Enterprise Security
セキュリティの最新化

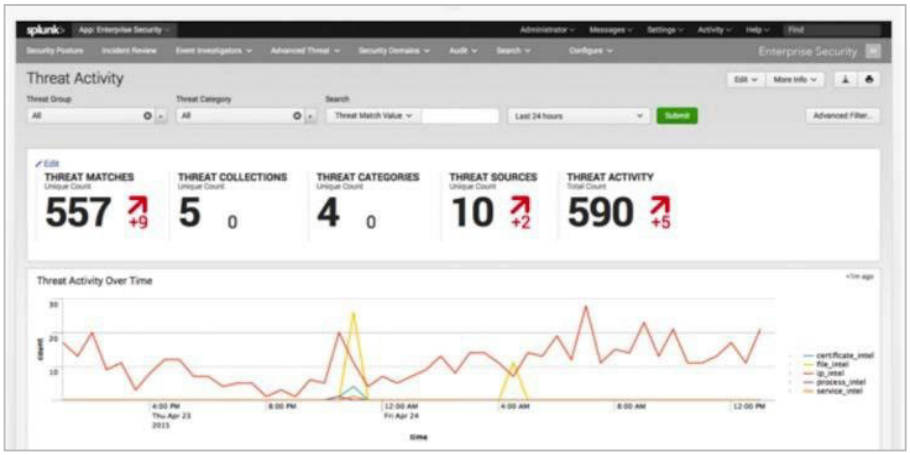
お客様自身のデータを使って
Splunkのセキュリティ分析を評価する

splunk>
turn data into doing™

目次

分析主導型セキュリティが必要である理由

複雑な課題に先手を打つには、適切なデータ戦略が主導する、より適切な認識と意思決定に基づいたセキュリティへの新しいアプローチが必要です。



Splunkでは、多くの組織から次のような声をよく耳にします。

- **サイバーセキュリティが役員レベルの懸念事項になっており**、SIEMプラットフォームが時代遅れであるかそもそも導入されていないため、役員の要求に対応できず**不安に感じている**。
- 新たな脅威の爆発的な増加に対応できず、不当な理由で**ヘッドラインニュースになることを恐れている**。
- **セキュリティ成熟曲線の初期段階にあり**、SOC (セキュリティオペレーションセンター)に十分なスタッフが揃っていない状態で、現在と将来のニーズにすばやく対応できる基本フレームワークを探している。
- リモートワークの拡大によりクラウドの利用や外部エンドポイントからの接続が増えたことで、サイバー攻撃の対象となる範囲が拡大し、**可視化できない部分が生じている**。さらに、攻撃対象が拡大し、分析すべきデータが増えたことで、SOCに大量のアラートが押し寄せ、トリアージの負担が増大している。
- クラウドやBYODを使用すると、データへのアクセス制御やセキュリティ態勢の維持が複雑で困難になることを知り**悩んでいる**。また、侵害が発生したことに最後まで気付かないという事態を避けたいと考えている。
- SOCスタッフを後手の対応から解放し、**先手の対策に集中させたい**。
- 観測結果や指標を補足するために複数のインテリジェンスソースからデータを取得しているが、**その調査を手動で行っているため時間がかかりすぎる**。

多くの組織が、**利用可能なデータのわずか20%以下に基づいて、セキュリティに関する意思決定を下す**ことを余儀なくされています。80%にも上るデータが可視化されていないために**盲点**が生じ、インシデントの調査が遅れている可能性があります。さらに追い打ちをかけるように、**インシデントが発生し手遅れになるまで**、その部分のデータにアクセスすることすらできません。その場でリアルタイムに適応して対応するのではなく、すでに起こったことに対応しているのです。

サイバーセキュリティが懸念される場合は、ガートナー社のSIEMに関するマジッククアドラントおよびクリティカルケイパビリティレポートでリーダーと評価された、Splunkのソートリーダーシップと業界トップクラスのソリューションをご利用いただけます。

セキュリティソリューションとしてのSplunk

Splunkは、社内外の攻撃を迅速に検出して対応するための機能をご提供します。

リスクを最小限に抑え、ビジネスを保護しながら、脅威の管理をシンプルにします。**Splunk**はセキュリティ運用のあらゆる側面を合理化しています。また、あらゆる規模と専門分野の組織に適しています。

継続的なリアルタイム監視、迅速なインシデント対応、効率の高いSOC、あるいは優先順位付けされたビジネスリスクの可視化を必要とする経営幹部の要求に応えることなど、導入の目的が何であれ、Splunk Enterprise Securityは、相関サーチ、アラート、レポート、ダッシュボードを特定のニーズに合わせてカスタマイズするといった柔軟性を提供し、セキュリティ運用を強化します。

Splunkの分析主導型SIEMのメリット

- **可視性**:組織全体から収集したセキュリティデータとそれ以外のデータを使用して、インシデント対応と調査を強化します。
- **コンテキスト**:複数のソースから脅威インテリジェンスを収集して集約し、重複排除と優先順位付けを実行して、セキュリティ調査を強化します。
- **効率**:個別サーチ、および静的、動的、視覚的な関連付けを使用して迅速な調査を実行し、悪意ある活動を特定することで、セキュリティ運用を合理化します。
- **適応力と拡張性**:リスクベースアラート(RBA)のアプローチにより、大量アラートの問題を解消し、後手の対応から先手の対策にシフトするとともに、サイバーセキュリティ運用やコンプライアンスのユースケースに対応します。
- **整合性**:監視、検出、対応、脅威ハンティングのアクティビティを、定評あるサイバーセキュリティフレームワークのいずれかと整合させます。

Splunkのリスクベースアラート(RBA)

大量アラートの問題を解消

毎日膨大な量のアラートが発生し、SOCがそのトリアージ、調査、修正で手いっぱいになっている。このような経験をしている組織は少なくありません。最近の調査では、**41%の組織が1日1万件以上のアラートを受信**していることが明らかになりました。驚くべき数字です。そこから生じる問題をさらに複雑化させているのが、かなりの数のアラートが誤検知であるという事実です。別の調査では、**40%以上の組織**が、**セキュリティアラートの半数以上が誤検知**であったと回答しました。

SOCは大量のアラートに疲弊しており、その多くが誤検知であるという現実は、SOCに明確な悪影響を与えています。まず、多くのアラートが未調査のままとなります。アナリストには、受信したすべてのアラートを確認できるほどの時間がないのです。そのため、ごく一部のアラート、おそらく重要度「最高」と「高」と思われるもののみを処理することになります。これでは、多くの未調査アラートの中の1つが環境内で起きている侵害を実際に示していたとしても、それを見逃す可能性があります。

環境内でアラートが大量に発生する場合、その処理や誤検知の問題の影響を直接受けるのがSOCのアナリストです。アナリストは日々、処理しきれないほどのアラートを次々に受け取り、調査しなければなりません。また、誤検知の対処に何時間も費やし、本当の脅威の修復に手が回らなくなっています。その結果、有能なアナリストたちが疲弊してしまいます。セキュリティの仕事をしているのではなく、仕事を少しでも効率的に行うためにツールやサーチの調整に明け暮れているように感じられるためです。

Splunk Enterprise Securityのリスクベースアラートがもたらす解決策

大まかに言うと、リスクベースアラートではまず関連するデータを収集します。これを「アトリビューション」と呼びます。そして、これをEnterprise Securityのリスクインデックスに送ります。注目すべき点は、このアトリビューションからアラートを直接生成しているのではなく、ただリスクインデックスにアトリビューションを送信していることです。

MITRE ATT&CKなどのサイバーセキュリティフレームワークとの整合

前述のアトリビューションの生成時に、関連するコンテキストを付加して拡充することができます。たとえば、リスクスコアを付加したり、資産やアイデンティティのコンテキストを保存したり、MITRE ATT&CKの該当する戦術やキルチェーンの段階に応じて注釈を付けたり、任意の注釈を入れたりすることができます。このプロセスを経ることで、リスクインデックスには高リスクな挙動が大量に蓄積され、マイニングが可能になります。厳密には、リスクインデックスに送る個々の観測結果は単独では脅威を示しているとは言えないかもしれません。しかし、以上のような高リスクのアトリビューションと注釈からなるコンテキスト内に置くことで、脅威が見つかることがあります。

Enterprise Securityでは、リスクインデックスに送信したアトリビューションに適用したさまざまな「レンズ」に基づいて、新しいタイプのリスクベースアラートを生成できます。レンズは、リスクインデックスに送ったアトリビューションに適用する分析タイプを指します。よく使われるレンズの1つが「リスクスコア」です。24時間以内にユーザーやシステムのリスクスコアが100を超えた場合にアラートを生成するのが一般的です。

また、リスクインデックスに送ったデータに対してサイバーセキュリティフレームワークのレンズを適用することもできます。そうすることで、任意のフレームワークに沿ってアラートを生成できます。たとえば、MITRE ATT&CK戦術の注釈を作成している場合は、「過去14日間に3つ以上のMITRE ATT&CK戦術に該当するアクティビティがあったリスクオブジェクトに対してアラートを生成する」というルールを作成できます。このアプローチにより、サイバーセキュリティフレームワークのメリットを検出に組み込み、有益なコンセプトをSOC運用の中心に据えることができます。

Enterprise Securityでは、リスクベースアラートの使用が推奨されており、**デフォルトでは有効になっています**。ただし、選択するユースケースによっては、関連付けられた相関ルールで「重要なイベント」を有効にする必要があります。リスクベースアラートのメリットをさらに活かすには、このアプローチをお勧めします。

SplunkのSecurity POVプログラム

Splunkでは、Splunkのセキュリティ分野の専門家が業界トップクラスのソリューションとソートリーダーシップを活用して**無料のProof of Valueプログラム**を提供しています。このプログラムでは、**お客様自身のデータを取り込んでSplunkがもたらす価値を確認していただき、組織が対処するべき最も重要なセキュリティユースケースをお客様にご説明します。評価プロセスを円滑にするため、対象とするユースケースは3つまでに限定させていただきます。**

Splunkによってどのように盲点をなくし、より効率的に脅威を調査し、リアルタイムで行動してそれらの脅威を阻止できるかを示すために、Splunkは、Splunkのセキュリティソリューションを利用してお客様のデータを活用するための環境と、セキュリティに関する専門知識をご提供します。Splunkのエキスパートがお客様のデータソースを取り込み、セキュリティに関するSplunkのベストプラクティスを提供し、最も重要なセキュリティユースケースをお客様にご説明します。Splunkのリスクベースアラート(RBA)を使用したセキュリティアプローチをお試しになり、検出、監視、調査プロセスにもたらすメリットをぜひ体感してください。作成可能なダッシュボード、レポート、サーチを確認していただいたら、最大30日間は引き続き無料でその環境を利用して評価し、価値を得ることができます。

Security POVプログラムでは、**Splunk Intelligence Management**を利用して社内外の脅威インテリジェンスデータをEnterprise Security内で直接活用していただくこともできます。Splunk Intelligence Managementでは、インテリジェンスソースのキュレーションと正規化が自動で行われ、それに基づいてEnterprise Securityの重要なイベントがエンリッチおよび優先順位付けされるため、調査を迅速化できます。Splunk Intelligence Managementを追加できるユースケースは、ネットワークトラフィックとリモートアクセス、リスクが高い可能性のあるエンティティとの通信、不審なエンドポイントアクティビティ、コマンドアンドコントロールの4つです。

Splunkは**18,000社を超えるお客様**にご利用いただいており、お客様が直面している課題と同様の課題に数多く対応しています。これらのお客様の成功事例をお読みいただくには、
https://www.splunk.com/ja_jp/customers.htmlにアクセスしてください。

POV後のSplunkの利用

POVの期間終了後も引き続きSplunkを利用する場合は、POVの期間中に作成したすべてのサーチ、ダッシュボード、およびその他の分析をそのまま活用して、価値実現までの時間を短縮できます。Splunkチームは、このPOV環境を本番環境へと移行するための提案を行います。Splunkを導入するかどうかの意思決定を行う前にPOV環境を評価する時間がさらに必要な場合は、月額料金で環境の利用を延長できます。

成功の可能性を高めるには...

このドキュメントは、達成する必要がある成功イベントを文書化するために使用します。これらの成功イベントはほとんどのProof of Valueに必要であり、お客様への最終成果物として各成功イベントの達成を記入します。

以下のセクションに入力して、アカウントチームに送信してください。

お客様自身のデータを使用してSplunkの効果を確認していただけるよう、お客様が希望する成果と、お客様のデータを取り込む簡単なプロセスを確認するための電話会議を設定いたします。

主な連絡先

お客様側の担当者とSplunkアカウントチームの主な連絡先：

POVテクニカルリード：	
エンドユーザー/評価者1：	
エンドユーザー/評価者2：	
エンドユーザー/評価者3：	

評価者の方はそれぞれ、splunk.comアカウントに登録し、無料のSplunk Fundamentals 1 Eラーニングを受講していただく必要があります。

Splunk Intelligence Managementをご利用の場合は、Intelligence Managementアカウント管理者にするエンドユーザーに注記を入れてください。

ここに記載した以外の評価者が参加する場合は、最後のページのメモセクションに追加してください。

コア機能の要件

SplunkのProof of Valueで特定の機能を評価したいとお考えのお客様もいらっしゃるかもしれません。Splunkが機能のデモンストレーションを行ううえで製品のどの領域に重点を置くべきかを把握するために、お客様およびお客様の組織がこのProof of Valueにおいて特に興味がある領域にチェックマークを入れてください。

Splunkのコア機能	
興味のある機能にチェックマークを付け、最も優先順位の高いものから1、2、3というように、**選択した機能に順位を付けてください**(3つまで選択してください)。	
___ コア機能(収集/インデックス作成/サーチなど) ___ アラート ___ レポート作成 ___ 調査 ___ アーカイブ ___ 脅威インテリジェンス	___ イベント調査と対応 ___ ログ管理 ___ ネットワーク監視 ___ ユーザーエクスペリエンス ___ リスクベースアラート(RBA)

セキュリティユースケースの要件

Splunkでは、Proof of Valueの期間中に実証できるユースケースのサンプルリストを用意しています。また、SplunkのProof of Valueで特定の機能を評価したいとお考えのお客様もいらっしゃるかもしれません。お客様およびお客様の組織がこのProof of Valueにおいて特に興味がある領域にチェックマークを入れてください。

Proof of Valueのユースケース	
興味のあるユースケースにチェックマークを付け、最も優先順位の高いものから1、2、3というように、**選択したユースケースに順位を付けてください**(3つまで選択してください)。	
☐ ユーザーアカウントの監視	☐ 不審なクラウドアクティビティ
☐ 異常な認証アクティビティ	☐ 不審なエンドポイントアクティビティ*
☐ ネットワークトラフィックとリモートアクセス*	☐ コマンドアンドコントロール*
☐ リスクが高い可能性のあるエンティティとの通信*	☐ 重大度が緊急または高レベルの脆弱性の検出
☐ 通常とは異なる地域からのクラウドプロビジョニングアクティビティ	
☐ 通常とは異なるユーザーによるクラウドインスタンス作成	

*この4つのいずれかを選択した場合は、POVにSplunk Intelligence Management (TruSTAR)を含めるかどうかを選択してください。

☐ Intelligence ManagementをPOVに含める(以下の項目をご記入ください)

- 「主な連絡先」で、脅威インテリジェンスアカウント管理者にするエンドユーザーに注記を入れてください。
- いずれかのISAC/ISAOのメンバーの場合は参加団体をご記入ください。

_____

- すでに登録しているインテリジェンスプロバイダーやフィードがある場合は、登録先をご記入ください。(それらのインテリジェンスをSplunkに取り込む際はAPIキーが必要です)

_____

☐ Intelligence ManagementをPOVに含めない

メモと情報

このPOVを成功させるために必要となる、その他の関連情報をご記入ください。

用語集

Splunkのコア機能	技術面の成功基準
コア機能	• プラットフォームは、ブール値/完全に一致するフレーズ/正規表現またはSPLによる高速サーチを実行できる必要がある。 • アラート通知を実行する。 • POVの指定デバイスからログを正常に収集する。 • アラート/レポート/サーチを簡単にカスタマイズできる。
アラート	• 相関エンジンが、複数のイベントを連続して関連付けできる。 • 相関エンジンが、発生していないアクティビティを検出できる。 • 相関エンジンが、複数のデバイスタイプにまたがるアクティビティを検出できる。
レポート作成	• 規制への準拠を示すレポートを作成する。 • レポートの作成を自動化、カスタマイズ、スケジュール設定する。
調査	• トレーニングや追跡に使用できるよう、重要なイベントを1つの調査にグループ化できる。
アーカイブ	• アーカイブされたログデータを、デジタルCoC用にハッシュ化する。
脅威インテリジェンス	• デフォルトの脅威リストを使用して脅威データに対するアラートを生成する。 • 正規化した脅威インテリジェンスを使用して重要なイベントを分析する。 • インテリジェンスを活用して脅威のコンテキストを把握し、優先順位付けしてトリアージを迅速化する。
イベント調査と対応	• デフォルトパラメータ内でログの生データに簡単にアクセスできる。 • イベントアクティビティに対して自動化されたレスポンス(アダプティブレスポンス)を実行する。 • イベントデータに対して指定されているリスクとその重要度を提供する。
ログ管理	• POVログソースを簡単かつ迅速に収集して正規化する。 • プラットフォームが、複数のデータストレージ階層にわたってデータのインデックス作成、アーカイブ、削除を迅速かつ簡単に行える。
ネットワーク監視	• ポートやアプリケーションの不正使用を検出できる。 • ネットワーク分析をSIEMソリューションとシームレスに統合できる。 • 許可されていないストリーミングやアプリケーションの使用を検出できる。 • クラウドまたはファイル共有サイトへの大量のファイル転送を検出できる。

ユーザーエクスペリエンス	• プラットフォームは、Enterprise Securityのダッシュボードを介してインタラクティブなドリルダウンサーチを実行できる必要がある。Enterprise Securityインターフェイスは、標準的な最新のWebブラウザを使用して、すべてのデバイスからアクセスできる必要がある。 • プラットフォームは、収集されたライブログデータのストリームの表示、ピボット、サーチを実行できる必要がある。
リスクベースアラート(RBA)	• 過剰なアラートを削減し、異常な挙動を精度の高いアラートに集約して真陽性率を向上させる。 • 挙動に関する属性に注目することで調査プロセスを迅速化する。

ユースケース

以下の各セキュリティユースケースに示す対象範囲とログソースは、規制/コンプライアンス要件への適合、監視、検出、調査、追跡などに必要なデータソースを判断するために役立ちます。また、相関ルールはあらかじめ用意されたもので、MITRE ATT&CKの(サブ)技法と関連付けられています。この技法情報に、関連するATT&CK戦術、脅威グループ、説明などのコンテキストが補足されて、その後の処理に使用されます。

Autobahn POVでは、以下の中から**最大3つのユースケース**をお選びいただけます。

1. ユーザーアカウントの監視

このユースケースでは、システム、ネットワーク、サービス、アプリケーション、クラウド、その他のITリソースでのユーザーの行動に関する知見を取得できます。ユーザーアカウントの監視を行うことで、故意であるかどうかにかかわらず社内外で発生する脅威を防ぐことができます。また、可用性を確保しながら情報を保護し、データプライバシーやセキュリティに関する規制に準拠することもできます。

名前	ユーザーアカウントの監視
対象範囲	サーバー、ワークステーション、クラウド
ログソース	Windowsイベントログ、認証システム、AD、Linux Syslog、AWS/Azure/GCP

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:永続化、認証情報アクセス、防衛回避、権限昇格、初期アクセス、ラテラルムーブメント **技法**:ドメインアカウント、ブルートフォース、有効なアカウント、クラウドアカウント、リモートサービス、追加のクラウド認証情報、アカウントの作成、リモートサービスの悪用、ローカルアカウント
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。	**RR - 新規 - 特権グループへのユーザーの追加 - 複合** **RR - ES - 感染マシンへの高または緊急レベルのユーザーログイン - 複合** **RR - ESCU - 基本的なブルートフォースの検出 - システム** **RR - ESCU - Oktaでのアカウントロックアウトイベント - 複合** **RR - ESCU - OktaでのSSO試行の失敗 - 複合** **RR - ESCU - Oktaでの同一IPからの無効な認証情報による複数のユーザーログイン - 複合** **RR - 新規 - システムからの高レベルのVPNログイン失敗 - 複合** **RR - ESCU - 新規ユーザーによるAWSコンソールログインの検出 - 複合** **RR - SSE - 複数の不正なアクセス試行の検出 - 複合** **RR - SSE - ユーザーがログインするホスト数の増加 - ユーザー** **RR - SSE - サービスアカウントからの新規インタラクティブログオン - 複合** **RR - Azureでの追加のクラウド認証情報へのアクセス - ユーザー** **RR - Azureでの管理者グループへのユーザー追加 - ユーザー** **RR - ESCU - クラウドインフラでの異常な回数のAPI呼び出し - ユーザー** **RR - ESCU - 通常とは異なるユーザーによるAWSインスタンスの作成 - ユーザー** **RR - 新規 - AWSでの新規ユーザーの追加 - 複合** **RR - アカウントの作成 - 複合** **RR - ESCU - 匿名アカウントによるコンピューター変更の検出 - システム** **RR - SSE - ローカル管理者アカウントの追加 - 複合**
確認用ダッシュボード	アクセスセンター、IDセンター、アカウント管理、エンドポイント変更、およびID調査ダッシュボードでの表示

2. 異常な認証アクティビティ

攻撃者は組織内を簡単に移動できるように認証情報を悪用します。そのため、組織内でアクセスリクエストや認証リクエストが発生したときに、その要求に異常がないかどうかを検証することは非常に重要です。異常な認証リクエストを検出するには、リクエストが不正である可能性の高いシナリオを洗い出します。これによってそれぞれに適切な対策を講じることができます。また、異常な動作だけではなく正常な動作も確認して、正規の認証アクティビティを把握しておくことも大切です。

名前	異常な認証アクティビティ
対象範囲	サーバー、ワークステーション、クラウド
ログソース	Windowsイベントログ、AD、Linux Syslog、Okta、AWS/Azure/GCP

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:認証情報アクセス、防衛回避、永続化、権限昇格、初期アクセス、ラテラルムーブメント **技法**:ブルートフォース、ドメインアカウント、有効なアカウント、クラウドアカウント、リモートサービス
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。	**RR - ES - 感染マシンへの高または緊急レベルのユーザーログイン - 複合** **RR - ESCU - 基本的なブルートフォースの検出 - システム** **RR - ESCU - Oktaでのアカウントロックアウトイベント - 複合** **RR - ESCU - OktaでのSSO試行の失敗 - 複合** **RR - ESCU - Oktaでの同一IPからの無効な認証情報による複数のユーザーログイン - 複合** **RR - 新規 - システムからの高レベルのVPNログイン失敗 - 複合** **RR - ESCU - 新規ユーザーによるAWSコンソールログインの検出 - 複合** **RR - SSE - 複数の不正なアクセス試行の検出 - 複合** **RR - SSE - ユーザーがログインするホスト数の増加 - ユーザー** **RR - SSE - サービスアカウントからの新規インタラクティブログオン - 複合**
確認用ダッシュボード	アクセス異常、アクセスセンター、アクセストラッカー、アクセスサーチ、アカウント管理、およびデフォルトアカウントアクティビティダッシュボードでの表示

3. ネットワークトラフィックとリモートアクセス

ITリソース間の通信の多くはネットワークインフラ(VPN、ルーター、スイッチ、ファイアウォール、IDS/IPSデバイスなど)を必ず通過するため、ネットワークドメインでは脅威や攻撃に関する重要なインサイトを取得できます。Splunkでは、ネットワーク全体のアクティビティをダッシュボードで確認して、通信の傾向やトラフィック量の変化を把握し、これらの変化の要因を調査できます。具体的には、暗号化されたPOSデバイスがランサムウェアによって攻撃される直前にファイアウォールがコマンドアンドコントロールの送信を許可したかどうか、またはマルウェアの感染が広がった後に大量の接続が試行されたかどうかなど、特定のファイアウォールアクションとこれらのアクションに関連する時間範囲を表示することで調査に役立てることができます。また、ネットワークトラフィックとリモートアクセスに関するアラートから生成された重要なイベントに、Splunk Intelligence Managementでキュレーションされた脅威インテリジェンスを付加して、イベント情報を補足することもできます。

名前	ネットワークトラフィックとリモートアクセス
対象範囲	サーバー、ワークステーション、ネットワーク
ログソース	Webプロキシ、ファイアウォール、DNS、VPN
脅威インテリジェンス	既知の不正なTorトラフィック、未許可のサイト、悪質なIPトラフィックのアラート生成に使用できる、OSINTと商用インテリジェンスのフィード

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**：認証情報アクセス、持ち出し、永続化、初期アクセス、コマンドアンドコントロール、探索、ラテラルムーブメント **技法**：C2チャネルを介したデータ持ち出し、代替プロトコルを介したデータ持ち出し、外部リモートサービス、セキュリティ保護されていない認証情報、アプリケーション層プロトコル、ネットワークサービススキャン、リモートデスクトッププロトコル、DNS、ドライブバイ攻撃、Webサービス、ファイル転送プロトコル、アプリケーション以外の層のプロトコル
相関ルール： デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。Splunk Intelligence Management (TruSTAR)の相関サーチでは、取り込まれたインテリジェンスデータとログソースが照合されて、重要なイベントが生成されます。	**RR - ESCU - プレーンテキストでの認証を通すプロトコル - 複合** **RR - 新規 - ホストからの高レベルのファイアウォールブロック - システム** **RR - 新規 - 海外からのVPNアクティビティ - 複合** **RR - 新規 - 新規IPからのVPN接続 - 複合** **RR - SSE - 急な離職リスクを示すWebブラウズ - ユーザー** **RR - SSE - 大容量のWebアップロード - 複合** **RR - ESCU - Torトラフィック - システム** **RR - リモートデスクトッププロトコル - 複合** **RR - SSE - ネットワークスキャンの検出 - システム** **RR - ES - 大量のDNS失敗 - システム** **RR - ES - 大量のDNSクエリー - システム** **RR - ESCU - 大量の送信ICMPパケットの検出 - システム** **RR - ESCU - 送信SMBトラフィックの検出 - システム** **RR - ESCU - ダイナミックDNSサービスに接続するホスト - システム** **RR - SSE - 未許可のサイトへのWebブラウズ - 複合** **相関サーチ=「脅威アクティビティ検出」**
確認用ダッシュボード	トラフィックセンター、トラフィックサーチ、Webセンター、Webサーチ、ポートとプロトコルトラッカー、HTTPカテゴリ分析、HTTPユーザーエージェント分析、新規ドメイン分析、およびURLの長さ分析ダッシュボードでの表示
脅威インテリジェンス	**検出**：Splunk KVストアにインジケーターを取り込んでアラート生成 **トリアージ**：インテリジェンスソースからの正規化したインジケータースコアとコンテキストに基づいて重要なイベントをトリアージ エンリッチメント：インテリジェンスソースからのインジケーター概要とコンテキストを付加してアラートとケース調査を補足

4. リスクが高い可能性のあるエンティティとの通信

高度な脅威の多くでは、特定の手法、インフラ、プロセスが使用されます。これらのプロセスには、脅威や攻撃に使用されるインフラとの通信が含まれます。Enterprise Security内の脅威インテリジェンスフレームワークでは、不審なアクティビティ、既知の脅威、潜在的な脅威の痕跡をイベントデータと相関付けることができます。潜在的なIoC (侵害の痕跡)に関する脅威インテリジェンスを管理することで、調査ワークフローにコンテキストを追加して検出能力を向上させ、プロアクティブにセキュリティ監視を行うことができます。Splunkには、複数の脅威インテリジェンスフィードに対応したインテグレーションがあらかじめ組み込まれ、デフォルトで有効になっています。このユースケースでは、潜在的なIoCを自動的に収集、管理し、イベントデータと相関付ける方法を探ることができます。Splunkでは、リスクが高い可能性のあるエンティティとの通信に関するアラートから生成された重要なイベントに、Splunk Intelligence Managementでキュレーションされた脅威インテリジェンスを追加して、イベント情報を補足することもできます。

名前	リスクが高い可能性のあるエンティティとの通信
対象範囲	サーバー、ワークステーション、クラウド、ネットワーク
ログソース	Webプロキシ、ファイアウォール、DNS、VPN、GCP、Azure、AWS
脅威インテリジェンス	Tor、Torrent、ダークフォーラムサイト、既知の悪質なエンティティに関連付けられたIPを監視するためのソースを示すインテリジェンスソース

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:コマンドアンドコントロール **技法**:アプリケーション層プロトコル、マルチホッププロトコル
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。Splunk Intelligence Management (TruSTAR)の相関サーチでは、取り込まれたインテリジェンスデータとログソースが照合されて、重要なイベントが生成されます。	RR - ESCU - Torトラフィック - システム RR - 宛先での外部プロキシ脅威インテリジェンスとの一致 - システム RR - 送信元での外部プロキシ脅威インテリジェンスとの一致 - システム RR - 宛先でのTorアクティビティ脅威インテリジェンスとの一致 - システム RR - 送信元でのTorアクティビティ脅威インテリジェンスとの一致 - システム 相関サーチ=「脅威アクティビティ検出」
確認用ダッシュボード	脅威アクティビティおよび脅威アーティファクトダッシュボードでの表示
脅威インテリジェンス	**検出**:Splunk KVストアにインジケーターを取り込んでアラート生成 **トリアージ**:インテリジェンスソースからの正規化したインジケータースコアとコンテキストに基づいて重要なイベントをトリアージ **エンリッチメント**:インテリジェンスソースからのインジケーター概要とコンテキストを付加してアラートとケース調査を補足

5. 通常とは異なる地域からのクラウドプロビジョニングアクティビティ

このユースケースでは、未知のIPアドレスから行われるクラウドプロビジョニングを検出して、クラウド環境への侵害のリスクを軽減します。前提として、アクセスを許可するIPアドレスについて厳格なポリシーを適用している必要があります。正規のユーザーが出張先からアクセスしたり、新しいオーケストレーションツールを使用したりする場合を除いて、この問題が検出されたときは、認証情報が不正に作成されたか乗っ取られて、攻撃者が悪用できる状態にあることを示します。この場合、データの流出、データの消去、コスト増大につながる可能性があります。

名前	通常とは異なる地域からのクラウドプロビジョニングアクティビティ
対象範囲	クラウド
ログソース	監査証跡、GCP、Azure、AWS

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:防御回避、永続化、権限昇格、初期アクセス **技法**:クラウドアカウント
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。	RR - ESCU - 通常とは異なる都市からのAWSクラウドプロビジョニング - 複合 RR - ESCU - 通常とは異なる国からのAWSクラウドプロビジョニング - 複合 RR - ESCU - 通常とは異なる地域からのAWSクラウドプロビジョニング - 複合
確認用ダッシュボード	ソースログ、アセット調査、およびID調査ダッシュボードでの表示

6. 通常とは異なるユーザーによるクラウドインスタンス作成

このユースケースでは、未知のユーザーによって行われるクラウドプロビジョニングを検出して、クラウド環境への侵害のリスクを軽減します。前提として、アクセスを許可するIPアドレスについて厳格なポリシーを適用している必要があります。正規のユーザーのロールが変わったり、新しいオーケストレーションツールを使用したりする場合を除いて、この問題が検出されたときは、認証情報が不正に作成されたか乗っ取られて攻撃者が悪用できる状態にあり、ラテラルムーブメントの可能性を示します。この場合、コスト増大などの問題につながる可能性があります。

名前	通常とは異なるユーザーによるクラウドインスタンス作成
対象範囲	クラウド
ログソース	監査証跡、GCP、Azure、AWS

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:防御回避 **技法**:クラウドアカウント
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。 特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。	**RR - ESCU - 通常とは異なるユーザーによるAWSインスタンスの作成 - ユーザー**
確認用ダッシュボード	ソースログ、アセット調査、およびID調査ダッシュボードでの表示

7. 不審なクラウドアクティビティ

オンライン化が進むにつれて、クラウドセキュリティのユースケースの重要性が高まっています。それと同時に、クラウドベースインフラを標的とする攻撃も増えています。パブリッククラウド環境が拡大すれば、攻撃者にとって魅力的な攻撃対象が増えます。攻撃者は、セキュリティの脆弱なクラウド接続経路を攻撃して内部に侵入し、ワークロードやデータにアクセスして損害を与えます。一方でクラウドユーザーのロール設定は緩くなりがちで、必要以上に高い権限を与えてしまうことも少なくありません。Splunkでは、オンプレミス、リモートワーク、クラウドという違いを超えて環境全体をシームレスに可視化できます。

名前	不審なクラウドアクティビティ
対象範囲	クラウド
ログソース	監査証跡、GCP、Azure、AWS

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:防御回避、永続化、権限昇格、初期アクセス、収集、影響 **技法**:クラウドアカウント、クラウドストレージオブジェクトからのデータ、リソースハイジャック、追加のクラウド認証情報、未使用/未サポートのクラウドリージョン
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。 特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。	RR - ESCU - AWSでの異常な数のインスタンス起動 - ユーザー RR - ESCU - 新規の公開GCPストレージバケットの検出 - 複合 RR - ESCU - 新規の公開S3バケットの検出 - ユーザー RR - ESCU - 新規IPからのS3アクセスの検出 - 複合 RR - ESCU - S3バケットの削除急増の検出 - ユーザー RR - New - AWSでの新規セキュリティグループの追加 - 複合 RR - New - AWS GuardDutyのアラート - 複合 RR - New - AWSでのキーペアの作成/削除/インポート - 複合 RR - New - AWSでの全員へのSSHの公開 - 複合 RR - SSE - AWSでの不審なコンテナイメージ名 - 複合 RR - ESCU - 新規ユーザーによるAWSコンソールログインの検出 - 複合 RR - Azureでの追加のクラウド認証情報へのアクセス - ユーザー RR - Azureでの管理者グループへのユーザー追加 - ユーザー RR - ESCU - クラウドインフラでの異常な回数のAPI呼び出し - ユーザー RR - ESCU - 通常とは異なるユーザーによるAWSインスタンスの作成 - ユーザー RR - 新規 - AWSでの新規ユーザーの追加 - 複合 RR - ESCU - 通常とは異なる都市からのAWSクラウドプロビジョニング - 複合 RR - ESCU - 通常とは異なる国からのAWSクラウドプロビジョニング - 複合 RR - ESCU - 通常とは異なる地域からのAWSクラウドプロビジョニング - 複合
確認用ダッシュボード	ソースログ、アセット調査、およびID調査ダッシュボードでの表示

8. 不審なエンドポイントアクティビティ

リモートワークの普及により、エンドポイントの可視化がかつてないほど重要になっています。未承認のアプリケーション/拡張機能のインストールなど、ユーザーの不用意な行動が発生しがちなエンドポイントは、攻撃者にとって格好の標的です。今日ではエンドポイントの可視化、検出、対応ソリューションが数多く提供されています。これらを使用すれば、ユーザーの行動やシステムの挙動を詳細に把握できます。Splunkでは、可視化されたエンドポイントのデータをオンプレミスやクラウドのアクティビティとシームレスに統合して分析できます。また、不審なエンドポイントアクティビティに関するアラートから生成された重要なイベントに、Splunk Intelligence Managementでキュレーションされた脅威インテリジェンスを付加して、イベント情報を補足することもできます。

名前	不審なエンドポイントアクティビティ
対象範囲	サーバー、ワークステーション
ログソース	Windowsイベントログ、AD、Office 365、Microsoft Defender、Linux Syslog、Sysmon、DNS、Okta、AWS/Azure/GCP
脅威インテリジェンス	マルウェアや既知のブラウザ脆弱性に関するインテリジェンスソース

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:収集、認証情報アクセス、探索、防御回避、ラテラルムーブメント、永続化、権限昇格、初期アクセス、実行、影響、コマンドアンドコントロール **技法**:アクセシビリティ機能、アカウント検出、システム情報検出、ユーティリティによるアーカイブ、ブラウザブックマーク検出、ユーザーアカウント制御のバイパス、デフォルトのファイル関連付けの変更、Windowsイベントログの消去、クリップボードデータ、CMSTP、コマンド/スクリプトインタープリター、コントロールパネル、レジストリ内の認証情報、ファイルまたは情報の難読化解除/デコード、クラウドファイアウォールの無効化/変更、ツールの無効化/変更、権限昇格の悪用、隠しファイル/ディレクトリ、システム回避の阻害、ローカルデータのステージング、LSASSメモリー、悪質なファイル、なりすましタスク/サービス、なりすまし行為、正規の名前または場所の照合、MSBuild、mshta、netshヘルパーDLL、ネットワーク共有検出、ネットワークスニッフィング、難読化されたファイルまたは情報、Pass the Hash、Pass the Ticket、権限グループ検索、PowerShell、レジストリRunキー/Startupフォルダー、Regsvr32、リモートメール収集、スケジュールタスク/ジョブ、セキュリティアカウントマネージャー、セキュリティソフトウェア検出、スピアフィッシングリンク、Kerberosチケットの窃盗/偽造、システム情報検出、システムネットワーク接続検出、システムオーナー/ユーザー検出、システムサービス検出、ユーザー実行、有効なアカウント、Windowsファイルとディレクトリの権限変更、Windows Remote Management、Winlogonヘルパーdll、ブルートフォース、リモートサービス、アカウント作成、ローカルアカウント、リモートサービスの悪用、DNS、ネットワークサービススキャン、リモートデスクトッププロトコル

相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。Splunk Intelligence Management (TruSTAR)の相関サーチでは、取り込まれたインテリジェンスデータとログソースが照合されて、重要なイベントが生成されます。	RR - システムでのユーザーアカウント制御のバイパスの検出 - 複合 RR - Regsvr32プロセスでのアプリケーションホワイトリストのバイパス - 複合 RR - WTDによる認証情報窃盗ツールの検出 - 複合 RR - データのステージングプロセス - 複合 RR - システム回復に関するファイル削除の検出 - 複合 RR - MSHTAの検出 - 複合 RR - Windows Defenderの起動の無効化 - 複合 RR - ESCU - デフォルトPowerShell実行ポリシーの設定の試行 - システム RR - ESCU - reg exeによるレジストリからの認証情報ダンピングの試行 - 複合 RR - ESCU - すべてのポートがオープンのAWSネットワークACLの作成 - ユーザー RR - ESCU - spoolsv.exeの子プロセス - 複合 RR - ESCU - comsvcs DLLによるLSASSからの認証情報ダンピング - 複合 RR - ESCU - LSASSアクセスによる認証情報ダンピングの検出 - システム RR - ESCU - エンドポイントからの過剰なアカウントロックアウトの検出 - 複合 RR - ESCU - リモートユーザーアカウント制御レジストリの無効化 - 複合 RR - ESCU - RC4で暗号化したSPNリクエストのKerberoasting - システム RR - ESCU - reg exeによるレジストリキーを介したファイルまたはディレクトリの非表示 - 複合 RR - ESCU - レジストリキーによる永続化 - システム RR - ESCU - レジストリキーによる権限昇格 - システム RR - ESCU - sc.exeによるWindowsサービスの操作 - 複合 RR - ESCU - エンドポイントの1文字のプロセス - 複合 RR - ESCU - プロセスを起動する不審なLNKファイル - システム RR - ESCU - 不審なwevtutilの使用 - 複合 RR - ESCU - 予期しない場所からのシステムプロセスの実行 - 複合 RR - ESCU - 異常に長いコマンドライン - 複合 RR - ESCU - Windowsイベントログの消去 - システム RR - Office 365でのSendAsまたはFullAccess権限の付与 - ユーザー RR - WTDによるマルウェア検出 - 複合 RR - なりすまし - バイナリの名前変更 - 複合 RR - MpCmdRun.exeの不正使用 - システム RR - ネットワーク共有検出 - 複合 RR - レジストリRunキーまたはStartupフォルダー - システム RR - スケジュールタスク - 複合 RR - スケジュールタスクのスクリプト実行への変更 - 複合 RR - cmd.exeへの固定キーの設定 - 複合 RR - SSE - ファイル名ごとの攻撃/検出ツールの集中的な実行 - システム RR - SSE - ホストのRunAs - 複合 RR - WTDによる不審なアクティビティまたは既知のフレームワークの検出 - 複合 RR - WTDによる不審なCLIコマンドの検出 - 複合 RR - WTDによる不審な情報収集関連CLIコマンドの検出 - 複合 RR - WTDによる不審なサービスまたはレジストリ変更の検出 - 複合 RR - システムネットワーク接続検出 - 複合 RR - TH - クリップボードデータへのアクセス - 複合 RR - TH - アカウント検出 - 複合 RR - TH - ブラウザブックマーク検出 - 複合 RR - TH - CMSTP - 複合 RR - TH - コントロールパネル項目 - 複合 RR - TH - レジストリ内の認証情報 - 複合 RR - TH - ファイルまたは情報の難読化解除/デコード - 複合 RR - TH - セキュリティツールの無効化 - サービス停止 - 複合 RR - SSE - 複数の不正なアクセス試行の検出 - 複合

	RR - SSE - ユーザーがログインするホスト数の増加 - ユーザー RR - SSE - サービスアカウントからの新規インタラクティブログオン - 複合 RR - WTDによるマルウェア検出 - 複合 RR - なりすまし - バイナリの名前変更 - 複合 RR - MpCmdRun.exeの不正使用 - システム RR - ネットワーク共有検出 - 複合 RR - レジストリRunキーまたはStartupフォルダー - システム RR - スケジュールタスク - 複合 RR - スケジュールタスクのスクリプト実行への変更 - 複合 RR - cmd.exeへの固定キーの設定 - 複合 RR - SSE - ファイル名ごとの攻撃/検出ツールの集中的な実行 - システム RR - SSE - ホストのRunAs - 複合 RR - WTDによる不審なアクティビティまたは既知のフレームワークの検出 - 複合 RR - WTDによる不審なCLIコマンドの検出 - 複合 RR - WTDによる不審な情報収集関連CLIコマンドの検出 - 複合 RR - WTDによる不審なサービスまたはレジストリ変更の検出 - 複合 RR - システムネットワーク接続検出 - 複合 RR - TH - クリップボードデータへのアクセス - 複合 RR - TH - アカウント検出 - 複合 RR - TH - ブラウザブックマーク検出 - 複合 RR - TH - CMSTP - 複合 RR - TH - コントロールパネル項目 - 複合 RR - TH - レジストリ内の認証情報 - 複合 RR - TH - ファイルまたは情報の難読化解除/デコード - 複合 RR - TH - セキュリティツールの無効化 - サービス停止 - 複合 RR - SSE - 複数の不正なアクセス試行の検出 - 複合 RR - SSE - ユーザーがログインするホスト数の増加 - ユーザー RR - SSE - サービスアカウントからの新規インタラクティブログオン - 複合 相関サーチ=「脅威アクティビティ検出」
確認用ダッシュボード	アクセスセンター、IDセンター、アカウント管理、エンドポイント変更、DNSアクティビティ、およびID調査ダッシュボードでの表示
脅威インテリジェンス	**検出**：Splunk KVストアにインジケーターを取り込んでアラート生成 **トリアージ**：インテリジェンスソースからの正規化したインジケータースコアとコンテキストに基づいて重要なイベントをトリアージ **エンリッチメント**：インテリジェンスソースからのインジケーター概要とコンテキストを付加してアラートとケース調査を補足

9. コマンドアンドコントロール

高度な脅威の多くでは、特定の手法、インフラ、プロセスが使用されます。これらのプロセスには、脅威や攻撃に使用されるインフラとの「コマンドアンドコントロール」チャネルの確立が含まれます。これにより攻撃者は、リモートから被害組織のリソースにアクセスして操作し、目的を達成するために必要な行動を起こすことができます。Splunkを使用することで、セキュリティチームは、外部の宛先への特定のトラフィックフローおよびユーザーレベルのアクティビティが、「コマンドアンドコントロール」の試行または確立を示しているかどうかを検出して検証できます。これには、「ビーコン」パターン、既知の不正なドメイン宛ての異常な量のトラフィック、および関連するアクティビティの範囲の証拠(脅威が侵入した方法、足掛かりを築いた場所、関連するラテラルムーブメントなど)の検出も含まれます。また、コマンドアンドコントロールに関するアラートから生成された重要なイベントに、Splunk Intelligence Managementでキュレーションされた脅威インテリジェンスを付加して、イベント情報を補足することもできます。

名前	コマンドアンドコントロール
対象範囲	サーバー、ワークステーション、ネットワーク、クラウド
ログソース	Linux Syslog、Sysmon、DNS、Okta、AWS/Azure/GCP、Webプロキシ、ファイアウォール、DNS、VPN
脅威インテリジェンス	既知の不正なドメイン、IP、Torインテリジェンス、プロキシ脅威インテリジェンス、マルウェア対応、既知の脆弱性を特定するインテリジェンスソース

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:コマンドアンドコントロール、防御回避、権限昇格 **技法**:DNS、アプリケーション層プロトコル、DNS、ドライブバイ攻撃、C2チャネルを介したデータ持ち出し、代替プロトコルを介したデータ持ち出し、Webサービス、ファイル転送プロトコル、アプリケーション以外の層のプロトコル、DNS、ダイナミックDNS、動的リンクライブラリインジェクション
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。Splunk Intelligence Management (TruSTAR)の相関サーチでは、取り込まれたインテリジェンスデータとログソースが照合されて、重要なイベントが生成されます。	RR - ESCU - 長いDNS TXTレコード応答の検出 - システム RR - ESCU - DNSトンネル - システム RR - ESCU - Torトラフィック - システム RR - ES - 大量のDNS失敗 - システム RR - ES - 大量のDNSクエリー - システム RR - ESCU - 大量の送信ICMPパケットの検出 - システム RR - ESCU - 送信SMBトラフィックの検出 - システム RR - ESCU - ダイナミックDNSサービスに接続するホスト - システム RR - SSE - 未許可のサイトへのWebブラウズ - 複合 RR - 宛先での外部プロキシ脅威インテリジェンスとの一致 - システム RR - 送信元での外部プロキシ脅威インテリジェンスとの一致 - システム RR - 宛先でのTorアクティビティ脅威インテリジェンスとの一致 - システム RR - 送信元でのTorアクティビティ脅威インテリジェンスとの一致 - システム RR - WTDによるコマンドアンドコントロールアクティビティの検出 - 複合 RR - 新規 - Punycodeドメイン - 複合 RR - WTDによる不審なプロセスまたはDLLの検出 - 複合 相関サーチ=「脅威アクティビティ検出」
確認用ダッシュボード	脅威アクティビティ、脅威アーティファクト、DNSアクティビティダッシュボードでの表示
脅威インテリジェンス	**検出**:Splunk KVストアにインジケーターを取り込んでアラート生成 **トリアージ**:インテリジェンスソースからの正規化したインジケータースコアとコンテキストに基づいて重要なイベントをトリアージ **エンリッチメント**:インテリジェンスソースからのインジケーター概要とコンテキストを付加してアラートとケース調査を補足

10. 重大度が緊急または高レベルの脆弱性の検出

このユースケースは、「リスクが高い可能性のあるエンティティとの通信」の拡張版で、新たな脅威に関するIoCまたは既存の脆弱性スキャンデータに基づいて、より多くの高度な脅威を検出します。高度な脅威の多くでは、特定の手法、インフラ、プロセスが使用されます。これらのプロセスには、脅威や攻撃に使用されるインフラとの通信が含まれます。Enterprise Security内の脅威インテリジェンスフレームワークでは、不審なアクティビティ、既知の脅威、潜在的な脅威の痕跡をイベントデータと相関付けることができます。潜在的なIoC (侵害の痕跡)に関する脅威インテリジェンスを管理することで、調査ワークフローにコンテキストを追加して検出能力を向上させ、プロアクティブにセキュリティ監視を行うことができます。Splunkには、複数の脅威インテリジェンスフィードに対応したインテグレーションがあらかじめ組み込まれ、デフォルトで有効になっています。このユースケースでは、ローカライズした脅威インテリジェンスデータを管理し、既知の脆弱性のあるシステムの調査コンテキストを収集する方法を探ることができます。さらに、リスク要因フレームワークを使用して、アセット、アイデンティティ、脆弱性スキャンのコンテキストを取得し、他の検出メカニズムで行動や挙動のアトリビューションをリスクインデックス/データモデルに書き込み、そのメカニズムに関連付けられたリスクスコアを評価する方法を探ることもできます。

名前	重大度が緊急または高レベルの脆弱性の検出
対象範囲	サーバー、ワークステーション、クラウド、ネットワーク
ログソース	Webプロキシ、ファイアウォール、DNS、VPN、GCP、Azure、AWS

プロセス	
MITRE ATT&CK 戦術と技法	**戦術**:コマンドアンドコントロール **技法**:アプリケーション層プロトコル、マルチホッププロトコル
相関ルール: デフォルトのアクションでは、結果をESのリスクフレームワークに書き込みます。特定のルールについて、従来のように重要なイベントを生成する必要がある場合はそのように設定することもできます。	RR - ESCU - ランサムウェア脆弱性 - システム RR - ESCU - SpectreおよびMeltdown脆弱性 - システム RR - 新規 - 重大度が緊急または高レベルの脆弱性の検出 - システム
確認用ダッシュボード	脅威アクティビティおよび脅威アーティファクトダッシュボードでの表示