HITACHI
Inspire the Next

Splunkを利用したSIEMソリューションのご紹介

Splunk Enterprise/Cloud×
Splunk Enterprise Security（ES）の
組み合わせでより効果的なSIEMソリューションを実現

内部不正など、お客様業務や運用を加味した高度な分析が必要となる脅威の検知

splunk>enterprise

・Splunk Enterpriseによるデータ取り込み、SPL（＊）による検知ルールやダッシュボード作成によりインシデントの可視化や攻撃対策が可能

・SPLの作成は容易かつ直観的に行えるだけでなく、数式を活用し、条件文ではできない高度な分析も可能

```
Index="index_name"
| stats count by host…
```

（＊）SPL（Splunk社独自のサーチ言語）

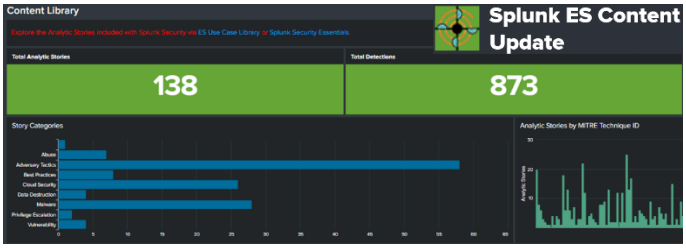
＋ 定型的な外部攻撃検知

Splunk Enterprise Security

・攻撃、外部脅威に対して豊富な検知ルールやダッシュボードを持つSplunkESを導入することで対策

No	相関サーチ例		
1	アカウントの削除	7	クリアテキストパスワードの検出
2	異常な監査証跡の検出	8	ログインの試み
3	新たなポートの検出	9	デフォルトアカウントの検出
4	新たなプロセスの検出	10	停止中のデフォルトIDの検出
5	新たなサービスの検出	11	大量のログイン失敗
6	7日以内のATT&CK閾値超過	12	大量のHTTPエラーレスポンス

・ES Contents Update（ESCU）により最新トレンドを押さえた相関サーチが迅速に配信される



定型的な外部攻撃への対策はSplunk Enterprise Securityに任せ、お客様の業務や運用に考慮が必要な箇所にリソースをかけることが可能

↓

より実用的なSIEMへ
深い分析も可能にしつつ、外部脅威も網羅的にカバー

Splunkは、2022年 Gartner® Magic Quadrant™ for Security Information and Event Management で、9回連続リーダーのうちの１社として評価されました。

出典：Gartner, Magic Quadrant for Security Information and Event Management, Pete Shoard, Andrew Davies, Mitchell Schneider, 10 October 2022
Gartnerは、Gartnerリサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するようにテクノロジーユーザーに助言するものではありません。Gartnerリサーチの発行物は、Gartnerリサーチの見解を表したものであり、事実を表現したものではありません。
Gartnerは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の責任を負うものではありません。

株式会社 日立ソリューションズ

Splunk Enterprise Securityを導入することによって定型的な外部攻撃への対策が容易になる

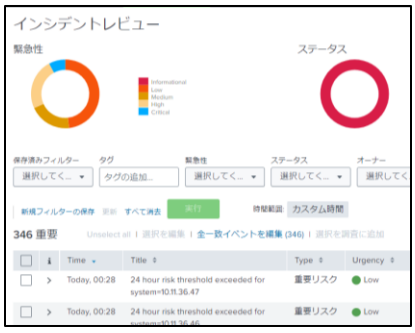
●外部攻撃対策のポイントと実現方法

定型的な外部攻撃対策のポイント	SplunkESにより実現可能
アナリストが迅速に対応できるインターフェースが必要	セキュリティダッシュボード
アラートが大量に検知されるため、対応の優先度を決めることが必要	リスクベースアラート
脆弱性情報の取得、選別、攻撃検知ロジックの構築を短時間で実施することが必要	相関サーチ

● 機能紹介

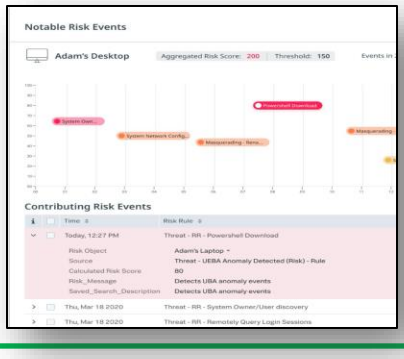
セキュリティダッシュボード

インシデントの詳細が表示され、アナリストが調査分析に利用する50種類以上の豊富なダッシュボード群



リスクベースアラート

リスクスコア付け、リスクにもとづいた高精度アラート生成、過剰なアラートを抑制



相関サーチ

網羅性のある検知ロジックに加え、最新のトレンドを盛り込んだセキュリティアラートを高頻度かつ迅速に提供

No	サマリ	相関ルール名
1	エンドポイントの異常値検出	Abnormally High Num
2	ソース毎の異常なHTTPメソッド	Abnormally High Num
3	アカウントの削除	Account Deleted
4	期限切れIDの活動	Activity from Expired
5	異常な監査証跡の検出	Anomalous Audit Trai
6	新たなポートの検出	Anomalous New Liste
7	新たなプロセスの検出	Anomalous New Proce
8	新たなサービスの検出	Anomalous New Servi
9	特定されないアセットオーナー	Asset Ownership Unsi
10	ブルートフォースの検出	Brute Force Access Be
11	1日以上のブルートフォース	Brute Force Access Be
12	クリアテキストパスワードの検出	Cleartext Password At
13	無効アカウントの検出	Completely Inactive A
14	ログインの試み	Concurrent Login Atte
15	デフォルトアカウントの検出	Default Account Activi

SplunkESを使用したSIEMの実現について日立ソリューションズにお任せください。
インストール・検知ルールのご相談および実装・チューニングなど、OneStopでご対応します。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/splunk/