

# Splunk 運用支援のご紹介

## Splunkの導入後のよくある悩み、課題を解決

- 新たな脅威の情報に合わせて、分析ルールを作らないといけないが、**最新の脅威情報がわからない**  
→支援メニュー①へ



- 今取得しているログでセキュリティに十分か**漠然としており不安**  
→支援メニュー①へ



- ログを追加したいが、取得方式を**設計する自信が無い**  
→支援メニュー②へ



- 現状の分析ルール、ダッシュボードを変更したいが、**時間が取れない**  
→支援メニュー②へ



- 導入したSplunkの調子が悪くパフォーマンスが出ない  
**何を調査すればいいかわからない**  
→支援メニュー③へ



- インシデントが発生した際に、**自分たちだけで対応できるか不安**  
→支援メニュー④へ



日立ソリューションズのエキスパートが  
お客様に最適な支援を提供

### 支援メニュー①

### 最新セキュリティ動向の提供

- 2ヵ月に1回、1時間程度の定例会をリモートで実施
- 日立ソリューションズセキュリティエキスパートが、**最新のセキュリティ動向とそれに対応する分析ルールをご提案**
- 分析ルールを実現するために必要なログがあれば、**どのようなログが必要かをご提案**



### セキュリティ動向報告例

#### 1. 2022/6時点のセキュリティ動向

HITACHI  
Inspire the Next

| #1   | タイトル                                                                                                | マルウェアEmotetの感染再拡大 |
|------|-----------------------------------------------------------------------------------------------------|-------------------|
| 詳細   | 2022年2月の第一週よりEmotetの感染が急激に拡大している                                                                    |                   |
| 攻撃手法 | マクロ付きのExcel Wordファイル、あるいはこれらをバインド付きZIPファイルとしてメールに添付する形式で感染<br>ファイルを開発後にマクロを有効化する操作を実行することでEmotetに感染 |                   |

© Hitachi Solutions, Ltd. 2022. All rights reserved. 40

#### #1 マルウェアEmotetの感染再拡大の対策

HITACHI  
Inspire the Next

| (1)     | 分析ルール名                                                               | HeaderFrom:EnvelopeFromが異なるメールサーバーの通信ログ |
|---------|----------------------------------------------------------------------|-----------------------------------------|
| 必要となるログ | HeaderFrom:EnvelopeFromが異なるメールサーバーに送信されているメールの送信元アドレスを抽出             |                                         |
| 分析手法    | 送信元アドレスの抽出                                                           |                                         |
| (2)     | 分析ルール名                                                               | 通常より多いメール送信                             |
| 必要となるログ | メールサーバーの通信ログ                                                         |                                         |
| 分析手法    | 外部宛の送信メール量が通常より大幅に増えているかを検知<br>送信元アドレス別に集計<br>先送との相違を、異常の閾値を超えたものを抽出 |                                         |
| (3)     | 分析ルール名                                                               | 大量のPortへのアクセス                           |
| 必要となるログ | Proxyログ                                                              |                                         |
| 分析手法    | 外部IPに多数Portアクセスしていないか検知<br>送信元アドレス別に集計<br>異常のPortで接続したものを抽出          |                                         |

© Hitachi Solutions, Ltd. 2022. All rights reserved. 41

#### 取得すべきログの方針

HITACHI  
Inspire the Next

今後、以下のログを取得することを推奨します。

■ 現状の課題  
メールを使っているインターネットのデータの取り扱いは管理出来ているが、Web通信の監視が出来ていないので、その部分のログを取得していきます

■ 今後の方針  
優先度を3つに分け、ログを取得していきます。インターネット系のログを優先度を上げて取得し、クライアントログ、その他のサーバーのログと拡張していきます

| 優先度   | 項目                      |
|-------|-------------------------|
| 優先度 高 | Proxyログ<br>Firewallログ   |
| 優先度 中 | クライアント側ログ<br>ネットワークパケット |
| 優先度 低 | EDRログ<br>ファイルサーバーアクセスログ |

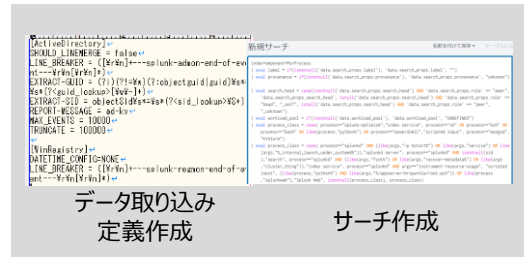
© Hitachi Solutions, Ltd. 2022. All rights reserved. 42

## 支援メニュー②

## オンサイト(リモート)支援

日立ソリューションズのSplunkエキスパートが、お客様先に  
オンサイト、もしくはリモート対応でお客様の実施したいことをヒア  
リングし、**ログの新規取り込み、ダッシュボード、アラートの作成を  
実施**します。

(オンサイト対応は首都圏に限ります。  
月1回の対応で一回あたり8時間を想定しています)

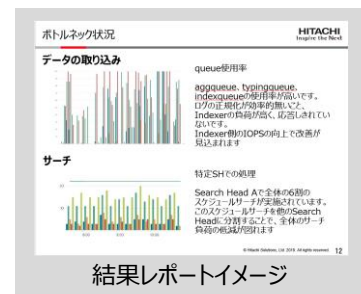


## 支援メニュー③

## 最適化チェック(Optimization Check)

日立ソリューションズのSplunkエキスパートが、オンサイト、もしくは  
リモート対応で、お客様内のSplunk環境に**エラーが発生していないか、  
ボトルネックが発生していないかを確認**します。  
問題が発生している箇所と、その改善方法をレポートにまとめ、  
報告いたします。

(訪問場所は日本国内全域、対応日数は2日間を想定しています)



## 支援メニュー④

## インシデント対応支援

万が一のインシデント発生時に、**対応方針策定や詳細な原因調査などを支援**。  
被害の深刻化を防ぐための適切なインシデント対応支援をセキュリティエキスパートがご提供します。

### 対応方針策定支援

インシデント発生時にセキュリティエキスパートが  
現地に駆け付け、初動対応を支援します。

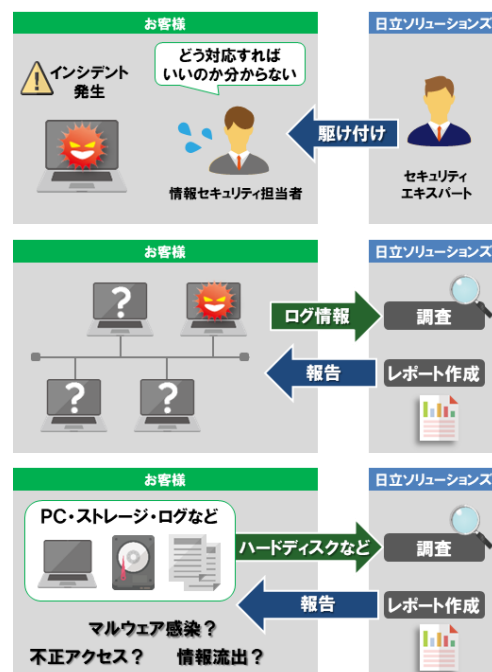
### 侵害調査支援

調査用スクリプトを配布し、そのログ情報をもとにマルウェア感染の原因や被害状況などの  
調査を支援します。

### コンピュータフォレンジック

ハードディスクに残る痕跡を調査し、情報の  
不正流出などインシデントの詳細把握を支援します。

(訪問場所は日本国内全域(島嶼、僻地を除く)で、公共交通機関  
で訪問できる場所になります)



※Splunkは、Splunk Inc.の米国およびその他の国における商標または登録商標です。※本リーフレット中の会社名、商品名は各社の商標、または登録商標です。 ※本文中および図中では、TMマーク、®マークは表記していません。 ※製品の仕様は、改良のため、予告なく変更する場合があります。 ※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取ください。なお、ご不明な場合は、当社担当営業にお問い合わせください。  
※本リーフレット中の情報は、作成時点のものです。