データシート

今こそEclecticIQとSplunkで飛躍するチャンス

EclecticIQプラットフォーム向けSplunk AppでCTIアナリストをSplunkチームのヒーローに

Splunk Appの特長

統合の自動化

EclecticIQプラットフォームには、Splunk EnterpriseおよびSplunk Phantomとのビルトイン統合が含まれています。

脅威への対応の優先順位付け

Splunk EnterpriseはEclecticIQのサイバー脅威データを分析、フィルタリングして、組織にとって最も関連の高い脅威を特定します。

即座に対策を実施

Splunk Appは、ダッシュボードゲージのデフォルトセットと共に出荷されます。Splunkユーザーはこのダッシュボードを使って、脅威の分析、データ分析から得られたセキュリティ侵害インジケーター(IOC)の選別を進めることができます。

チームのメリット

CTIへのメリット

CTIチームはSplunkから重要な検知を自動的に受け取って、進行中の脅威分析の優先順位付けを強化、支援します。

SOC/インシデント対応へのメリット

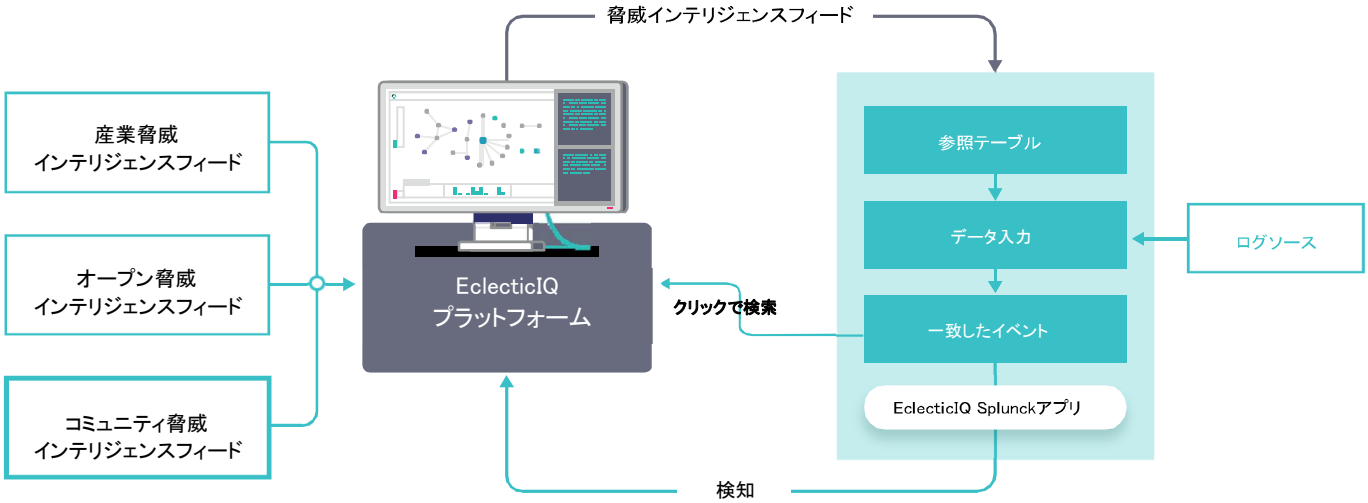
SOC/IRチームは、EclecticIQプラットフォームから背景情報を得て、より効果的で効率的なSplunkアラート分析を推進します。

セキュリティリーダーへのメリット

CTIとSOCの運用を緊密に統合して、調査にかかる時間を大幅に短縮することで、診断までの平均時間(MTTD)と対応までの平均時間(MTTR)を短くします。

EclecticIQプラットフォームとSplunkの統合

関連フィード(半減期、関連性、TLP、機密度、悪性度、タグ付け)



データシート

EclecticIQとSplunkのユースケース

SOCの拡張

課題

Ponemon Instituteによると、組織の半数以上が、自社SOCのエビデンスの収集、脅威源の調査と発見の能力が不十分だと考えています。1

SOCが脅威を的確に特定し、優先順位を付け、対応するには、正しいデータをタイミングよく適切なコンテキストで得る必要があります。SOCが、最大のリスクをもたらす脅威を先見的に特定するには、CTIを集約して優先順位を付ける必要があります。

ソリューション

EclecticIQプラットフォームはSplunkとのビルトイン統合を搭載して、SOCによるSIEMとしてのSplunkの利用を強化します。

Splunk Appは以下の作業を促進します。

- ソース、エンティティ、観察可能な挙動をきめ細かく制御
- コンテンツ、タグ、悪性度、減衰度、TLPなどに基づき、統合されたインテリジェンスをフィルタリング
- 複数のセキュリティコントロールとワークフローシステムの統合
- 特定のインテグレーションに対する共有種別のフィルタリングと上書きのTLP管理

成果

EclecticIQのアラートとテレメトリの強化機能により、SOCアナリストは重要な作業に集中できます。

- 脅威インテリジェンスの強化で誤検知を認定および削減
  EclecticIQはコンテキストを失わずにすべてのデータを転送
- フィールドの匿名化でデータの機密性を保護し、GDPRに準拠
- アナリストは、きわめて非常に迅速な分析と対応を実現するパワフルなグラフ可視化ツールと検索ツールでインシデントのコンテキストを容易に確認

EclecticIQ SOC拡張機能で重要な処理に集中

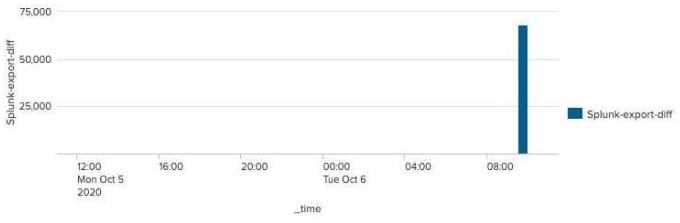
Total Count of Observables in Splunk

68099

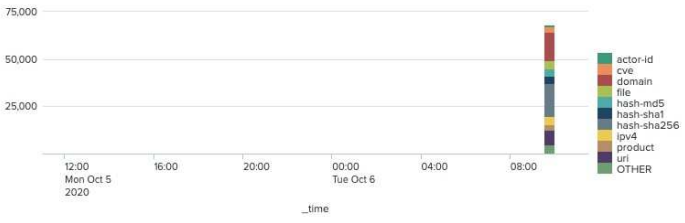
Observables Distribution

Feed ID	Feed Name	Update Strategy	Count
7	Splunk-export-diff	DIFF	68099

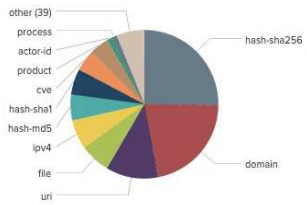
Downloaded Observables by time



Downloaded Observables by Time and Type

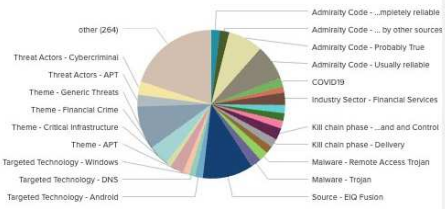


Count of Observables by Type



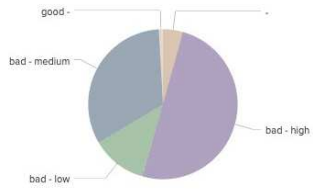
Observable type	Count
hash-sha256	17154
domain	14857
uri	7796
file	4473
ipv4	4400
hash-md5	3838

Count of Observables by Tag/Taxonomy



Tag/Taxonomy	count
Source - EIQ Fusion	33268
Theme - Generic Threats	28763
Admiralty Code - Usually reliable	23157
Admiralty Code - Probably True	22868
Theme - Financial Crime	13705

Count of Observables by Classification/Confidence



Classification	Confidence	count
bad	high	29035
bad	medium	19267
good		9102
bad	low	7796
		2899

データシート

EclecticIQとSplunkのユースケース

SOAR統合

課題

アラート選別、インシデント対応（IR）、IOCハンティング、脆弱性管理（VM）、インテリジェンス共有など、CTIは複数のSOARユースケースを強化できます。
ただし、これらのユースケースを適切に実装するには、重要なCTIプラクティスをSOCチームワークフローに変換する必要があります。これらのプラクティスには、セキュリティコントロールの拡大、ウォッチリストの自動更新、検知の利用などがあります。

ソリューション

EclecticIQプラットフォーム向けSplunk Phantom AppはSplunk Phantomにシームレスに統合します。CTIアナリストはこの統合を通じて、EclecticIQプラットフォームから直接Phantomの戦術をトリガーできます。
また、Splunkから双方向的に検知が届くため、CTIのアクションが強化されます。

このシームレスな統合は、インテリジェンス主導型セキュリティの核となります。Splunk Phantom Appは以下の作業を促進します。

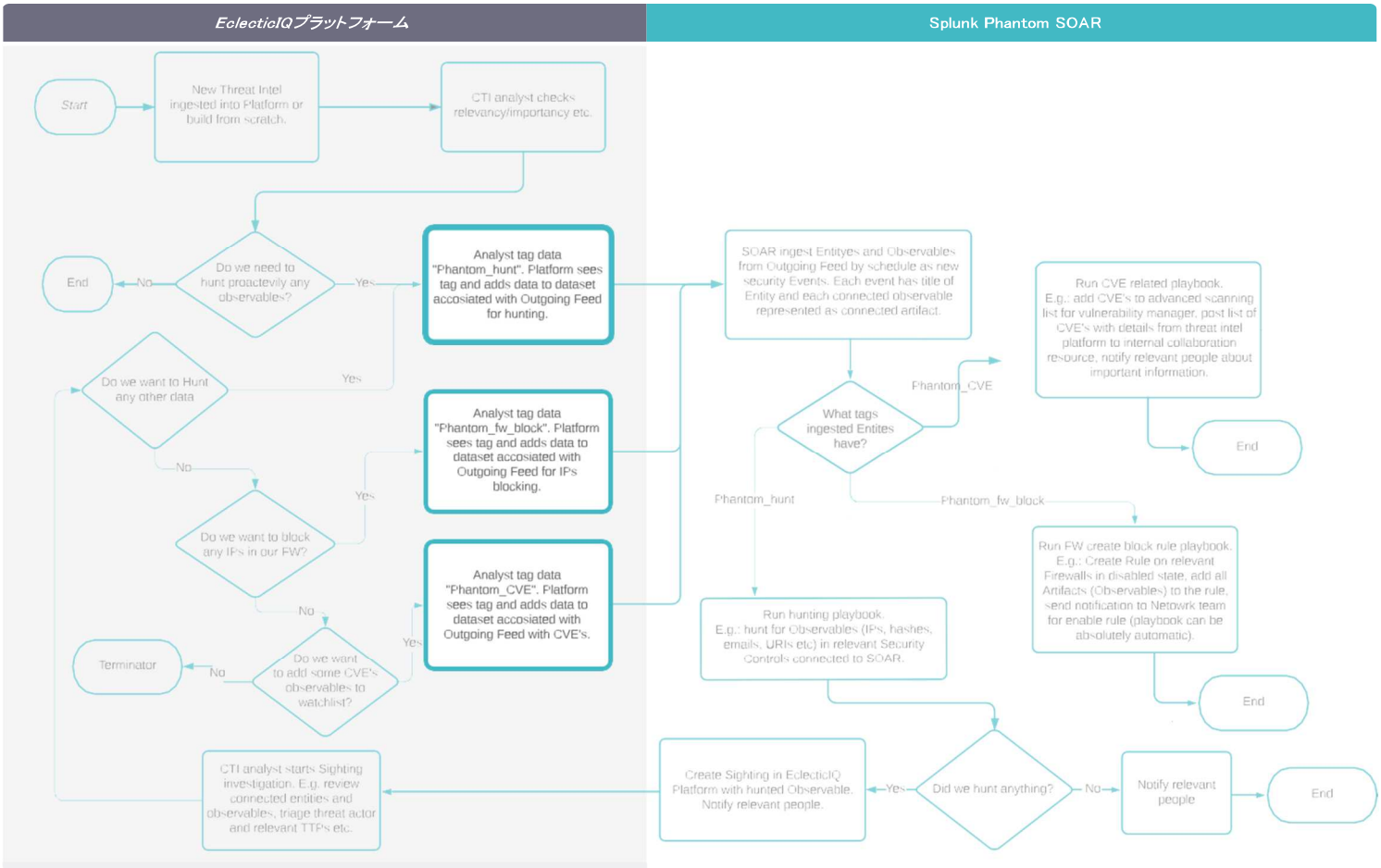
- 脅威インテリジェンスとデータを先見的にハンティング
- セキュリティコントロールの統合を自動化：IPのブロック（FW）、ハッシュのブラックリスト追加（EDR）
- CVEの観察可能な挙動をウォッチリストに追加

成果

Splunk PhantomをEclecticIQプラットフォームに統合することで、診断までの平均時間（MTTD）、対応までの平均時間（MTTR）を短縮し、インシデントを修正します。メリットは次のとおりです。

- EclecticIQが提供する高信頼の脅威インテリジェンスで戦術の効果が上がり、調査が迅速化
- インジケーターのエンリッチメントを自動化することで、誤検知を軽減
- 高信頼の脅威情報を既存のIOCと脆弱性に自動的に相関付けることで、パワフルな脅威ハンティングを実現
- 脅威インテリジェンスチームがPhantom自動化機能で、サイバーセキュリティコントロールを安全に調整
- 調査をトリガーして、検知から、脅威アクターおよび関連するTTPの選別まで実行

EclecticIQとSplunk Phantomで戦術の効果を改善



データシート

EclecticIQについて

EclecticIQは公式なSplunk Technology Alliance Partnerです。弊社は、行政機関と一般企業を対象に、インテリジェンスで強化したサイバーセキュリティを実現します。お客様のサイバーセキュリティの焦点を脅威の現実に合わせる、アナリストを中心に考えた製品とサービスを開発しています。これにより、インテリジェンス主導型セキュリティ、検知と予防の向上、コスト効率に優れたセキュリティ投資が実現します。

Splunk Appの詳細：
https://splunkbase.splunk.com/app/4176/

デモ版については以下にお問い合わせください。
info@eclecticiq.com
+31 (0) 20 737 1063

[1] Ponemon Institue, LLC：『Improving the Effectiveness of the Security Operations Center』2019年6月9日

EclecticIQ
INTELLIGENCE POWERED DEFENSE