AWS Security HubとSplunkを利用した

セキュリティ対策

セキュリティの脅威を検出、修復、防止する

splunk> | aws

目次

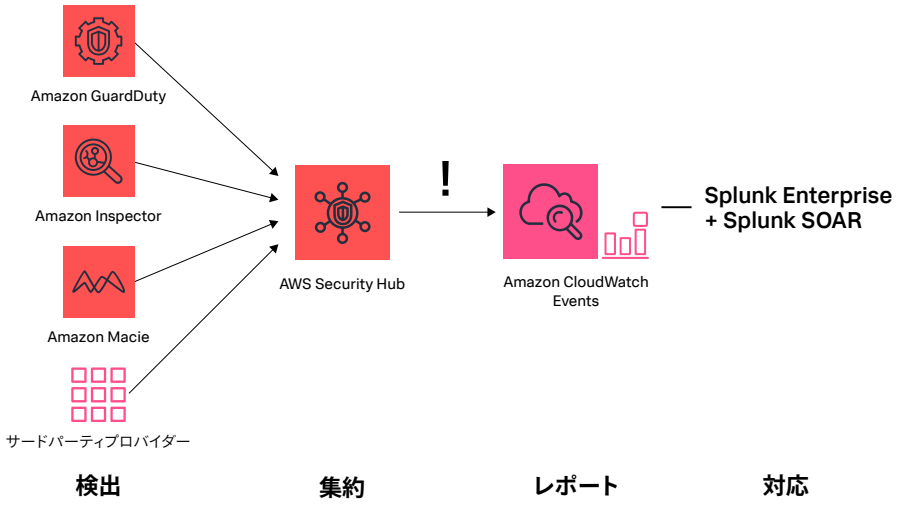
大量のデータが組織の足元を脅かす

新しいクラウドサービスを導入するたびに、組織には大量のデータが発生します。それにどう対処するかによって、データは成功への架け橋にも、泥沼への道にもなります。特にセキュリティ領域では、その差は歴然です。

アマゾン ウェブ サービス(AWS)では、Amazon GuardDuty、Amazon Inspector、Amazon Macieなど、AWSアカウントのセキュリティ体制を監視するために密接に統合された幅広いセキュリティサービスが提供されています。

AWS Security Hubは、AWS環境に導入されているすべてのAWSセキュリティサービスとサードパーティプロバイダーからの情報を集約、識別、優先順位付けします。

Splunkは、AWSと連携してクラウドのアプリケーション、インフラ、アカウントをリアルタイムで可視化するData-to-Everythingプラットフォームを提供します。そのインテリジェントな自動アシスタントによってセキュリティの脅威にすばやく効率的に対応し、リスクを低減できます。



AWS Security Hub：セキュリティアプローチの一元化を実現

- AWS環境全体のセキュリティ検出結果を集約
- セキュリティの検出結果を適切なターゲットに転送して対応を実行
- AWS環境に対して業界標準のコンプライアスチェックを実行
- Insightsによって注意が必要な領域を特定
- セキュリティに関するインサイトとアラートを視覚的な表示ですばやく確認

AWS GuardDuty：AWSワークロードを監視して問題を検出

- 重大度に基づく優先順位付けにより脅威検出の精度と可用性を向上
- 脅威の自動対応と自動修復を設定
- AWS Security Hubと統合してセキュリティ検出結果の活用範囲を拡大

SplunkとAWS Security Hubで強固な基盤を構築

Splunkプラットフォームは、AWS環境をエンドツーエンドでリアルタイムに可視化して、セキュリティアラートの分類、表示、対応を支援します。

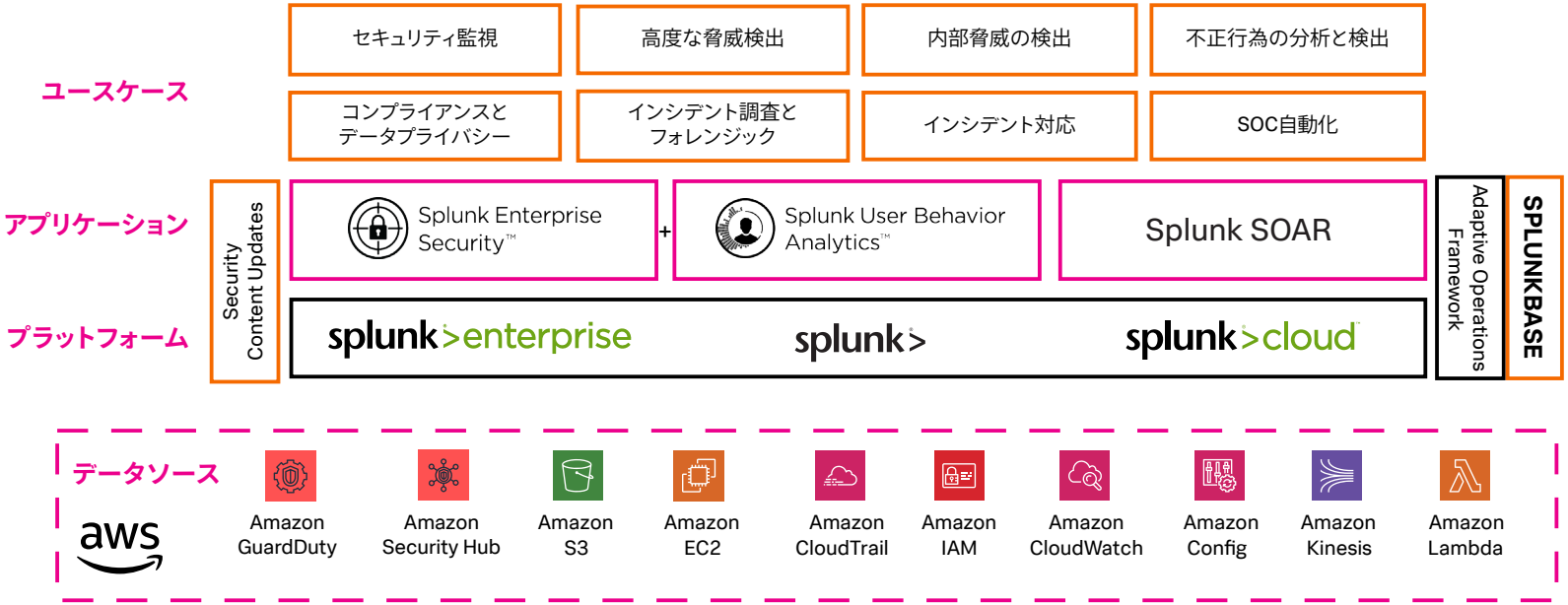
AWS Security Hubは、AWSやサードパーティのソースからのセキュリティ検出結果を集約し、単一の統合ポイントを介してSplunkに転送します。新しいデータソースはいつでも簡単に追加できます。 また、AWS Security Hubの設定オプションでSplunkに転送するセキュリティ検出結果を指定し、必要に応じて設定を変更することもできます。

Splunk SOARでは、機械学習とAI機能を活用して検出結果に基づく対応を自動化できます。SplunkとAWSを統合すると、セキュリティの脅威を未然に検出し、セキュリティチームの負担を軽減して、より価値の高い業務に人員を割り当てることができます。

SplunkとAWS Security Hubを統合するための4つのステップ

1. Splunk Add-On for AWSで統合ポイントを構築する
2. Splunk SOAR (セキュリティのオーケストレーションと自動化によるレスポンス)でSOARサービスを追加する
3. Splunk SOARのプレイブックでセキュリティ対応を自動化する
4. Splunk Mission Controlでセキュリティ体制を監視する

各ステップの詳細はこちら →



ステップ1：

Splunk Add-On for AWSで統合ポイントを構築する

AWS環境でSplunkを使用するためのベストプラクティスは、Splunk EnterpriseまたはSplunk CloudをAWSのデータ統合ポイントとして導入し、Splunk SOARを使用してデータにルール、自動化、インテリジェンスを適用することです。

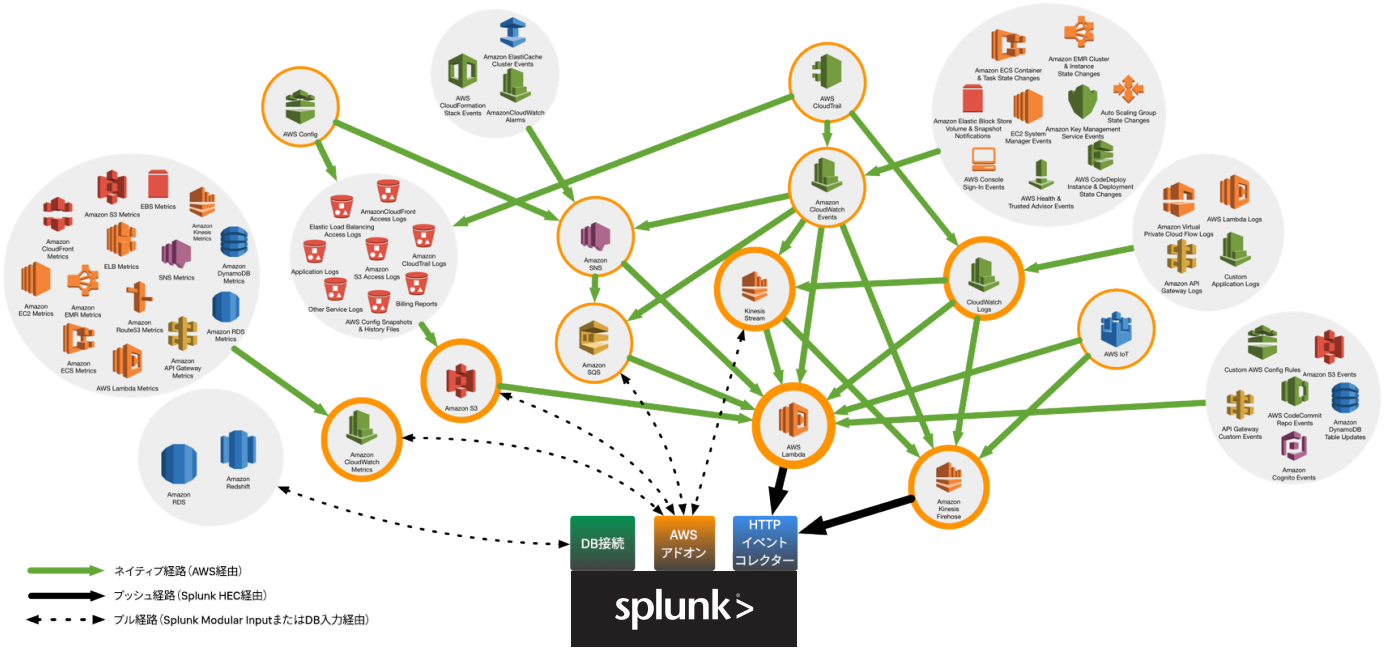
Splunk Enterpriseは、組織のデータ分析ニーズに対応する統合データプラットフォームソフトウェアです。Splunkでは、IT運用、セキュリティ、ビジネス向けのすべてのシステム、アプリケーション、デバイスで生成される構造化データと非構造化データを簡単に表示、調査、相関付けできます。また、AIと機械学習を活用してこれらの環境を監視および分析し、ほぼリアルタイムで問題に対応して、ビジネス価値を実現できます。

Splunk Cloudは、Splunk Enterpriseの利点を柔軟なクラウドサービスとして提供するAWSベースのサービスです。

SplunkプラットフォームとAWS間の統合ポイントを作成するには、Splunk Add-On for AWSを使用します。このアドオンの設定方法について詳しくは、ホワイトペーパー『Getting Data Into (GDI) Splunk From AWS (AWSからSplunkへのデータの追加(GDI))』を参照してください。

Splunk Add-On for AWSを使用したSplunkへのAWSデータの取り込み

*Splunk Enterpriseを使用せずにSplunk SOARを使用することもできます。この構成を適用する場合の注意点については、Splunkアカウントマネージャーにお問い合わせください。



ステップ2：

Splunk SOARで SOARサービスを追加する

AWS Security HubからSplunkにセキュリティ検出結果を転送したら、そのデータをすぐに活用する必要があります。

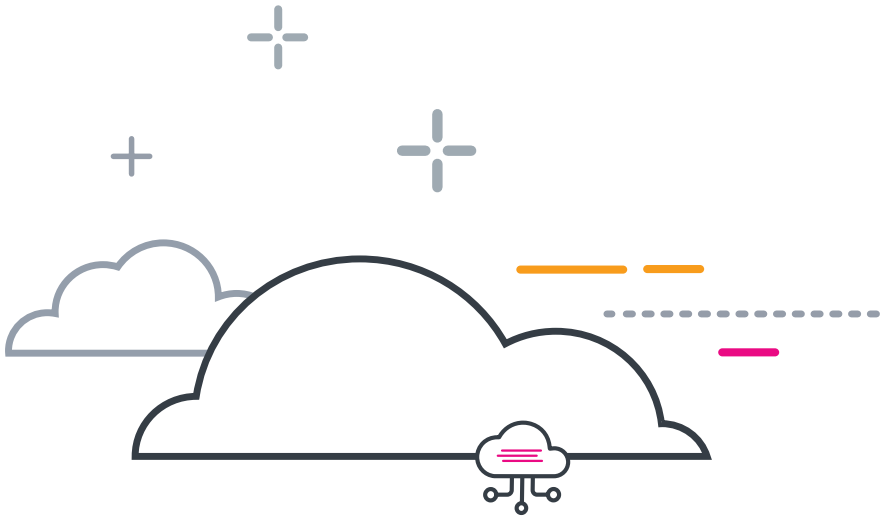
Splunk SOARは、セキュリティデータをフル活用して判断を自動化する、SOAR (セキュリティのオーケストレーションと自動化によるレスポンス)サービスです。

Splunk SOARの自動化フレームワークを使用すれば、AWS Security Hubから転送された検出結果を即座にアクションにつなげることができます。AWS Security HubとSplunk SOARの相乗効果により、AWS EC2インスタンスに対するSSHブルートフォース攻撃からAWS IAM認証情報の漏えいまで、あらゆるインシデントの対応時間を大幅に短縮できます。

Splunk SOARでは、8種のAWSサービスのほか、AWS Security Hubの情報に基づいて自動的に開始されるプレイブックなど、AWS Marketplaceで提供されているその他250種以上のセキュリティツールを統合できます。

Splunk SOARでは、インシデント、脅威の兆候、脆弱性、メールなど、セキュリティデータのタイプまたはソースに基づいてアクションが実行されます。また、サポートされる外部SIEMツールや分析ツールからSplunk SOARにデータをプッシュすることも、Splunk SOARから各種ツールのデータをプルすることもできます。

Splunk SOARに対応する1,200以上のAPIと225以上のAppインテグレーションで、ほぼすべてのデータを統合



SOC (セキュリティオペレーションセンター)を支援するSplunk SOARの6つの主要な機能

自動化：
コーディングが不要な視覚的なエディター、または内蔵のPython開発環境を使用して、ワークフローをコード化して自動化されたプレイブックを作成できます。

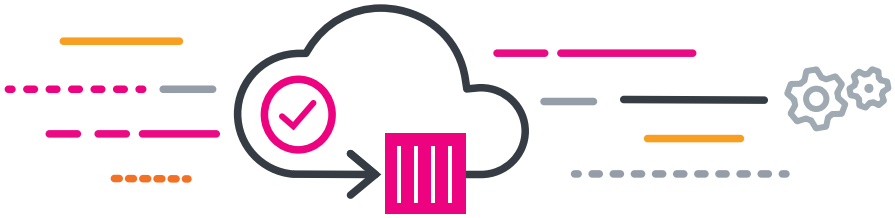
オーケストレーション：
数百のアプリと数千のAPIによってシステムを統合することで、チームとツールを横断する複雑なワークフローを連携および調整できます。

コラボレーション：
組み込みのチャット機能でケース情報などを共有してコミュニケーションを促進するとともに、プロセス全体でガイダンスを提供して作業を効率化できます。

イベント管理：
レベルの低いイベントやその他のセキュリティオブジェクトを自動、半自動、または手動で迅速にトリアージできます。

ケース管理：
確認したイベントを、Splunkのケーステンプレートや独自のテンプレートを使用してケースにエスカレーションすることで、ケースの状況や進捗を追跡および監視できます。

レポート作成とメトリクス：
セキュリティの状況把握に必要な重要情報をダッシュボードやレポートにまとめることで、人が行う監督や監査を効率化できます。



ステップ3：

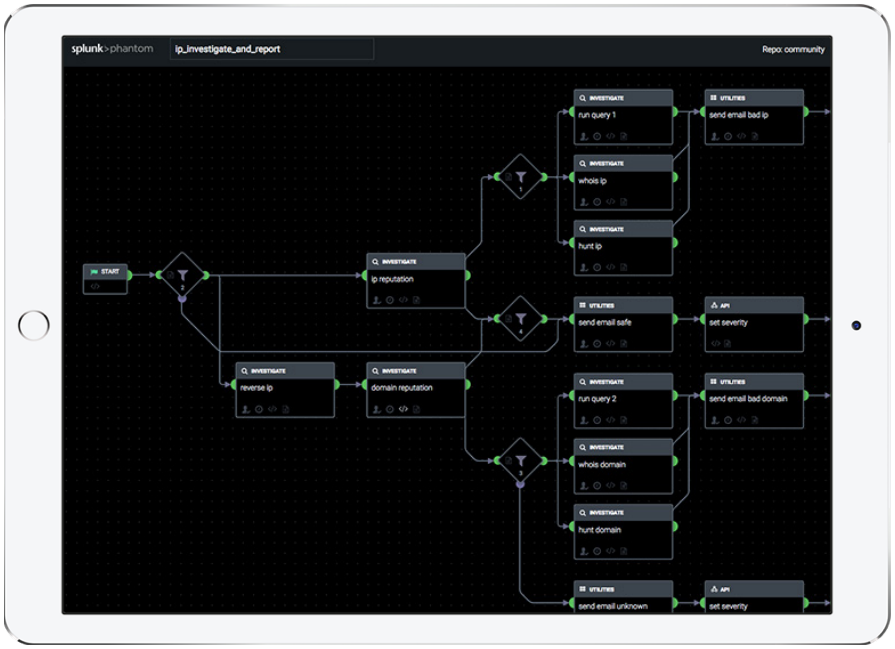
Splunk SOARのプレイブックでセキュリティ対応を自動化する

Splunk SOARには、セキュリティ運用(SecOps)計画をコード化するプレイブックが用意されています。その実体は、タスクを実行するためにSplunk SOARによって解釈される高レベルのPythonスクリプトです。プレイブックにより、Splunk SOARプラットフォームとその機能によって適切なアクションが自動的に実行され、セキュリティ運用に関するプロセスの再現性と監査可能性が確保されます。

プレイブックを使用すれば、手作業で行うと数時間はかかるセキュリティインフラでの一連の作業を数秒で実行できます。コーディングが不要な視覚的なエディター、または内蔵のPython開発環境を使用して、ワークフローをコード化し、自動化されたプレイブックを作成できます。

Splunk SOARのVisual Playbook Editor (VPE)では、開発の経験を問わず、複雑なSplunk SOARプレイブックをドラッグ＆ドロップでグラフィカルに作成およびカスタマイズできます。また、バックグラウンドでリアルタイムに実行されるすべてのサポートコードが自動生成されます。

さらに、関数ブロックやコネクターを使って操作の順序を指定したプレイブックを作成することもできます。



アクションは、Splunk SOARプレイブックで利用できる高レベルの基本要素です。たとえば以下のものがあります。

- **ファイルのデトネーション**
  サポート対象のサンドボックス内でファイルを実行します
- **IPの位置情報検索**
  指定されたIPアドレスの位置情報を検索します
- **ファイルの追跡**
  エンドポイントで特定のファイルを検索します
- **URLのブロック**
  ネットワーク境界上のデバイスで特定のURLをブロックします
- **デバイスの隔離**
  NACによって特定のデバイスをネットワークから切り離します

ステップ4：

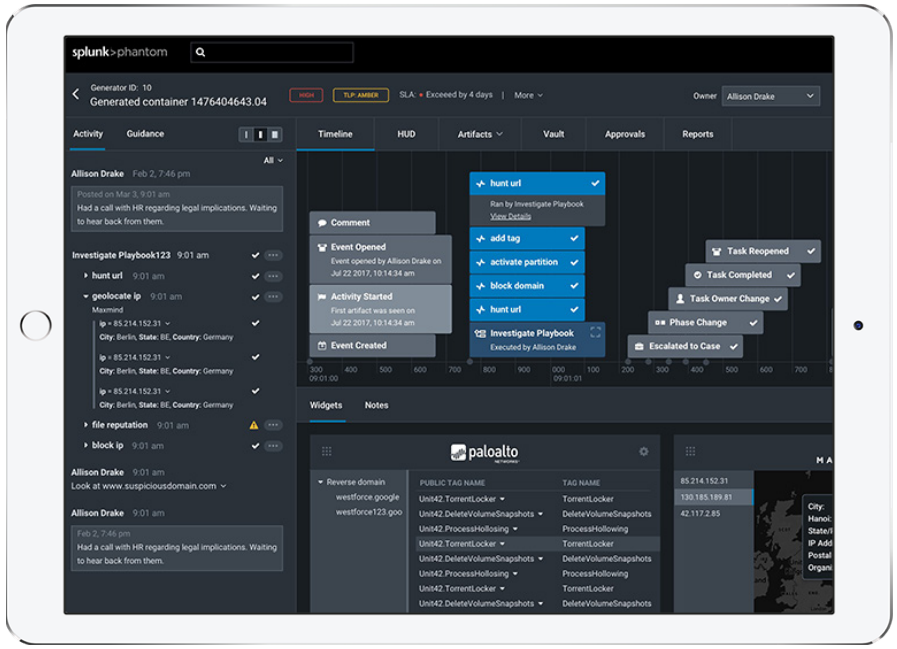
Splunk Mission Controlで セキュリティ体制を監視する

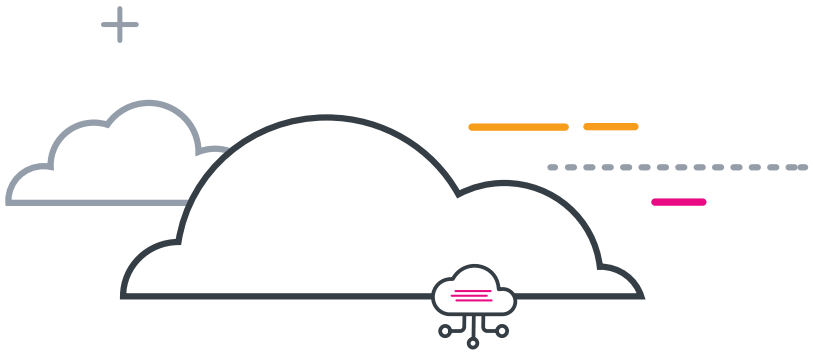
Splunk Mission Controlでは、イベントデータとSOCツールが1つの画面に統合されます。これによって画面やツールを切り替える手間を省き、イベントの確認、調査、対応を効率化できます。ステップ3で説明したプレイブックのアクションの結果を1つの画面で確認できるため、次に何を行うべきかをすばやく判断できます。

この画面から、すべてのイベントアクティビティの履歴、コンテキストに沿ったインタラクティブなデータ表示、添付ファイルのデジタルVault、さらに完全に統合された自動化およびケース管理コントロールにアクセスできます。

Mission Controlに統合されたSplunk SOAR Mission Guidanceは、セキュリティイベントの調査、封じ込め、除去、修復に役立つ推奨事項を提供してセキュリティ運用アナリストを支援するインテリジェントアシスタントです。Mission Controlは、セキュリティイベントデータを、設定済みのSOCツールやプレイブックとマッピングすることで機能します。Splunk SOARミッションガイダンスは、経験の浅いアナリストが適切な手順を学ぶため、そして経験豊富なアナリストが自身の判断を確認するために役立ちます。

Splunk Mission Controlのアクティビティフィードには、現在表示しているイベントに対して実行された現在および過去のすべてのアクションとプレイブックアクティビティが表示されます。このフィードで、イベントに対するすべての自動処理の成否、実行中のアクション、結果をすばやく確認できます。また、自動化の詳細やその他のデータにインラインで組み込まれたチームコラボレーション機能を使用して、すべての関連イベント情報の記録を確認することもできます。





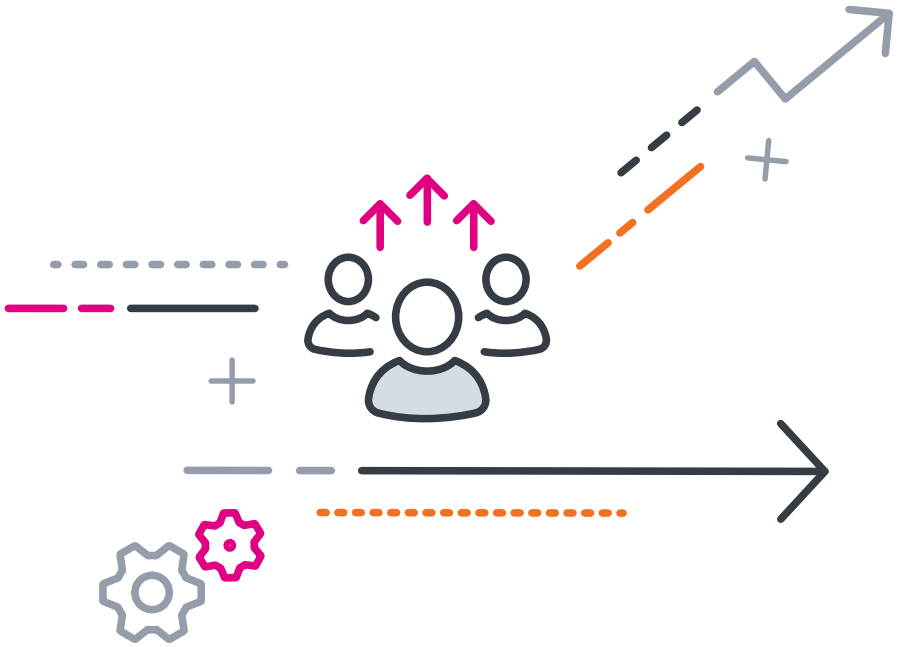
Splunkの実績あるソリューションでAWSアカウントを保護

AWS Security Hubを使用すれば、AWS環境のアラートや脅威の兆候を簡単に集約できます。さらにSplunkやSplunk SOARと統合してシームレスに連携させることで、対応をすばやく実行してセキュリティ体制を強化できます。

Splunkは、AWSから以下のコンピテンシーパートナーとして繰り返し認定されています。

- AWSアドバンスドテクノロジーパートナー
- AWSセキュリティコンピテンシー
- AWSデータと分析コンピテンシー
- AWSクラウド管理ツールコンピテンシー
- AWSコンテナコンピテンシー
- AWS DevOpsコンピテンシー
- AWS教育コンピテンシー
- AWS政府機関コンピテンシー
- AWS IoTコンピテンシー
- AWS MSPテクノロジーコンピテンシー
- AWS Marketplaceパートナー
- AWSセキュリティ自動化とオーケストレーションパートナー
- AWS SaaSプログラムパートナー
- AWS GovCloud (米国)スキルパートナー

今日、世界中の多くの先進企業がAWSアカウントのセキュリティソリューションとしてSplunkを利用しています。



Splunk Enterprise、Splunk Cloud、またSplunk SOARの
無料体験版をぜひダウンロードしてください。

21-14106-Splunk-Stay afloat using AWS Security Hub-JA-202109