④対応」を自動化します。ログ収集～脅威検知～相関分析～応答までをAI主導で自動的に行います。従来、手動で行っていた作業をAIが実施することで、パフォーマンスの向上および運用コストを削減します。平均検出時間(MTTD)で8倍、平均復旧時間(MTTR)で20倍の改善を実現します。



統合されたサイバーキルチェーン

Stellar Cyberのサイバーキルチェーンは５つのステージ（①最初の試み ②永続的な足場 ③ 探査 ④伝搬 ⑤浸透と影響）から構成されております。AIが脅威を分析し自動的に各ステージに分類します。セキュリティアナリストは、サイバー攻撃がどの段階にあるのか素早く把握することができます。

AIを活用した効率的なインシデント相関分析

AIを活用してアラートをリスク別にランク付け、インシデントに自動的に統合し、優先順位を付けて、攻撃の検出効率と有効性を大幅に向上させます。インシデントを分析のツールとして使用することにより、セキュリティチームは攻撃をより迅速に見つけ対処することができます。

SOCの生産性と効率を改善したいなら ステラサイバー！

Open XDR

- 運用･導入が容易
- ３６０度の可視性、AIが「脅威検知～脅威対処」を自動化、サイバー攻撃から保護
- AI主導のインシデント相関分析、アラート過検知･誤検知を削減、人手不足を解消
- オープン(Open)：ベンダーロックしない、3rd party製品連携、 既存資産を有効活用
- マルチテナンシー