opentext™ | Cybersecurity

記事

ArcSight 最新アップデート

ArcSight 2023.1 の新機能

ArcSight 2023.1：リアルタイム検出で ArcSight SaaS を次のレベルに引き上げる

一般リリース—ArcSight 2023.1 リリース

OpenText Cybersecurity は、OpenText™ ArcSight 2023.1 のリリースを発表いたします。ArcSight SaaS プラットフォームでのリアルタイム脅威検出の開始と、ArcSight ユーザーにとっての新時代の始まりを告げる歴史的なリリースです。ArcSight ユーザーが、クラウドホスト環境で ArcSight ポートフォリオの全機能を利用できるようになったのです。当社は、リアルタイムの脅威検出、SOAR、脅威インテリジェンス、行動分析、検索、ログ管理、コンプライアンス機能に支えられた、市場でも数少ない完全な SIEM as a Service (SaaS) ソリューションを、サイバーセキュリティチームに提供いたします。

SOC (セキュリティオペレーションセンター) にとって重要な時期でのリリースです。ますます複雑になる脅威に直面しながら、拡大し続ける攻撃対象領域を監視するセキュリティチームにとって、最新のサイバー脅威に対する防御は大きな課題です。潜在的な脅威が拡大し、熟練したセキュリティ専門家不足の影響が続くなかで、セキュリティチームは、組織が脅威にさらされないよう懸命に努力していますが、その仕事量は増加しています。さらに悪いことに、多くのチームは、システム管理、保守、セキュリティツールのアップデートに多大な時間と労力を費やさなければなりません。

ArcSight はこれらの課題を理解しています。2023.1 リリースは、絶え間なく変化する今日の脅威の実態に対応できる、業界をリードするセキュリティソリューションの提供への取り組みを示すものです。ArcSight 2023.1 では、リアルタイム検出、ネイティブ SOAR、検索の強化、新しい統合などにより、セキュリティ運用を簡素化し、脅威にさらされる時間を短縮できます。

ArcSight は、SaaS 上でのリアルタイムの脅威検出機能を実現することで、一般的な SIEM 市場の製品を超越する完全な SIEM as a Service ソリューションを提供します。リアルタイム検出と自動応答を組み合わせることにより、セキュリティチームが既知の脅威を迅速に検出して対応できます。これにより、平均検出時間 (MTTD) と平均応答時間 (MTTR) の目標を達成し、組織全体のサイバーリスクと脅威への露出を低減できます。

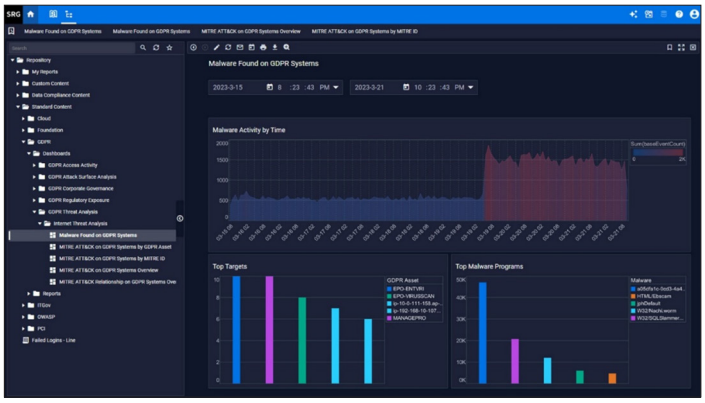

図 1. ArcSight SIEM as a Service 内の GDPR ダッシュボード

OpenText™ ArcSight SaaS を使用すると、サーバーの購入、インストール、管理が不要になるため、セキュリティ運用エクスペリエンスが簡素化されます。SIEM as a Service によって、インフラストラクチャのワークロードと保守の手間、習得に要する時間が低減されるため、アナリストチームに時間の余裕ができ、効率的な脅威ハンターやサイバーセキュリティでの実績を挙げることに専念できます。

ArcSight は、SIEM 分野での 20 年の経験に支えられ、最先端ソリューションのポートフォリオをお客様とそのチームに提供しています。これらのソリューションは、SaaS 環境とクラウド外環境の両方に完全に導入でき、その全方位の脅威分析と合理化されたリアルタイムサイバー防御により、チームが最新の脅威に対処できます。

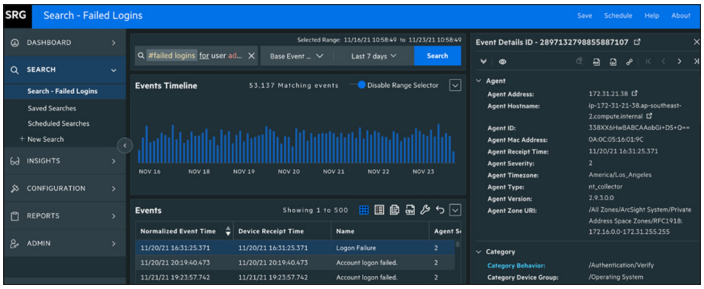

図 2. ArcSight SIEM as a Service のイベント詳細パネル

ArcSight SaaS のリアルタイムの脅威検出

脅威に迅速かつ効率的に対応することは、セキュリティ運用に不可欠です。今日の市場には多くの有用な脅威検出テクノロジーがありますが、サイバー環境で既知の脅威を発見してエスカレートする方法の中では、SIEM によるリアルタイムのイベント相関付けが最速です。イベント相関付けでは、アナリストがバッチ検索を待つ必要がなく、脅威関連のイベントをアナリストにリアルタイムで警告します。ArcSight は、リアルタイムの脅威検出で長年市場をリードしてきました。現在、この機能を SaaS 分野で提供している数少ないベンダーの 1 つとなっています。

ArcSight SaaS Real-Time Detection は、包括的なデータ収集とリアルタイムの脅威分析のソリューションとして機能し、既知の脅威が発生したときに SOC アナリストに警告します。ネイティブ SOAR (詳細は後で説明) と、最新の脅威と悪意のあるキャンペーンに関する最新情報を提供するネイティブの脅威インテリジェンスフィード (GTAP) がサポートする OpenText™ ArcSight SaaS Real-Time Threat Detection を使用すると、被害が発生する前に、セキュリティチームが脅威指標やサイバーインシデントに迅速かつ正確に対応できます。動的なイベントリスクスコアリングと優先順位付けによって、アナリストが誤検出を防止し、優先度が最も高い脅威に集中できます。ArcSight SaaS Real-Time Threat Detection では、脅威の可視化の強化、ダッシュボード、コンプライアンスサポート、MITRE ATT&CK 統合などの機能により、組織がそのセキュリティ体制をより明確に把握することもできます。

ArcSight SaaS Real-Time Threat Detection は、OpenText™ ArcSight Enterprise Security Manager (ESM) の後継製品です。クラウド外環境では残念なことにアーキテクチャの保守が必要ですが、ArcSight ユーザーは、市場をリードする ESM のリアルタイム検出機能の恩恵を長年受けてきました。ArcSight SaaS 上でリアルタイムの脅威検出が開始されたことで、SOC チームが時間のかかる保守の欠点を解消し、ESM ユーザーが重視してきた全社規模の脅威の可視性を維持できます。さらに、ArcSight SaaS はレポーティング機能とケース管理機能が強化されているため、将来に向けて SIEM をさらに強化する道筋ができます。

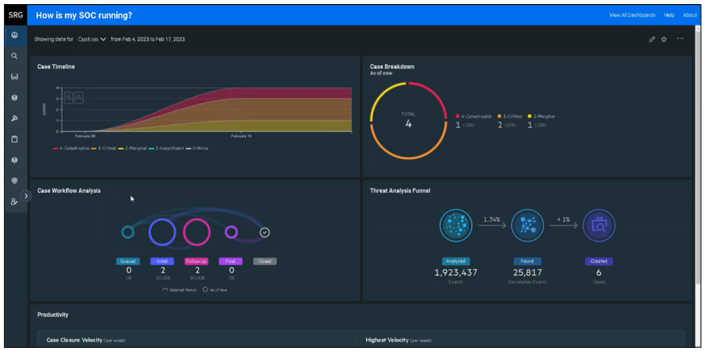

図 3. リアルタイムの脅威検出内の SOC Metrics ダッシュボード

ArcSight SaaS SOAR

OpenText™ Security Orchestration, Automation, and Response (SOAR) は、最新のセキュリティ分析において非常に重要です。組織が脅威に対して迅速かつ結束して対応できるからです。SOAR は、誤検出を減らし、対応を自動化し、チームのコラボレーションを促進するため、セキュリティ運用の効率化に不可欠です。

ArcSight は、2020 年に ArcSight SOAR (クラウド外) をリリースして以来、SOAR を補完的なネイティブソリューションとして提供してきました。そして 2022 年 12 月、その SOAR を、ArcSight SaaS プラットフォームのネイティブコンポーネントとして、SaaS の分野に導入しました。すぐに使える戦略ガイドと 120 以上の統合プラグインを備えた ArcSight SOAR は、トリアージ、調査、応答アクティビティを効果的かつ効率的に自動化し、オーケストレーションします。また、視覚的なワークフロー戦略ガイド、KPI に関する詳細なレポート、詳細なケースタイムラインによる優れたチームコラボレーションをサポートします。

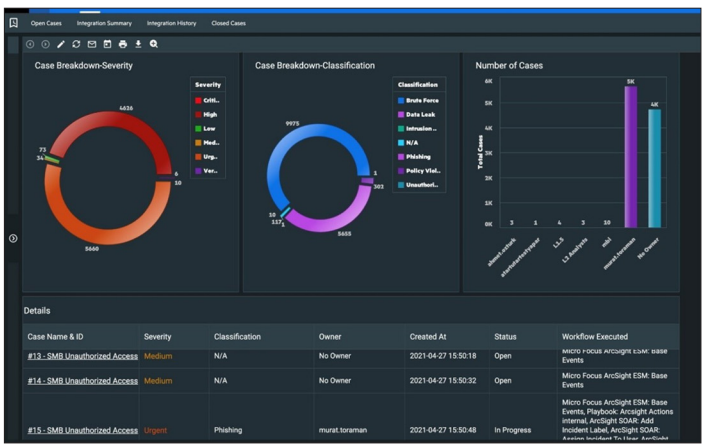

図 4. ArcSight SOAR レポートとダッシュボード

SOAR は、リアルタイムの脅威検出と密接に連携し、OpenText™ ArcSight SaaS プラットフォームのすべてのケース管理と自動応答を処理します。リアルタイムで脅威を検出し、最もリスクの高い脅威に優先順位を付けたあと、自動応答と強調的なチームの取り組みにより SOAR をこれらの脅威に向けることで、ArcSight は脅威への露出を減らすとともに、運用効率を向上させます。

ArcSight 関連の最新のニュースと認識

- プレスリリース：ArcSight は堅調な評価とイノベーションのニュースで 2022 年を好調に締めくくる
- ArcSight、GigaOm Radar で SIEM のリーダーとファストムーバーとして認定される
- ArcSight、MITRE ATT&CK に焦点を当てたこの競合ベンチマーク評価で 10 点満点のスコアを獲得

ArcSight 2023.1 は次の最新リリースで構成されています。

- ArcSight SIEM as a Service (SaaS)
- OpenText™ ArcSight Platform 23.1
- OpenText™ ArcSight ESM 7.6.4
- OpenText™ ArcSight Intelligence 6.4.4
- OpenText™ ArcSight Recon 1.5.1
- ArcSight SOAR 3.5
- OpenText™ ArcSight GTAP 2.0
- OpenText™ Transformation Hub 3.7
- OpenText™ ArcSight Management Center 3.2
- OpenText™ ArcSight SmartConnectors 8.4.1
- OpenText™ ArcSight Logger 7.2.2

ArcSight 2023.1 リリースの主な機能と改善点を以下に示します。詳細については、個別のリリースドキュメント (**この記事の最後にリンクがあります**) をご覧ください。

ArcSight SIEM as a Service (SaaS) のリリースの概要

リアルタイムの脅威検出

主な特長

- **リアルタイムの脅威検出の効率化。**市場をリードする ArcSight の相関テクノロジーを活用して、脅威関連のイベントが発生するとアナリストに警告します。
- **動的なリスクスコアリングと優先順位付け。**アナリストが最初に最もリスクの高い脅威に集中すると同時に、誤検出を阻止できます。
- **ネイティブ SOAR。**ArcSight SaaS Core Platform を介して、自動応答、戦略ガイド、SOC 分析などを促進します。
- **高度なケース管理。**SOAR 統合によって実現されます。
- **強化されたレポート機能。**100 種類以上のカスタマイズ可能な事前構築済みのレポートとダッシュボードによって、セキュリティ体制を視覚化できます。
- **効率的なコンプライアンスモジュール。**規制要件に対応するコンプライアンスチームの負担を軽減します。
- **検索機能とハント機能。**リアルタイムの脅威検出チームの対応範囲を拡大し、ソリューションの中核となるリアルタイム検出機能を補完します。

SOAR

主な特長

- **SOAR 機能の導入。**ArcSight SIEM as a Service (SaaS) ベースのプラットフォーム製品内に組み込まれています。これにより、自動化されたトリアージ、調査、応答のメリットを ArcSight SaaS のすべてのお客様が活用できます。追加のライセンスや料金は不要です。
- **新しい統合プラグイン。**次の分野に重点を置いています。
  - **エンドポイント保護 /EDR：**Microsoft Defender for Endpoints、CrowdStrike
  - **脅威インテリジェンスデータベース：**CyberRes Galaxy、FraudGuard、Intezer
  - **クラウドサービス：**AWS Network FW、Azure Security Groups、AWS Lambda
- **Microsoft Teams や Slack との統合。**ChatOps をサポートし、SOC 以外の部門やエンドユーザーを調査や対応活動に参加させられます。
- **生産性とケースによる負荷ダッシュボードウィジェット。**アナリストチームのワークロードとパフォーマンスを可視化します。
- **近日リリース：**SentinelOne EDR、Microsoft Defender for Cloud Apps、BMC Helix Remedyforce、Sailpoint、Domaintools、Netskope、Cisco Umbrella との追加統合

ログ管理とコンプライアンス

主な特長

- **改ざん防止イベントストレージ。**データソースから受信したイベントに不変性を強制します。
- **新しい検索演算子。**「wheresql」などの新しい検索演算子が、複雑な検索で強力な脅威ハンティング機能を発揮します。
- **検索演算子チェーン。**別々のクエリを実装するのではなく、複数の検索演算子を 1 つのクエリに連結して、複雑なクエリステートメントを構築できます。
- **拡張された検索機能。**データを表示するための多くのオプション (リニアスケールやログスケールなど)、ヒストグラムバーをクリックして一致するイベントをドリルダウンする機能、イベントを選択してイベントインスペクターを開く機能などをアナリストが使用できます。

- ［Search Home］タブ。検索アクティビティの概要が表示され、すべてのセッション (保存されていない) 検索のリストに加え、保存された検索クエリ、保存された検索条件、保存された検索結果、フィールドセット、ルックアップリストの状態を示すウィジェットが示されます。
- データ処理監視ダッシュボード。データベースへのイベントの取り込み速度の監視に役立つ、Database Event Ingestion Timeline ウィジェットを備えています。

行動分析

主な特長

- データ取り込みの最適化。
- セキュリティ更新プログラム。潜在的な脆弱性に対応します。
- 一般的なバグ修正。

ArcSight GTAP Basic 2.0 (2022 年 11 月リリース)

主な特長

- 追加料金なし。ArcSight をご利用のお客様は、追加料金なしで、基本レベルの脅威インテリジェンスコンテンツを利用できます。
- プラグアンドプレイ SmartConnector。脅威インテリジェンスの利用を簡単に開始できます。
- SOAR による自動応答。脅威インテリジェンス実装後のアナリストの作業が軽減されます。

ArcSight GTAP+ 2.0 (2022 年 11 月リリース)

主な特長

- プレミアム脅威インテリジェンス。OpenText Galaxy チームが収集したより具体的な情報により、情報に基づく適切な意思決定が可能になります。
- 意味の深い脅威インテリジェンス。30 以上のエンリッチメントフィールドにより、フィード内の個々の脅威のコンテキストを詳細に表せます。
- 自動ブロック。確実性の高い IoC を自動ブロックして、アナリストの業務負担を軽減し、瞬時にカバレッジを提供します。
- プラグアンドプレイ SmartConnector。脅威インテリジェンスの利用を簡単に開始できます。
- SOAR による自動応答。脅威インテリジェンス実装後のアナリストの作業が軽減されます。

ArcSight プラットフォーム (オンプレミス / クラウド外) のリリースの概要

ArcSight ESM 7.6.4

主な特長

- Java、SQL、Kafka、OS の広く使用されているアップデート。
- 安定性、セキュリティ、パフォーマンスの強化。
- 一般的なバグ修正。

ArcSight Intelligence 6.4.4

主な特長

- セキュリティ強化。
- 一般的なバグ修正。

ArcSight Recon 1.5.1

主な特長

- 改ざん防止イベントストレージ。データソースから受信したイベントに不変性を強制します。
- 新しい検索演算子。「wheresql」などの新しい検索演算子が、複雑な検索で強力な脅威ハンティング機能を発揮します。
- 検索演算子チェーン。別々のクエリを実装するのではなく、複数の検索演算子を 1 つのクエリに連結して、複雑なクエリステートメントを構築できます。
- 拡張された検索機能。データを表示するための多くのオプション (リニアスケールやログスケールなど)、ヒストグラムバーをクリックして一致するイベントをドリルダウンする機能、イベントを選択してイベントインスペクターを開く機能などをアナリストが使用できます。
- ［Search Home］タブ。検索アクティビティの概要が表示され、すべてのセッション (保存されていない) 検索のリストに加え、保存された検索クエリ、保存された検索条件、保存された検索結果、フィールドセット、ルックアップリストの状態を示すウィジェットが示されます。
- データ処理監視ダッシュボード。データベースへのイベントの取り込み速度の監視に役立つ、Database Event Ingestion Timeline ウィジェットを備えています。

ArcSight SOAR 3.5

主な特長

- SOAR 用の新しい統合プラグイン：
  - CyberRes Galaxy Threat Accelerator プラグイン。OpenText Galaxy 脅威インテリジェンスデータベースに含まれる IP アドレス、ドメイン、ファイル、URL を補完します。
  - Microsoft Defender for Endpoint プラグイン。攻撃を阻止し、マシンをネットワークから分離して、Defender のアラートを検索、管理します。
  - CrowdStrike Falcon Integration プラグイン。ネットワーク上の IOC を検索し、疑わしいエンドポイントをネットワークから分離します。
  - AWS Network Firewall プラグイン。脅威への対応の一環として、AWS ネットワークファイアウォールポリシーとルールを管理します。
  - Azure Network Security Groups プラグイン。応答アクティビティの一環として、Azure ネットワークセキュリティグループとルールを管理します。
  - Intezer Malware Analysis プラグイン。Intezer Malware Analysis サービスの疑わしいファイルを分析します。

  - **FraudGuard** プラグイン。カスタムブラックリストとホワイトリストを管理し、FraudGuard.io から評価スコアを照会します。
  - **AWS Lambda Integration** プラグイン。顧客のクラウド環境で Lambda 関数を呼び出します。
- **プラグインの向上**。Okta、Azure Active Directory、および McAfee Web Gateway 統合プラグインの向上により、デバイス関連のエンリッチメントとアクション、権限リストの作成、グループアクション、バージョンの互換性が容易になります。
- **生産性とケースによる負荷ダッシュボードウィジェット**。アナリストチームのワークロードとパフォーマンスを可視化します。

ArcSight GTAP Basic 2.0 および GTAP+ 2.0 (2022 年 11 月リリース)

主な特長

- ArcSight SIEM as a Service セクションの GTAP ノートを参照してください。

ArcSight Transformation Hub 3.7

主な特長

- パフォーマンスの向上および軽微なバグ修正。
- 詳細なドキュメントはこちら。

ArcSight Management Center 3.2

主な特長

- パフォーマンスの向上および軽微なバグ修正。
- 詳細なドキュメントはこちら。

ArcSight SmartConnectors 8.4.1

主な特長

- パフォーマンスの向上および軽微なバグ修正。
- 詳細なドキュメントはこちら。

ArcSight Logger 7.2.2

主な特長

- **メンテナンスリリース**。Logger 7.2.1 で発見されたセキュリティ上の脆弱性などの問題に対処します。
- **検索イベントのエクスポート**。以前のリリースと比較して、8.42 倍速く処理されます。
- **時刻同期**。Chrony ではなく NTP によって処理されるようになりました。この改善は、以前はスタンドアロンパッチとしてリリースされていましたが、現在は製品に統合されています。
- **近日公開：Logger 7.3**。セキュリティ脆弱性の修正、OBC の更新、ライブラリの更新に重点を置いています。

ArcSight のドキュメント

ユーザーガイド、リリースノートなど

- ArcSight SIEM as a Service (SaaS) 23.3.1
- ArcSight Platform 23.1
- ArcSight ESM 7.6.4
- ArcSight Intelligence 6.4.4
- ArcSight Recon 1.5.1
- ArcSight SOAR 3.5
- ArcSight GTAP 2.0
- Transformation Hub 3.7
- ArcSight Management Center 3.2
- ArcSight SmartConnectors 8.4.1
- ArcSight Logger 7.2.2

ArcSight の最新バージョン一覧

製品名	最新バージョン
ArcSight SIEM as a Service	常に更新
ArcSight プラットフォーム	23.1
ArcSight ESM	7.6.4
ArcSight Intelligence	6.4.4
ArcSight Recon	1.5.1
ArcSight SOAR	3.5
ArcSight GTAP	2.0
ArcSight Transformation Hub	3.7
ArcSight Management Center	3.2
ArcSight SmartConnectors	8.4.1
ArcSight Logger	7.2.2

詳細はこちら：
www.arcsight.com

お問い合わせ

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防、検出、対応から、リカバリ、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームが、包括的なセキュリティポートフォリオによるサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを利用できる OpenText Cybersecurity のお客様は、有効性の高い製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットを活かしてビジネスリスクを管理できます。

772-JA0001-009 | O | 12/23 |