高度脅威分析センターとセキュリティ監視の将来

（p. 24-31に掲載した論文の和訳）

Advanced Threat Centre and Future of Security Monitoring

Paul McEvatt

あらまし

データと人々の生活が密接につながることでデジタル社会が形成され，インターネットを介してやり取りされるデータやトランザクション処理が絶えず増加している。デジタル社会では，現実社会と仮想空間の境界線が曖昧になり，サイバー攻撃による被害が増加している。このような状況の中，全てのビジネスにおいて必要不可欠となるのがサイバー攻撃を検知するセキュリティ監視である。通常，セキュリティ監視はセキュリティオペレーションセンター（SOC）の管理下で行う。しかし，増え続けるサイバー攻撃に対応し，後手に回らないようにするためには，組織全体の継続的なイノベーションが必要である。

本稿では，SOCにおけるインシデント対応を改善するための革新的なアプローチ，あるいは効果的なセキュリティ監視を支える新しいモデルとして，セキュリティの自動化およびオーケストレーションを実現するATC（高度脅威分析センター）による対応について述べる。

Abstract

Electronic data and people's lives are becoming more closely intertwined, leading to the formation of a digital society where the Internet is being used to process an ever-increasing volume of data exchanges and transactions. This trend is blurring the boundary between the real world and virtual spaces, resulting in a greater impact from cyberattacks. A fundamental requirement for all businesses is security monitoring to detect such attacks. Security monitoring is usually performed under the management of a security operations centre (SOC). However, to cope with the continued rise in cyberattacks, organisations as a whole must continue to innovate. This paper describes an innovative approach to improve incident response in SOC or a response by ATC (the Advanced Threat Centre) which realizes security automation and orchestration as a new model to support effective security monitoring.

1. まえがき

サイバーセキュリティを脅かす攻撃が複雑さを増し，拡大し続ける中，企業のセキュリティを強化するセキュリティオペレーションセンター（SOC）は，現代のビジネスが直面するあらゆる攻撃には対応することが難しくなっている。セキュリティ監視は極めて重要であり，効果的なセキュリティ監視ができなければ，企業活動の説明責任を果たす能力が制限される。SOCによるセキュリティ監視が必要となるのは，このためである。

SOCは，セキュリティに対する組織の基本方針を基に，継続的に監視・分析するための情報セキュリティチームを擁する機関と定義されている。[(1)] 従来，SOCはシグネチャマッチング（サイバー攻撃を検知するルールに合致しているか機械的に調べる方法）などの技術や手作業に基づいて，構築・運用されていた。しかし，それではもはや効果的なセキュリティ監視には不十分である。現代のサイバー攻撃に対抗するためには，斬新かつプロアクティブ（予防的）なアプローチが必要である。

本稿では，富士通高度脅威分析センター（ATC：Advanced Threat Centre）の構築と導入の方法について説明する。

2. セキュリティ自動化およびオーケストレーション

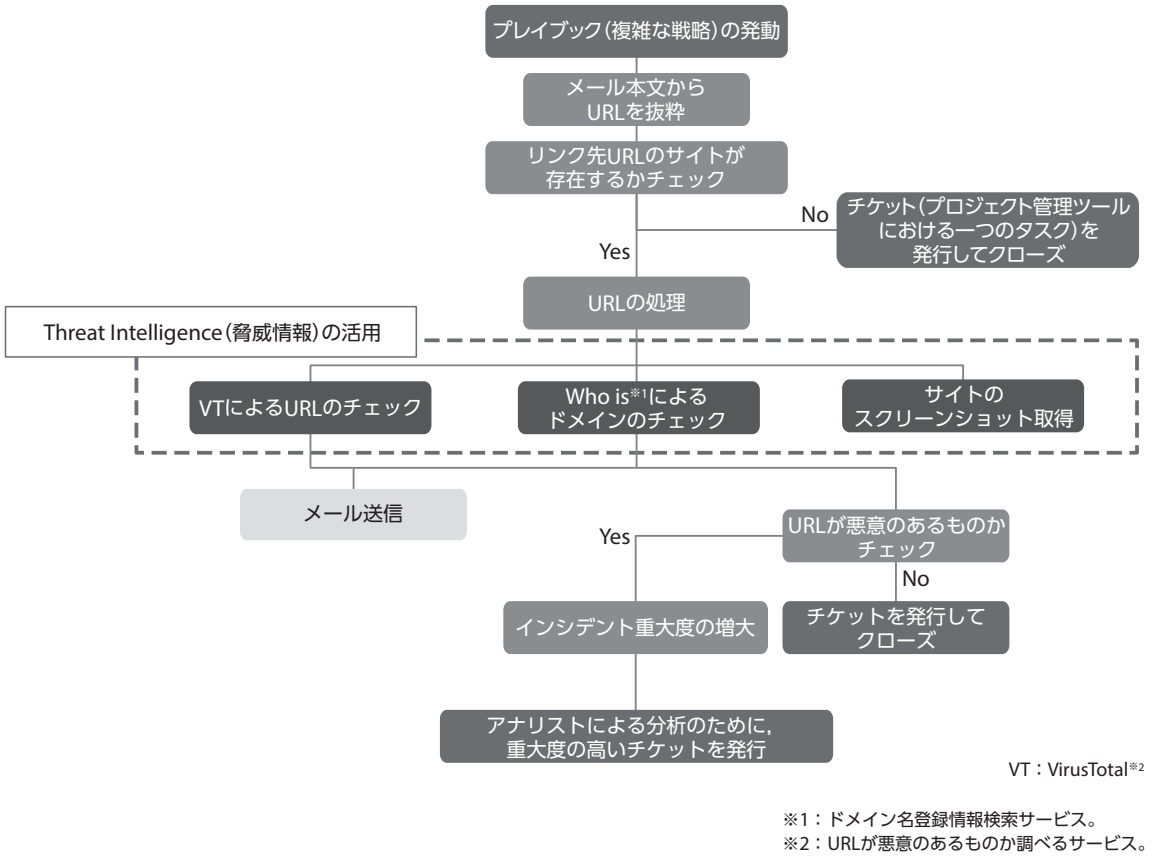
セキュリティの自動化とは，ビジネスプロセスを自動化して，SOCのファーストライン（手順に基づいてオペレーターで処理）およびセカンドライン（アナリストが臨機応変に処理）で処理するインシデント（脅威となり得る事態）と日常的なチェックの数を削減することである。一方，オーケストレーションとは，セキュリティ技術が合理的に協調して機能するようにまとめ上げることである。これによって，SOCのアナリストは豊富な情報を入手でき，攻撃のブロックを自動化できるようになる。

どちらのコンセプトも，組織の環境とセキュリティ技術に合わせた戦略的アプローチを使用する。ここで言う戦略とは，チームの様々な戦略を意味するスポーツ用語に由来する，プレイブックとも呼ばれ，この戦略を採用することで，市場の勝者を目指すことができる。[(2)] 一般的な戦略は，ビジネスプロセスとセキュリティ技術のオーケストレーションによって，組織構成に合わせてカスタマイズできる。フィッシング詐欺警戒のプレイブックを図-1に示す。

2.1 セキュリティ自動化およびオーケストレーションがもたらす効果

セキュリティ自動化およびオーケストレーション（SAO：Security Automation and Orchestration）がもたらす主な効果を以下に示す。

- 反復可能，予測可能なチェックを自動化することで削減できる。
- 毎日のチェックなどの基本的な作業を減らすことで，サイバースキルのギャップを埋めるとともにセキュリティ技術者の士気を向上させ，アナリストに脅威ハンティング（Threat Hunting：侵入した脅威をログ解析や機械学習などを用いて狩る方法）という本来行うべき分析タスクに取り組む余裕を与えることができる。
- 全ての標準的なセキュリティ技術を統合して，プレイブック主導型で標準化されたAPI（Application Programming Interface）インシデント対応アプローチを提供できる。
- MTTR（Mean Time To Recovery：平均修復時間）が短縮されるにつれて，インシデント対応とサービスの質が改善され，顧客のインシデントに対してより効率的に対応できる。
- 状況に応じて脅威情報を自動的に抽出することでインシデント対応を充実させる。これによって，誤検出を削減できる。
- プロキシサーバやファイアーウォールのルールなどによって，ネットワークを遮断して，インシデント対応のオーケストレーションを行う。
- ファーストラインとセカンドラインのアナリストが対応するインシデントの数を減らすことによって，セキュリティ運用部門におけるアラート対応の工数を削減する。
- 富士通が，エンタープライズCSIRT（Computer Security Incident Response Team），EDR（Endpoint Detection and Response），詐欺防



※1：ドメイン名登録情報検索サービス。
※2：URLが悪意のあるものか調べるサービス。

図-1　フィッシング詐欺警戒のプレイブック

止などの高度な分析手法に移行するに伴って，信頼性が高い高度標的型攻撃対策のセキュリティサービスの開発を可能にする。

・MSSP（Managed Security Service Provider）オファリングを通じて，複数のSOCや顧客環境にわたって使用できる基本的な戦略を使用できる。

・機械学習などの新しい技術を活用し，インシデントの割り当て，一括管理，セキュリティダッシュボードなどを用いて脅威の概要を迅速に把握するなどを可能にする。

以降の節において，これらの効果の一部について詳細を述べる。

2.2 機械学習

カーネギーメロン大学における機械学習分野の調査によると，2021年までにサイバーセキュリティにおける同分野への投資が960億ドル（約10兆円）に増加すると予測されている。[3] 侵入検知，ウイルス対策，セキュリティ情報イベント管理（以下，SIEM）などの従来のセキュリティ技術は，ベンダーがスケーラブルなクラウドネットワークを利用して，ソリューションに機械学習を導入することで進化している。

SAOとして市場に投入されている新しい技術でも，機械学習を活用することで，サイバーセキュリティアナリストと同様の理に適った意思決定ができる。これは，富士通ATCのアナリストにとって重要なセキュリティ自動化の推進力にもなる。

2.3 サイバースキルのギャップ

サイバーセキュリティの市場は競争が激しいため，組織は継続的に受ける攻撃だけでなくスタッフ数とレベルの維持にも課題を抱えている。Burning Glass[4] の調査では，サイバーセキュリティ技術者は，従来のICT技術者に比べて一人あたり年間平均6,500ドル多い報酬が必要となる可能性があるとしている。現在，サイバーセキュリティ技術者の需要

と供給には大きなギャップがあり，2019年の時点で150万人の技術者が不足すると報告されている。[5]

SOCでのファーストラインとセカンドラインの監視プロセスを自動化することによって，富士通のセキュリティ技術者は，より興味深い分析や，上級アナリストレベルの作業に取り組めるようになる。また，それに伴ってセキュリティ技術者のモチベーションや士気の向上，セキュリティ技術者の定着などが，非常に競争の激しいサイバーセキュリティの雇用市場において，重要な役割を果たす。

SOCをATCへと変えるために，富士通は成長分野に合わせた新しいサービスを開発し，市場に投入する必要がある。Gartnerは，今後3年間でEDRが高い成長率を見せると予測している。

従来のウイルス対策は今日の企業でも行われているが，今後のセキュリティオペレーション監視では，特定された脅威を理解できるEDRソリューションおよびATCアナリストが必要となる。そこで極めて重要になるのが，このアプローチを支えるのに適したテクノロジーを選択することと，アナリストのスキルを真の脅威ハンティングのレベルまで引き上げることである。

2.4 評価方法としてのMTTRと平均所要時間（MTTD）

マネージドセキュリティサービスについては，サービスレベルアグリーメント（SLA）が依然として正式なKPI（Key Performance Indicator：重要業績評価指標）である。しかし，組織はインシデント対応を評価するための新たな指標を次々に採用していくことになると考えられる。

英国政府は，サイバー攻撃に対応する方法を次のように述べている。「攻撃に効果的に対応できるかどうかは，まず攻撃が発生している，あるいは発生しつつあることを認識できるかどうかにかかっている。攻撃を防ぎ，攻撃による影響や被害を最小限に抑えるには，迅速な対応が不可欠である。」[6]

この目的を達成するために，近年採用されているインシデント対応の評価基準がMTTRである。この指標を用いることで，インシデントへの対応時間が徐々に短縮していることを示すことができる。一方，MTTD（Mean Time To Detect）は，攻撃者が検出されるまでにネットワーク内に潜んでいる日数を表す用語である。FireEyeによる研究では，全世界のMTTDが，2016年の99日から2017年には101日に延びている。[7]

このような状況下で，定められた時間内にインシデントに手動で対応することは，もはや効果的とは言えない。これに対して，SAOを基盤とする高度標的型攻撃の対策エコシステムに移行することで，富士通はファーストラインとセカンドラインの作業を自動化し，アナリストはほかの作業に集中できる。

SAOを使用して脅威情報のインシデントの事例を充実させることによって，インシデントへの迅速かつ多様な対応が可能になる利点を図-2に示す。今日のSOCでは，複数の情報源をまたがって脅威の存在を示す痕跡（IOC：Indicator of Compromise）を手作業で相互参照することがアナリストに求められており，余分な時間がかかっていた。これを自動的に行い，リスクスコアに基づいて潜在的な脅威を事前に遮断することが，顧客にとって大きなメリットとなる。

2.5 アナリストの考え方の変化

SOCからATCへの転換は，セキュリティ監視へのアプローチにおける根本的な変化であり，アナリストは考え方を大きく変える必要がある。ウイルス対策を例に取ると，従来のセキュリティ技術ではSOCアナリストに対して，シグネチャが一致する特定のマルウェアに関する警告を行っていた。ATCへと転換することで，マルウェアが悪質な迷惑メールの大量発信によって生じたものであるかどうかを簡単に判断でき，パソコンやサーバの検疫と駆除によって簡単にインシデントに対応し，解決できる。

AI（人工知能）や機械学習のアルゴリズムなどを使用する新しいセキュリティ技術を実装すると，異常なトラフィックだけを識別できる。パソコンやサーバの不審な動作がその例であり，通常と異なる時間のログオンやスクリプトの実行などが考えられる。事後対応のアプローチの場合，アナリストは実際に悪意のある行動が存在するか否かを判断するために，複雑なアラートを調査する必要がある。

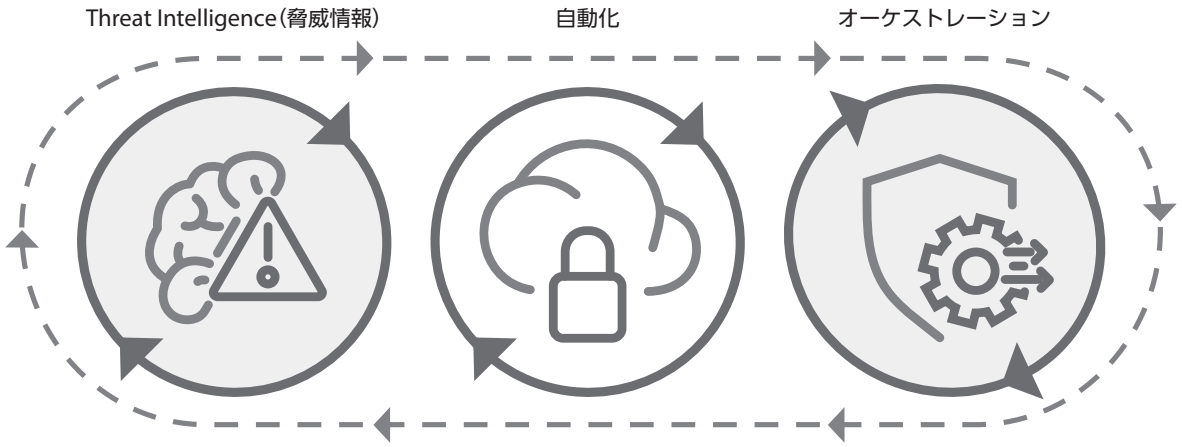


図-2　脅威情報を蓄積・活用するためのSAOサイクル

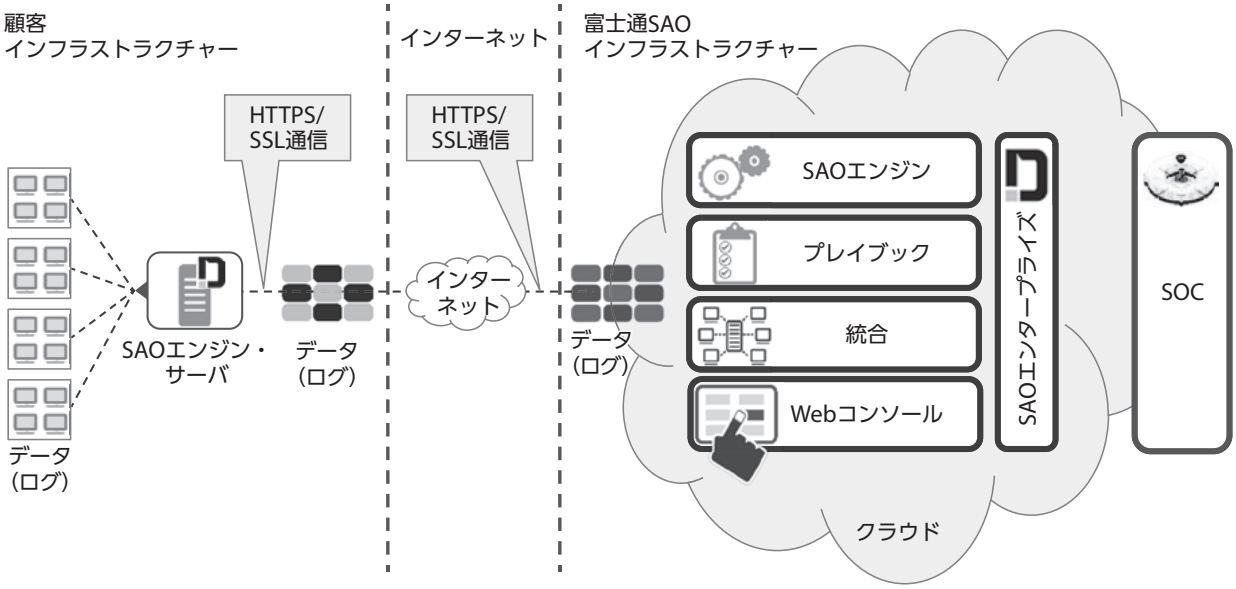


図-3　SAOの基本構造

一方，事前対応のアプローチでは，プロキシサーバや電子メールサーバなどに実装されているセキュリティ技術によって検出されなかったものも含め，攻撃者が隠そうとする最も複雑な脅威を想定して検索するという考え方がアナリストに求められる。したがって，SAOによって，できる限りノイズを除去する，あるいは脅威情報によってインシデントの事例を充実させるというニーズに対応することが最優先課題となる。富士通が提供する管理サービスとしてのSAOの基本構造を図-3に示す。

3.　ATCが提供するサービス

SOCからATCへ移行する主な目的は，顧客に対して従来のSOC技術では識別できなかった攻撃に対応するエンタープライズCSIRTサービスを提供することである。顧客からの信頼度が高く，攻撃の誤検出率が低く，脅威情報によって充実したデータが備えられ，より迅速で効果的なインシデント対応を顧客に提供することが，このソリューションに求められる。

図-4に示すように，エンタープライズCSIRTモデルを導入することによって，富士通は顧客の情報セキュリティチームとインシデント対応チームを補完できる。顧客によっては，他社が提供するサービスを導入していたが，経験豊富なアナリストがいなかったか，または適切なインシデント対応を行うことができないなどの問題があった。

このCSIRTモデルに適合するサービスの例は，以下のとおりである。

・サイバーセキュリティ脅威情報の提供
・サイバーセキュリティ脅威への対応
・脆弱性管理
・EDR
・MDR（Managed Detection & Response）
・ユーザーおよびエンティティ（管理対象となる情報資源，データ資源）の行動分析
・高度製品分析
・詐欺行為検知サービス
・脅威ハンティングサービス

これらのサービスの中には，富士通のオファリングメニューとして既に利用可能なものもあり，今後開発予定のものもある。この開発にあたっては，ATCの脅威分析エコシステムをサポート・強化していく技術パートナー（特に，SAOと統合する能力を持つパートナー）を探すことが重要である。

セキュリティ監視において，事前に攻撃発生を認識して迅速に対応することが重要であり，事後対応アプローチでは，現代の攻撃を予測・検出し十分な対応を行うことはもはや不可能である。顧客のネットワークにおいては，SIEM技術などのソリューションが依然として重要である。しかし，これらは従来型のネットワーク中心のモデルであり，コンプライアンス要件や規制に対応するために導入されたものであるため，標準的な相関ルール以外のアラームは網羅しきれない場合もある。プロキシサーバ，DNS（Domain Name System）サーバ，更にはエンドポイントなどの大量のログは，ログ送信元の1秒あたりのログメッセージ数に影響するため，SIEM技術によるアプローチに適合しない場合もある。

これらのログ全体にわたる脅威ハンティングは，スクリプトやエンドポイントにおけるなりすまし，DNSサーバやプロキシサーバの制御によるビーコン発信など，セキュリティ技術をすり抜ける可能性のある攻撃を特定して保護するために重要である。

脅威ハンティングは，1週間に数時間だけ実行するといったモジュール型のサービスとして顧客に提供できる。また，エンドポイント，Webサイト，電子メールの管理サービスなど，既存のコモディティサービスにも適用できる。その例を図-5に示す。

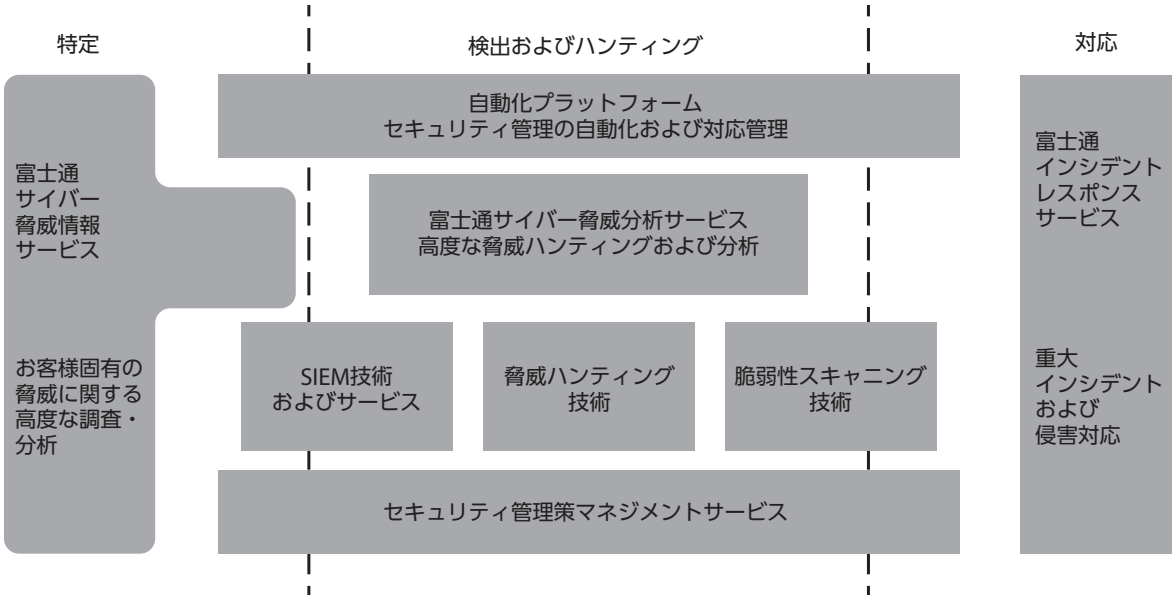


図-4　エンタープライズCSIRTモデル

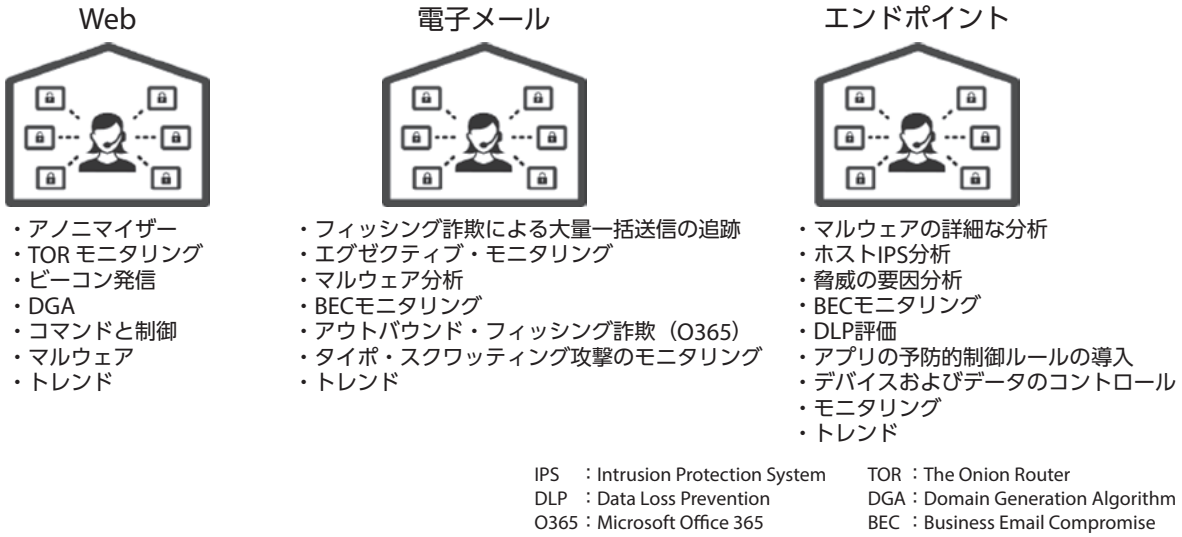


図-5　脅威ハンティングのサービス例

サービスとしての脅威ハンティングは，以下のような結果をもたらす。

・早期に検出率の向上
・従来のセキュリティ技術では見落とされていた脅威の特定
・攻撃の標的となるポイントを全体的に削減する
・既存のSIEM技術への上乗せができる
・既存のコモディティサービスへの上乗せができる

4. 今後の展開

セキュリティへの脅威は複雑さを増し続けており，富士通はこれに対して適切に対応しなければ効果的なセキュリティ運用を提供できない。

ATCは，サイバーセキュリティの脅威情報を利用して，脅威のアクティビティと顧客のビジネスに対する影響を結び付け，状況に応じた情報を積極的に提供する。これによって，顧客のブランドをセキュリティインシデントの影響から守る。富士通は，攻撃者を追跡し，新たな脅威の出現を絶えず監視し，脆弱性管理の結果と組み合わせることで，顧客が直面する脅威に対応していく。

富士通は，リアルタイムの脅威分析に基づいたセキュリティビジネスフレームワークを提供し，脅威ハンティングモデルで新たな脅威と侵害の兆候を見つけ出していく。そして，これらは全ての，高度標的型攻撃対策のエコシステムにおける新しいセキュリティサービスによって支えられる。

富士通は，これを実現するために，セキュリティの自動化およびオーケストレーションによって日常業務やインシデントを合理化する。そして，これを基盤としてエンタープライズCSIRTサービスを提供していく。

5. むすび

本稿では，富士通ATCの構築と導入方法，およびそのメリットについて述べた。

セキュリティの成熟に伴って組織が成長し，セキュリティ対策の導入が増える中，攻撃者も絶えず変化している。したがって，富士通も変化する脅威に都度対応を続けていかなければならない。セキュリティ監視の領域において，自動化，オーケストレーション，AI，EDR，脅威ハンティングなどは，比較的新しい分野である。富士通は，ATCへの移行によって，お客様に代わってこれらのサービスを導入・管理できる。

富士通は，既知と未知の両方の脅威を検出する能力を高め，結果を理解できるセキュリティ技術者の人材開発と育成を図っていく。SAOを導入することで，より効率的で予測可能な方法でその能力を高め，最適な運用管理サービスと効果的なインシデン

ト対応を実現していく。

参考文献

(1) N. Lord：What is a Security Operations Center (SOC)?
https://digitalguardian.com/blog/what-security-operations-center-soc
(2) K. Townend：What's a Playbook and why do I need one?
https://gdsengagement.blog.gov.uk/2014/03/26/whats-a-playbook-and-why-do-i-need-one/
(3) E. Kanal：Machine Learning in Cyber Security.
https://insights.sei.cmu.edu/sei_blog/2017/06/machine-learning-in-cybersecurity.html
(4) Burning Glass：Cybersecurity jobs.
http://burning-glass.com/research/cybersecurity/
(5) D.Culbertson et al.：Indeed spotlight: The Global Cybersecurity skills gap.
http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/
(6) National Cyber Security Centre：10 steps：Monitering.
https://www.ncsc.gov.uk/guidance/10-steps-monitoring
(7) FireEye（2017）M-Trends EMEA 2016.
https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

著者紹介

Paul McEvatt
Fujitsu Services Ltd.
EMEIA（Europe, the Middle East, India and Africa）向けサイバーセキュリティサービスの企画・開発・運営に従事。

Advanced Threat Centre and Future of Security Monitoring

(original of previous paper on pp. 16–23)

Paul McEvatt

Electronic data and people's lives are becoming more closely intertwined, leading to the formation of a digital society where the Internet is being used to process an ever-increasing volume of data exchanges and transactions. This trend is blurring the boundary between the real world and virtual spaces, resulting in a greater impact from cyberattacks. A fundamental requirement for all businesses is security monitoring to detect such attacks. Security monitoring is usually performed under the management of a security operations centre (SOC). However, to cope with the continued rise in cyberattacks, organisations as a whole must continue to innovate. This paper describes an innovative approach to improve incident response in SOC or a response by ATC (the Advanced Threat Centre) which realizes security automation and orchestration as a new model to support effective security monitoring.

1. Introduction

As attacks that threaten cybersecurity continue to increase in complexity and scale, the security operations centres (SOCs) are finding it difficult to respond to all the attack faced by modern day businesses. Security monitoring is vitally important, and businesses that lack control over their security measures will be limited in their ability to exercise accountability for their actions. This is why security monitoring by SOCs is so important.

An SOC is defined as a body that organises an information security team to perform continuous monitoring and analysis on the basis of an organisation's basic policies on security.[1)] Traditionally, SOCs were built and operated on the basis of technology and procedures such as signature matching (a method that check mechanically against rules that detect cyberattacks). However, this approach is no longer sufficient for effective security monitoring. A fresh, proactive (preventative) approach is required to counter modern-day cyberattacks.

This paper describes the construction and implementation of Fujitsu's Advanced Threat Centre (ATC).

2. Security automation and orchestration

Security automation refers to the automation of business processes with the aim of cutting down on the number of routine checks and incidents (potential threat situations) processed by the SOC's first line (handled by operators following established procedures) and second line (handled on an ad hoc basis by analysts without following procedures). On the other hand, orchestration refers to the process of weaving security techniques together so that they can function through rational cooperation. This facilitates the acquisition of abundant information by SOC

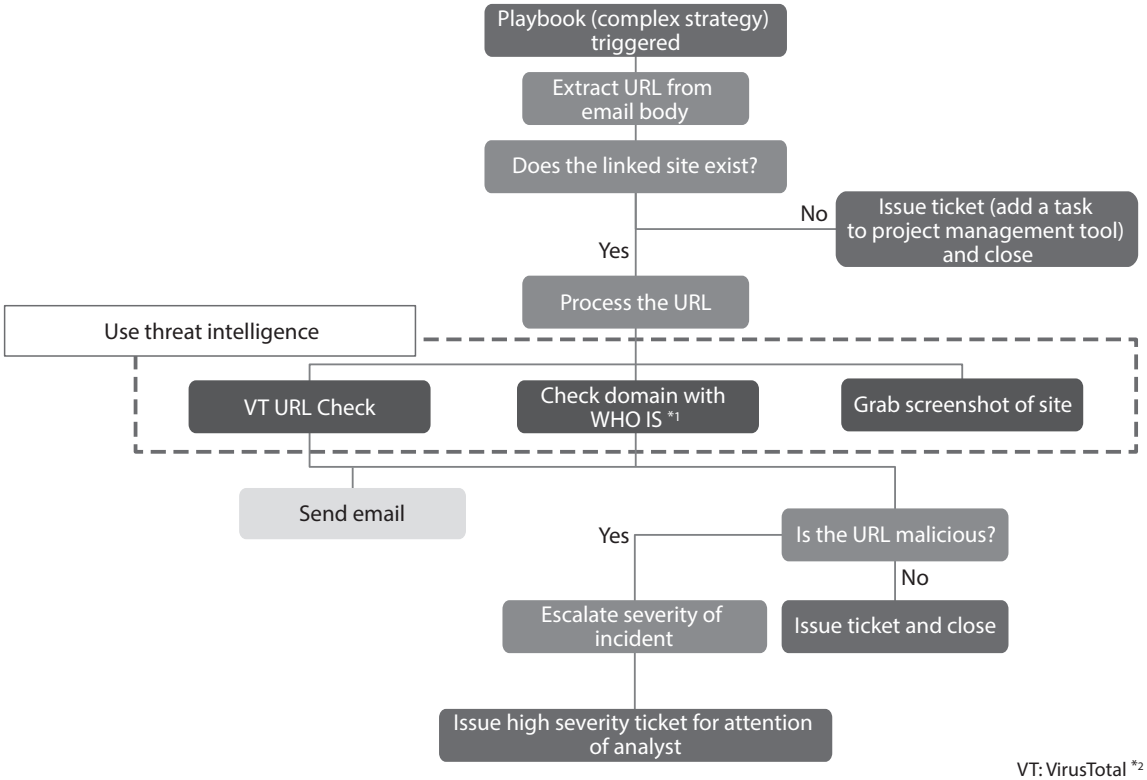
analysts, allowing them to automate the blocking of attacks.

Both of these concepts use a strategic approach that is tailored to the organisation's environment and security technologies. This strategy, also called a "playbook", is derived from the sports terminology that describes the team's various strategies. By adopting this strategy, the team can aim to become a winner in the market.[2] Common playbooks can be customized to an organisation's structure by orchestrating the organisation's business processes and technologies. Figure 1 shows an example of a playbook for phishing fraud alerts.

2. 1 Effects of security automation and orchestration

The principal effects of security automation and orchestration (SAO) are shown below.

- Reducing wasted effort by automating repeatable and predictable checks/incidents
- Closing the cyber skills gap and boosting the morale of security staff by reducing basic tasks such as daily checks, thereby providing analysts with the space to work on the true analytical task of threat hunting (using techniques such as log analysis and machine learning to track down intrusive threats)
- Delivering an API-to-API, playbook-driven, standardised approach to incident response by integrating all standard security technologies
- Improving incident response and service quality in line with ongoing improvements in mean-time-to-recovery (MTTR) metrics, demonstrating the ability to respond to



*1: Domain name registration information retrieval service.
*2: Service to check for malicious URLs.

Figure 1
Playbook for a phishing alert.

customer incidents more efficiently

- Enriching the response to incidents by automating the extraction of threat information on the basis of a strategy adapted to each set of circumstances, and thereby reducing the incidence of false positives
- Orchestrating incident responses by using strategic decision-making to take steps such as blocking out networks on the basis of the use of proxy servers or firewall rules
- Alleviating alert response fatigue in security operations by reducing the number of incidents faced by first line and second line analysts
- Allowing Fujitsu to develop highly reliable security services for highly targeted attacks as we move towards advanced analytical methods such as the Enterprise Computer Security Incident Response Team (CSIRT), Endpoint Detection and Response (EDR) and fraud prevention
- Deploying basic strategies that can be used across multiple SOCs and customer environments through Managed Security Service Provider (MSSP) offerings
- Leveraging the technical functionality of several new technologies, such as machine learning, to provide capabilities such as incident assignment, integrated management, and rapid appraisal of overall threat parameters through the use of security dashboards

Some of these effects are described below in more detail.

2. 2 Machine learning

According to a study in the field of machine learning at Carnegie Mellon University, investment in machine learning for cybersecurity applications is expected to reach $96 billion (Approximately 10 trillion yen) by 2021.[3] Traditional security technologies such as intrusion detection, antivirus, and security information & event monitoring (SIEM) are evolving as vendors use scalable cloud networks to introduce machine learning into their solutions.

The new technologies in the SAO market, it is possible to use machine learning to make the same logical decisions as cybersecurity analysts. This will also be a key driver for security automation for analysts in Fujitsu's ATCs.

2. 3 Cyber skills gap

Due to fierce competition in the cybersecurity market, organisations are also facing staff retention challenges in addition to dealing with continued attacks. A study by Burning Glass[4] found that cybersecurity workers could expect to be paid $6,500 more a year on average compared to traditional ICT workers. There is currently a large gap between the supply and demand for cybersecurity workers, and as of 2019, there are reported to be 1.5 million unfilled positions.[5]

By automating the SOC first line and second line monitoring processes, Fujitsu's security workers will become able to tackle more interesting analyses and work at a senior analyst level. They will also be able to get involved in more interesting security work, resulting in security workers with higher morale and stronger motivation as well as a greater retention of security workers. These are key objectives in a very competitive cybersecurity employment market.

To transform our SOC into an ATC, Fujitsu will need to develop new services aligned to growth areas and invest in these markets. EDR is one approach that is predicted by Gartner to show a high rate of growth over the next three years.

Although traditional antivirus measures still have a place in modern enterprise, the security monitoring of the future will also require EDR solutions and ATC analysts that can understand identified threats. It is therefore extremely important that we select the correct technologies to

support the approach and ensure that analysts are skilled to the right level for true threat hunting.

2. 4 Mean Time to Respond (MTTR) and Mean Time to Detect (MTTD) as metrics

For managed security services provided to customers, the performance guarantee of a service level agreement (SLA) is still a formal key performance indicator (KPI). However, organisations will increasingly adopt new metrics for the evaluation of incident responses.

The UK government describes cyberattack response methods as follows: "An effective response to an attack depends upon first being aware that an attack has happened or is taking place. A swift response is essential to stop the attack, and to respond and minimise the impact or damage caused." [6)]

The mean time to respond (MTTR) is an incident response evaluation criterion that has been adopted in recent years to achieve this objective. Using this metric, it can be shown that the time taken to respond to incidents is gradually decreasing. However, the mean time to detect (MTTD) is a term representing the number of days for which an attacker is able to remain hidden inside a network before being detected. According to a study by FireEye, the global average dwell time of attackers from intrusion to discovery went up from 99 days in 2016 to 101 days in 2017.[7)]

Under these circumstances, it is no longer effective to respond to incidents manually within the specified time frame. Instead, by moving towards an SAO-based ecosystem for dealing with advanced threats, Fujitsu will be able to automate first line and second line work so that our analysts can concentrate their efforts elsewhere.

By using SAO to gather and store information about threats and incidents, it will be possible to provide prompt and diverse incident responses. Figure 2 shows an overview of the SAO cycle. In today's SOC, an analyst would be required to manually cross-reference an indicator of compromise (IOC) across multiple intelligence sources, which takes too long. By automating this process and proactively blocking latent threats on the basis of risk scores, this will provide huge improvements for customers.

2. 5 Change in analyst mind-set

The transformation from SOC to ATC will involve fundamental changes in the approach to security monitoring and will require major

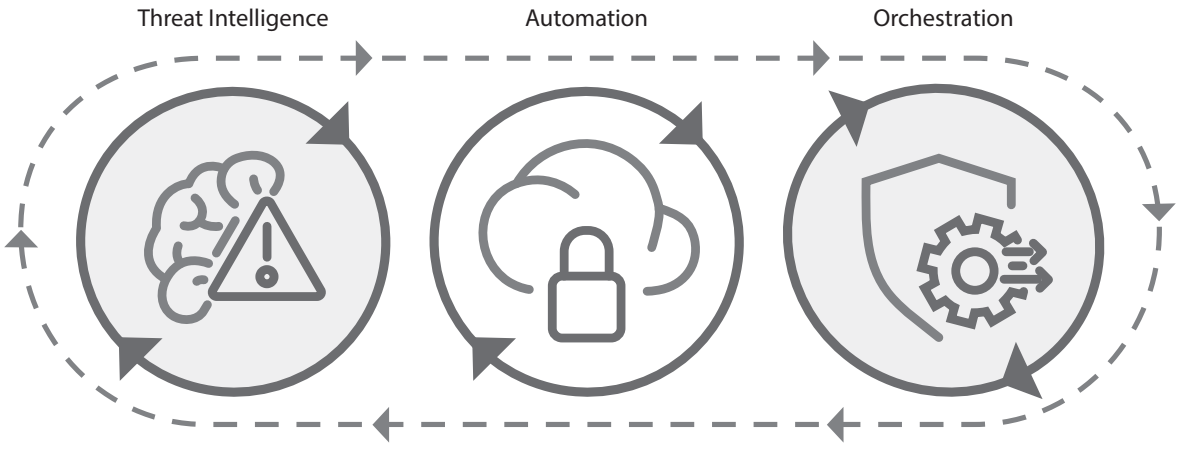


Figure 2
SAO cycle for storage and use of threat intelligence.

changes in the mind-set of analysts. Take antivirus, for example, conventional security technologies issue warnings to SOC analysts about specific pieces of malware that match a signature. By switching over to ATC, it is easy to tell whether or not malware was delivered by a large-scale malicious spam campaign, in which case the incident can be dealt with and solved simply by quarantining and disinfecting the affected PCs and/or servers.

If new types of security technology that uses AI, machine learning algorithms, et al, are implemented, then it will be possible to identify only anomalous traffic. Examples of this include odd behaviour by users or servers, such as running scripts or logging in at unusual times. This reactive approach will require analysts to investigate alerts that are more complex to determine whether malicious activity is indeed taking place.

Conversely, a proactive approach requires analysts with a mindset that leads them to search for the most complex threats that attackers try to hide, including threats that are not picked up by security technologies such as proxy servers or email servers. It is therefore of paramount importance that SAO is used to address the need for removing as much noise as possible or to enhance incident case through threat information. Figure 3 shows the basic structure of SAO provided by Fujitsu.

3. Services provided by ATC

The primary objective of the shift from SOC to ATC is to provide our customers with enterprise CSIRT services that focus on attacks that could not be identified by traditional SOC security technologies. ATC needs to have a greater level of trust from customers, a lower false positive attack detection rate, a repository of threat information for enriched threat analysis, and the ability to provide customers with a faster and more effective incident response.

As shown in Figure 4, the introduction of an enterprise CSIRT model enables Fujitsu to complement the threat information identification teams of our customers. Although our customers may previously have introduced services provided

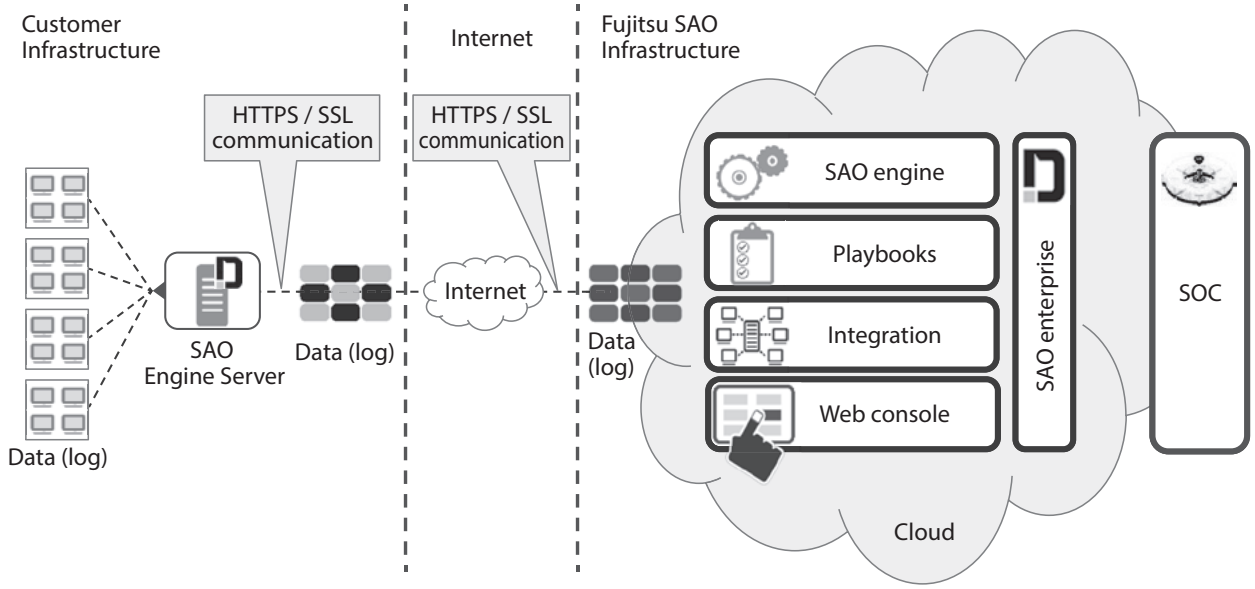


Figure 3
Basic structure of SAO.

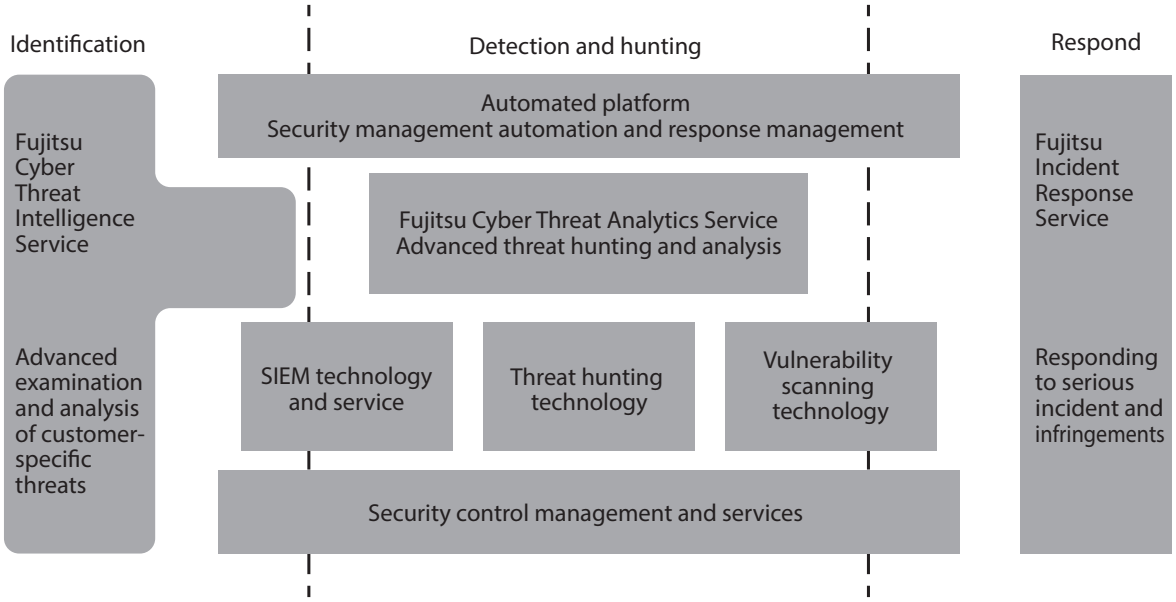


Figure 4
Enterprise CSIRT model.

by other companies, they may lack experienced analysts or the ability to deploy adequate incident responses.

Examples of services that fit with this CSIRT model include the following:

- Provision of cyber security threat intelligence
- Response to cyber security threats
- Vulnerability management
- Endpoint detection & response (EDR)
- Managed detection & response (MDR)
- Behaviour analysis of users and entities (managed information resources and data resources)
- Advanced product analytics
- Threat hunting service
- Fraud detection services

Some of these services are already available as Fujitsu's offerings, while others are in the works. Appropriate technology is vital for supporting and strengthening ATC threat analysis ecosystems, especially ecosystems that can be integrated with SAO. It is also essential to develop ecosystems in cooperation with our partners.

In reactive approaches to security monitoring, it can no longer be considered adequate to predict, detect and respond to modern-day attacks. Whilst solutions such as SIEM technology are still important in customer networks, these are traditional network-centric models introduced to conform with compliance requirements and regulations, and do not always provide comprehensive alarms beyond the standard correlation rules (combinations of phenomena that are simultaneous and strongly interrelated). The large log files of devices such as proxy servers, domain name system (DNS) servers, and endpoint equipment are sometimes unsuitable for an SIEM approach due to the impact on the number of messages per second.

Threat hunting across all these logs is essential to identify and protect against attacks that may have bypassed security technologies, such as scripting or identity theft at an endpoint, or beaconing activity through DNS or proxy controls.

Threat hunting can be offered to customers as a service in modular blocks such as a set number of hours per week. This can also be applied to existing commodity services such as endpoints,

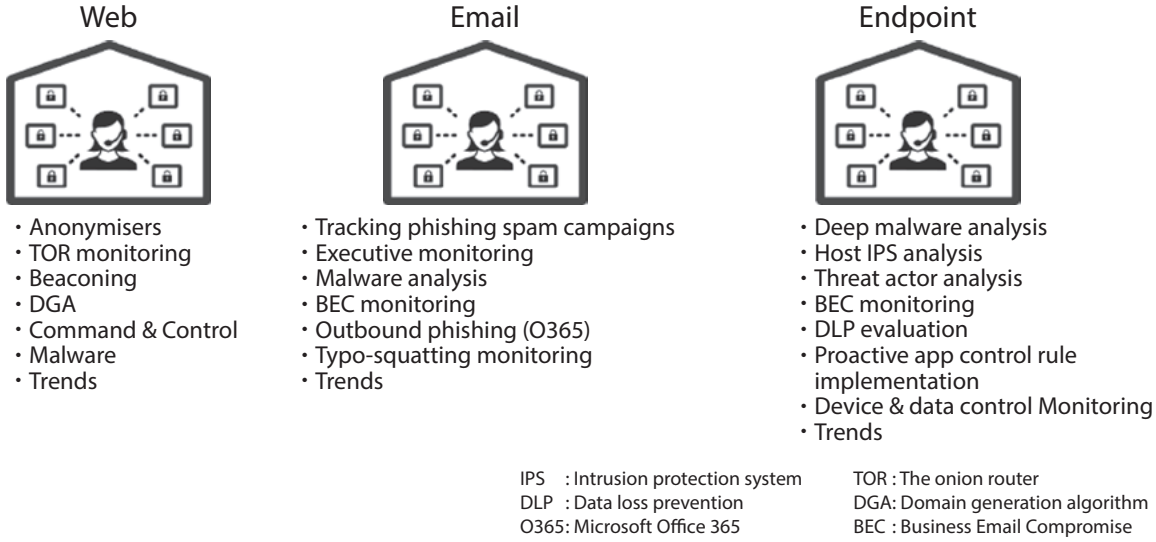


Figure 5
Examples of threat hunting services.

Web services and email management services. An example is shown in Figure 5. Threat hunting as a service will result in:

- Improvement of detection rates in a faster time period
- Identification of threats that are missed by traditional security technologies
- Reduction of the overall target of attacks
- Additional security measures beyond existing SIEM technologies
- Additional security measures to existing commodity services

4. Future prospects

Security threats will continue to increase in complexity, and unless Fujitsu responds appropriately, we will be unable to provide effective security operations.

The ATCs will use cyber threat intelligence to correlate threat activity to its impact on the customer's business and actively provide contextual information. Thereby, they will shield the customer's brand from the effects of security incidents. Fujitsu will track attackers, keep a continual look-out for new threat, and will combine this with the results of vulnerability management to address the threats faced by our customers.

We will provide a security business framework based on real time threat analytics to discover new threats and signs of compromise in a threat-hunting model. All of this will be supported by new security services in an advanced ecosystem of countermeasures to targeted threats.

To achieve this, Fujitsu will use SAO and orchestration to streamline routine tasks. Based on this, we will provide enterprise CSIRT services.

5. Conclusion

In this paper, we have described the construction and deployment of Fujitsu ATC and its merits. As organisations grow as security matures and introduce more security measures, the attackers they face also continue to change. It is therefore vital that Fujitsu keeps responding to these changing threats. In the field of

security monitoring, techniques such as SAO, orchestration, AI, EDR, and threat hunting are all relatively new. A transition towards ATCs will allow Fujitsu to introduce and manage these services on behalf of our customers.

At Fujitsu, we will improve our ability to detect threats, both known and unknown, and we will grow and develop analytical staff who can understand the results of this detection. By introducing SAO, we will improve our ability to make this happen in a more efficient and predictable manner, delivering optimal operational managed services and effective incident responses.

References

1) N. Lord: What is a Security Operations Center (SOC)? https://digitalguardian.com/blog/what-security-operations-center-soc
2) K. Townend: What's a playbook and why do I need one? https://gdsengagement.blog.gov.uk/2014/03/26/whats-a-playbook-and-why-do-i-need-one/
3) E. Kanal: Machine Learning in Cyber Security. https://insights.sei.cmu.edu/sei_blog/2017/06/machine-learning-in-cybersecurity.html
4) Burning Glass: Cybersecurity jobs. http://burning-glass.com/research/cybersecurity/
5) D. Culbertson et al.: Indeed spotlight: The Global Cybersecurity skills gap. http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/
6) National Cyber Security Centre: 10 steps: Monitoring. https://www.ncsc.gov.uk/guidance/10-steps-monitoring
7) FireEye (2017) M-Trends EMEA 2016. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

Paul McEvatt

Fujitsu Services Ltd.

Mr. McEvatt is currently engaged in planning, development, and operation of cybersecurity services for EMEIA (Europe, the Middle East, India and Afirica).