

Log Analysis・SIEM

Backgrounds and Issues

Log analysis realizes to deter damage expansion and promotes preventive measures by defining damages and attack paths when occurring security incidents.

On the one hand, when adopting log analysis to your organization, you will see the following issues: “We need human resources with basic skills in TCP/IP and extensive knowledge across layers.”; “We will face time restrictions if manually performing log analysis.”

- The team members can acquire IT skills in various layers, which is the basis of log analysis, and identify incident indicators from the logs stored in multiple NW and security equipment.
- The team members can decide to adopt SIEM*, a log analysis tool, and determine its rules.

*SIEM (Security Information and Event Management)

A mechanism that notifies administrators of anomalies and measures based on the log information collected from each machine and application.

Issue-Solving and Outcomes

The project team proceeded with learning under a dominant principle, “deepen our insights through hands-on.”

Processes of our Efforts

- 1 **Basic Learning** : Collecting information from books and publications.
- 2 **Building Emulation Networks** : Establishing practical environments.
- 3 **Penetration Testing** : Determining and implementing attack scenarios
- 4 **Performing Log Analysis** : Examining logs and recording attack indicators
- 5 **Adopting SIEM and Determining Detection Rules** : Formulating, adopting, and verifying detection rules based on analysis results

As a result of the efforts, the project team created two materials as their outcomes.

Methods for Utilizing Log Utility Tools Against Targeted Attacks

The team compiled their outcomes into two methods: **Manual log analysis** under penetration testing and **Automated and efficient log confirmation** using SIME and EDR.

*EDR (Endpoint Detection and Response)

A technology that continuously monitors and responds to cyber threats at endpoints of computer systems.

Rulemaking Procedures for Log Aggregation and Detection Using SIEM

The project team outlined the rules to set log aggregation and detection using free and open-source SIEM products. This material is to **provide the procedures necessary for the log aggregation for operators** while furnishing **the ideas and an implementing method of detection rules using SIEM** for security personnel.

Interviews with A Graduate



Mr. SAJI Yuki
OPTAGE Inc.

What is your utmost benefit from this project?
I could learn a range of IT skills through the project. I constructed servers, connected them to networks, and installed SIEM into systems; I did conduct environment creation through verification by myself. I sometimes give staff consultations as a CSIRT member within the company. Due to my experiences absorbed through the project, I can respond to my colleagues with consistent images of systems.

Methods for utilizing project outcome
For example, we can utilize our outcomes for educational programs in log analysis for beginners and for achieving mutual understanding among practitioners. I also take advantage of these outcomes when explaining to newly appointed junior

fellows. Since we outlined the methods to operate free and open-source SIEM on the setting procedures, we can utilize the outcomes during the phase considering the adoption of commercial SIEM.

This is unique to the ICSCoE!
I could build a connection with the other members. In general, we never have the experience of learning with the same members for one year after entering the working world; however, I could establish a professional network with colleagues where I discuss issues not superficially but genuinely with them. Furthermore, I could dramatically improve my knowledge and skills throughout the program; now I feel that “I can contribute to my company.” and “I can proactively involve in in-house activities.” My change in awareness is also unique to the ICSCoE.



The ICSCoE Report is a public relations newsletter on ICSCoE's activities.

The Core Human Resource Development Program for 5th Cohort

Introducing Our Efforts of Final Projects

A final project is that our trainees utilize their knowledge and experience absorbed through a one-year curriculum and tackle the issues set for their dispatching company and industry as a team. The fifth-cohort trainees undertook 21 projects. We will introduce three of them.

English Reading for Security Engineers

Backgrounds and Issues

The characteristics of the cybersecurity world are “rapid change” and “no borders”. Security engineers must promptly and accurately utilize information from around the world; thus, English reading comprehension is indispensable.

In the meantime, we see an issue that many security engineers in Japan have an aversion to dealing with English. This project was designed to **improve the motivation and competency of English reading comprehension**.

Issue-Solving and Outcomes

The trainee, who conducted this project, produced two outcomes to aim to improve two abilities: **information-gathering ability** and **growth ability**. Information-gathering ability enables us to collect precise information from around the world and apply that information in practice, while growth ability empowers us to utilize voluminous information from English and improve our capability as an engineer.

Study Guide to improve English Reading Comprehension

He created the materials condensing a variety of hints to improve English reading comprehension and information-gathering ability.



セキュリティ英語特有の意味・用法

セキュリティ分野特有の言葉や、一般的な意味・用法とセキュリティ分野でよく使われる意味・用法が異なる言葉がある。あらかじめ押さえておくことで混乱を避けられる。

表現	セキュリティ特有の意味・用法の例	一般的な意味・用法の例
in the wild	(マルウェアや攻撃コードが) 実際の攻撃に使われている	野生の
compromise	～を侵害する	妥協する
actor	攻撃者、アクター	俳優
PoC (Proof of Concept)	(脆弱性を実証する) 攻撃コード	概念実証

This study guide outlines the contents of materials and a variety of hints to read English sentences.

Security English Vocabulary

The trainee created the English vocabulary list specialized for security engineers. He analyzed the overseas security news articles, considering the number of occurrences and uses, and carefully selected approximately 330 frequently used words. Furthermore, the trainee prepared the translations and usage cases based on the usages of the analyzed articles; thus, the English vocabulary list benefits security engineers who can utilize it practically. Since the security English vocabulary list is prepared in PDF and CSV files, security engineers can leverage it for rote exercises in various ways – importing it into an application.

Feature 1 Carefully select “actually used” words in security news articles.
Feature 2 Provide meanings and usage examples unique to security.

単語	意味	関連語	使用例
include	～を含む	【名】Inclusion: 包含、含まれるもの 【形】Inclusive: すべてを含んだ	the email including a malicious macro 悪意のあるマクロを含むメール
steal	～を盗む		steal sensitive information 機密な情報を盗む
exploit	(脆弱性) を突いて攻撃する 【名】Exploit(プロット・コード)	【名】Exploitation: (脆弱性を突く) 攻撃 【形】Exploitable: 悪用可能な	actively exploited vulnerability よく攻撃に使われる脆弱性
release	～を入手可能な状態にする 【名】Release(プログラムの) リリース		updates released today 今日リリースされたアップデート
target	～を標的とする 【名】Target: 狙われた、標的の	【形】Targeted: 狙われた、標的の	targeted attack 標的型攻撃
allow	～を可能とする、許可する	【名】Allowlist: 許可リスト	the bug allowing attackers to execute arbitrary code 攻撃者に任意のコード実行を許可するバグ

Please visit our ICSCoE website for more information on “English Reading for Security Engineers”. You can download the study guide and English vocabulary list from the following QR code and link. This project was also covered on news sites.

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/english-reading.html



