Advanced Threat Centre and Future of Security Monitoring

● 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 cyber attacks. 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 cyber attacks, organisations as a whole must continue to innovate. This paper describes an innovative approach to improve incident response in SOC or a response by the Advanced Threat Centre (ATC) 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 cyber attacks). However, this approach is no longer sufficient for effective security monitoring. A fresh, proactive (preventative) approach is required to counter modern-day cyber attacks.

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.

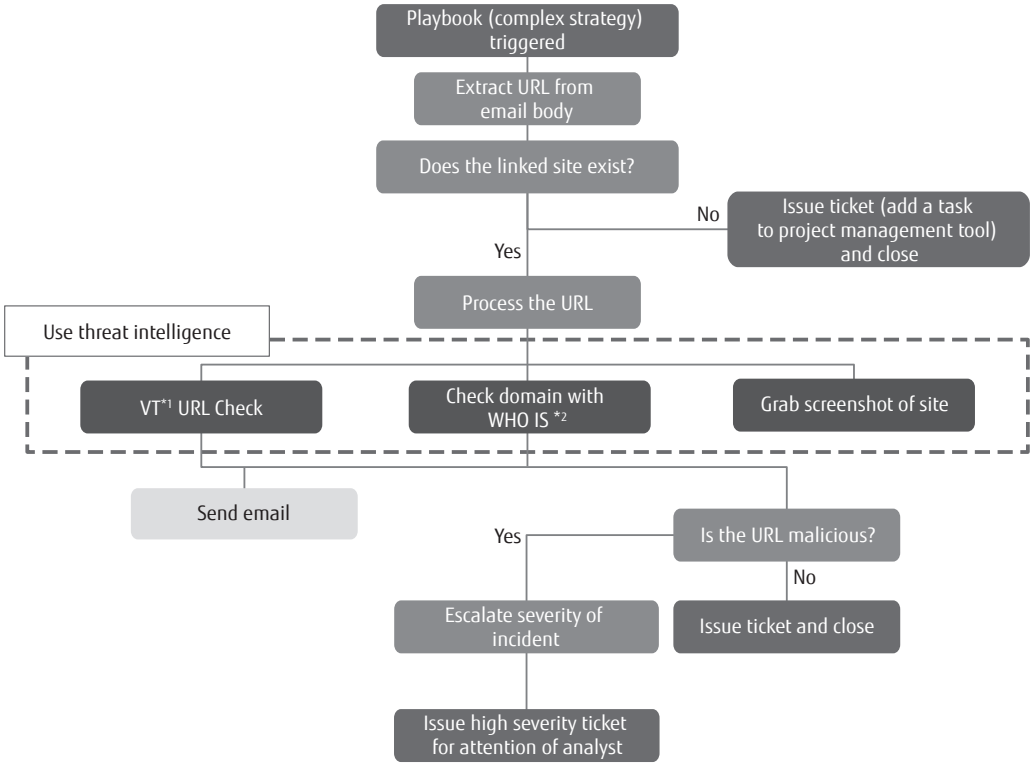

Figure 1
Playbook for a phishing alert.

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

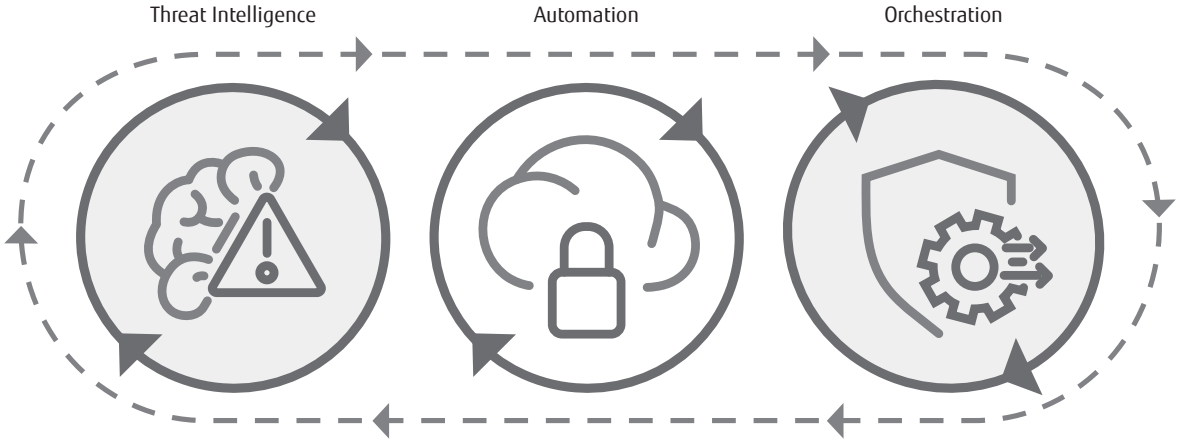

Figure 2
SAO cycle for storage and use of threat intelligence.

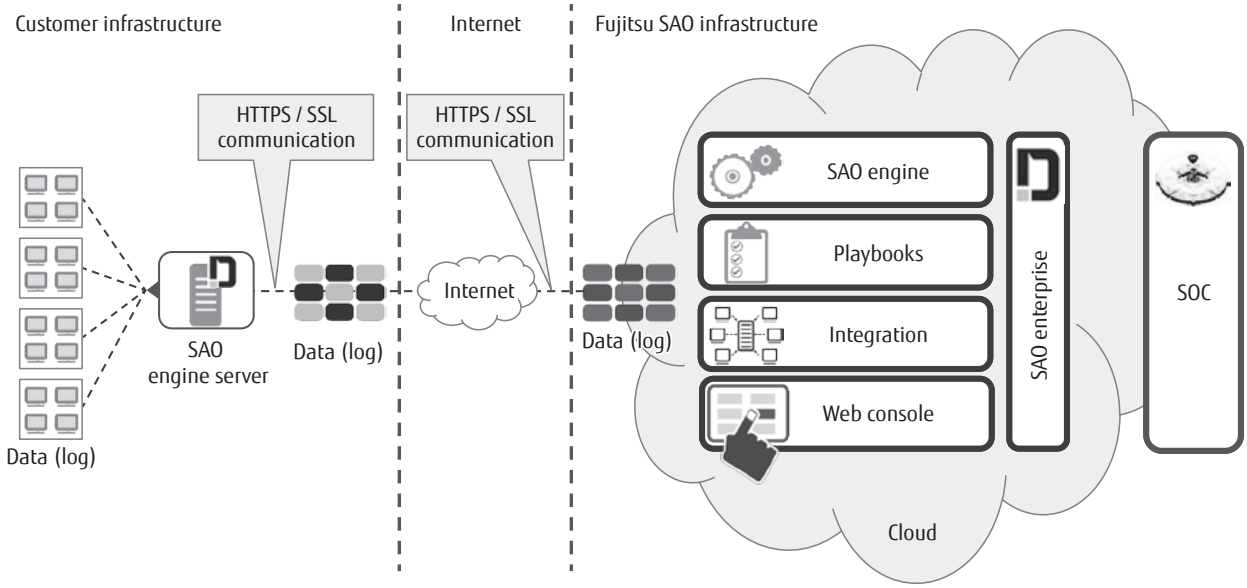

Figure 3
Basic structure of SAO.

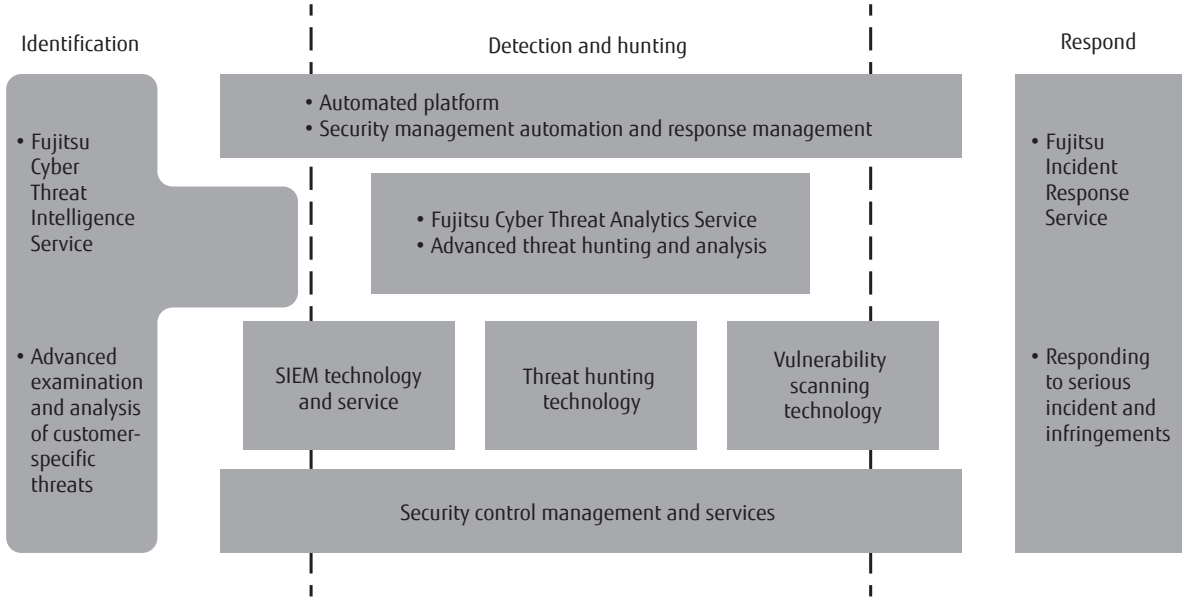

Figure 4
Enterprise CSIRT model.

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

- Provision of cybersecurity threat intelligence
- Response to cybersecurity 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, 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

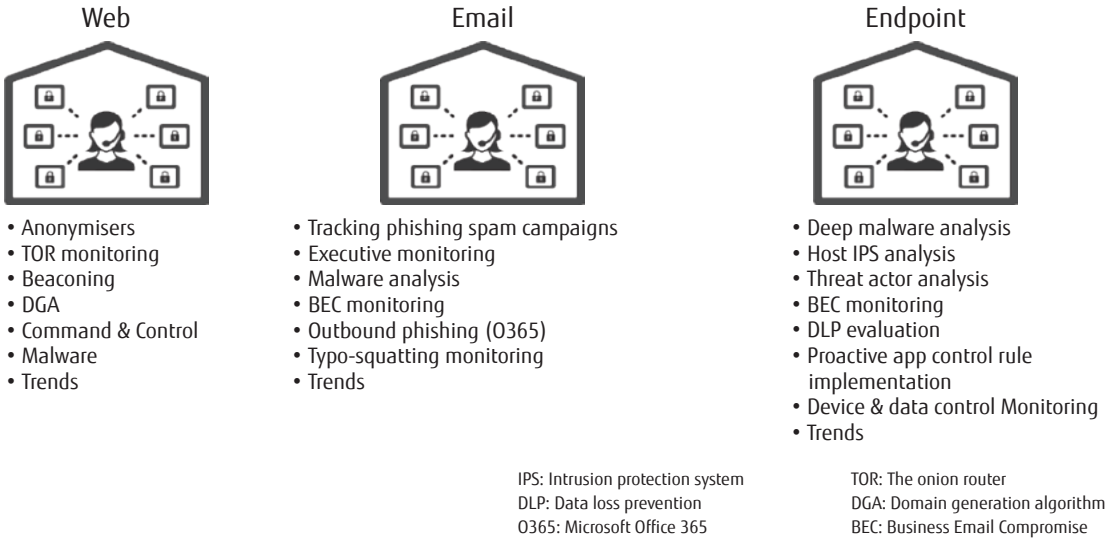

Figure 5
Examples of threat hunting services.

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

This paper 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: Demand for Cybersecurity Workers Outstripping Supply. *https://www.burning-glass.com/blog/demand-for-cybersecurity-workers-outstripping-supply/*
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 to cyber security–Monitoring. *https://www.ncsc.gov.uk/guidance/10-steps-monitoring*
7) FireEye: M-Trends 2018. *https://content.fireeye.com/m-trends/rpt-m-trends-2018*

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 Africa).