IPA Better Life with IT

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

8.31.2023

vol. 16

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

Participation in “Interop Tokyo 2023” Received Attention to Our Efforts in Cybersecurity Human Resource Development

In June 2023, “Interop Tokyo 2023” was held, and the Industrial Cyber Security Center of Excellence (ICSCoE) participated. The trainees and graduates of the “Core Human Resource Development Program” gave their presentations regarding the outcomes of their final projects.

Interop Tokyo is a historical event focusing on Internet technologies and applied businesses. The ICSCoE participated in this event as a place to present the outcomes of the Core Human Resource Development Program and give back their knowledge and skills absorbed through the program to societies. Twenty members from Kanae-kai, the graduate community, and the 6th cohort attending the program (as of June 2023) took the stage in the venue. The members released the technical outcomes derived from their final projects and the insights for cybersecurity; thus, they could strongly impress the contents of the Core Human Resource Development Program to the participants of this event.

Great Response to Cybersecurity Manga for Kids Even After Completing Final Project

Mr. Harunobu YAGI (4th Cohort)
Central Japan Railway Company

The project members presented the outcomes of the one-year educational projects at the exhibition booth, and Mr. YAGI from Central Japan Railway Company took the stage. Mr. YAGI gave a presentation regarding his production project of cybersecurity manga for Kids two years ago and its subsequent results. This project aims to make children interested in cybersecurity and recognize the need for cybersecurity to improve Japan's cybersecurity levels in the future, where children will flourish. Mr. YAGI said, “ Many previously published cybersecurity manga in Japan focused on what not to do, which led children to distance themselves from cybersecurity.” To solve this issue, he characterized security techniques and illustrated how to deal with cyber attacks in an approachable way. He aimed to make cybersecurity more approachable and relatable. As part of their project outcomes, Mr. YAGI conducted a questionnaire targeting children who read the cybersecurity manga. He shared the results that the children drastically deepened their understanding and increased their cool images of cybersecurity after reading the manga. The manga is also very effective for the children to be interested in working in the cybersecurity field in the future. This product, titled “Everyday Zeroday ”, is available for free at the online store and published in both English and Japanese versions. Mr. YAGI said, “ I established the Cybersecurity awareness-raising subcommittee for younger generations and have kept performing the cybersecurity activities for kids within the “ Kanae-kai”, our graduate community, after completing the final project. By working together and collaborating with a variety of people in the Kanae-Kai, I believe I can achieve the goal of this project.”

Original author/ Harunobu YAGI
Comic artist/ Sohsuke

Total 2 episodes

▼Please visit the website for more details at https://tapas.io/series/EVERYDAY-ZERODAY/info

On the following page, we will introduce the presentation at the booth by the 6th cohort trainees.

Developed the OT Incident Response Training Program and Inherited it after the Completion

Ms. KAWAKAMI Rika (6th Cohort)
JFE Steel Corporation

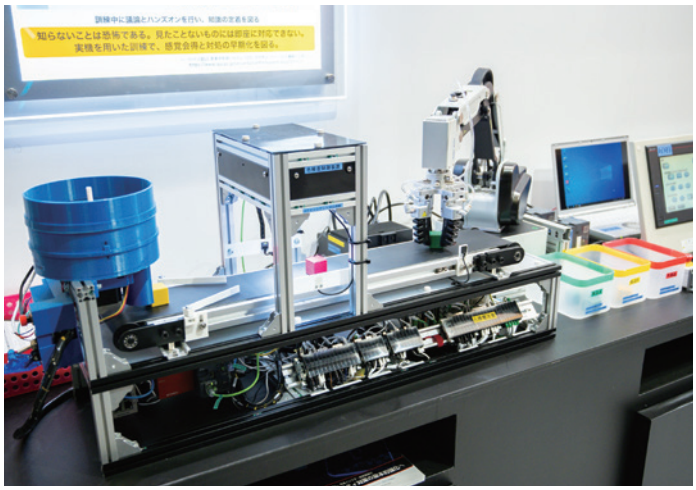
Mr. OTA Satoru (6th Cohort)
Hitachi Solutions, Ltd.

Today, the targets of cyber-attacks are not limited to the information systems but have been expanding to the OT systems without directly connecting to the Internet. To prevent attacks against OT, which cause immense damage, immediate response to and recovery from actual security incidents is required. Against these backgrounds, Ms. KAWAKAMI and Mr. OTA developed a training program for responding to security incidents against IT systems related to OT during their final project. This training program aims to enable OT personnel to absorb skills and the sense of acknowledgment to cooperate with the security department and promptly respond to and recover from actual incidents when they occur. The project members set up the simulated plant produced through their project at the booth; thus, the participants could glimpse into the demonstrations performed by the project members.

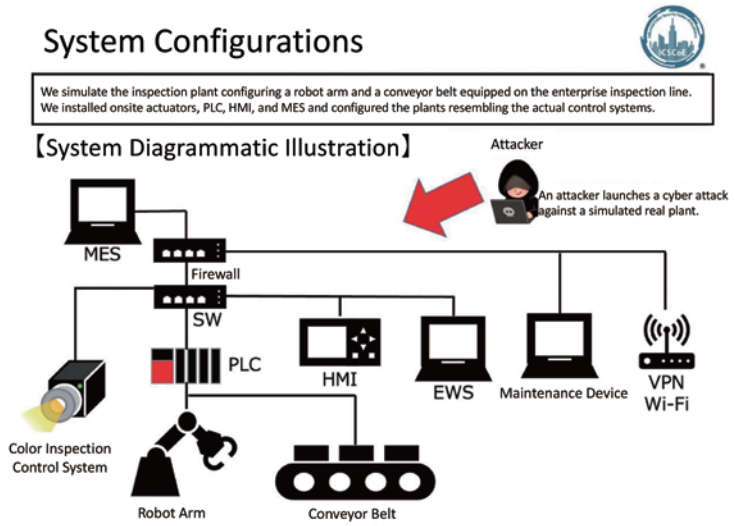
The contents of this training program are to experience network, log analysis, threat analysis, defense products, regulation, education/ training, BCP, and attack methods through a series of exercises.

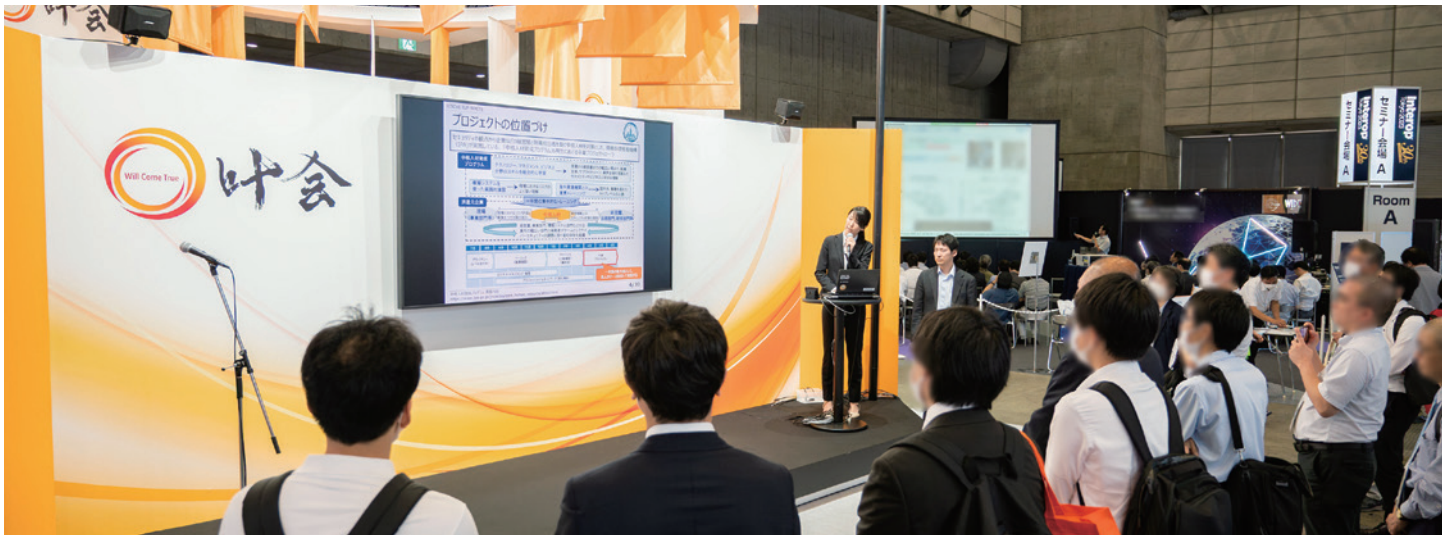
For this program, the project members prepared five scenarios, such as Trigger Malfunction Caused by Unauthorized Devices, Shutdown Plants Caused by Suspicious USBs, Infiltrate from Unmanaged Wi-Fi, Infect Malware on Control Devices, and Compromise through VPN Devices. These scenarios intend to simulate and respond to the inspection plant by configuring a robot arm and a conveyor belt on the enterprise inspection line. The participants discussed the activities to restore and recover from the security incidents by scenario and obtained the skills to promptly respond to and recover from these incidents through practical operations leveraging the transportable equipment.

Ms. KAWAKAMI and Mr. OTA said, " To protect OT systems, we need enterprise-wide measures and obtain comprehensive knowledge and skills in IT and OT. We must cooperate with entities, each of which has its unique expertise." They also emphasized the importance of defense strategies collaborating with IT and OT. " Our goal is that the members can utilize the deliverables produced through this project even after completing the ICSCoE program and further enhance them," and they concluded their presentation.



The simulated real plant produced through the final project





Many people listened to the demonstrations at the booth.

Create Best Practices for Vulnerability Responses as the Deliverables

Mr. YAMAMOTO Shinya (6th Cohort)
Chubu Electric Power Co., Inc.

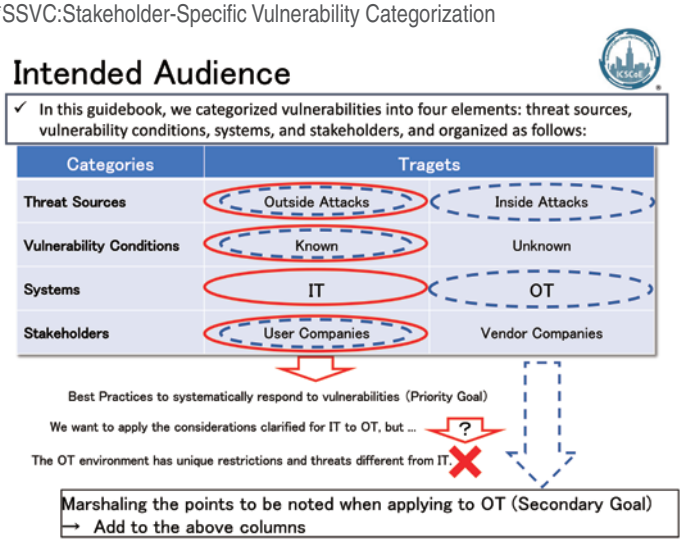
Mr. YAMAMOTO and MR. WATANABE, the 6th cohort trainees, set up the theme of their final project of "Vulnerability Handling." Their final project is based on the threats exploiting the vulnerabilities underlying systems ranked in "Information Security Threats Top 10, 2023 version," published by the IPA; thus, the project aims to marshal the conditions to undertake the measures against these threats and provide the best practices.

In this project framework, the members focused on the states of measures for IT and OT undertaken and categorized targets of vulnerabilities in four evaluation axes: threat sources, vulnerability conditions, systems, and stakeholders. With these four elements, the personnel can organize concrete countermeasures applying to each category and enable them to undertake effective responses.

Mr. WATANABE Takuya (6th Cohort)
Sumitomo Chemical Co., Ltd.

Moreover, from the perspective of how to treat and determine input vulnerability information, they amplified the outcomes and issues occurring when leveraging SSVC. Besides, they clarified how to estimate the days to apply the extracted points undertaking measures to OT and take each response, and they introduced precise know-how necessary for coherent practices through the establishment, implementation, and operations. Mr. YAMAMOTO concluded, "We will strive to continue sharing the outcomes, knowledge, and know-how obtained through this final project and further leverage them among the members."

*SSVC:Stakeholder-Specific Vulnerability Categorization



Create Guidelines and Educational Content from Practical Exercise Environments.

Mr. KAMIIKE Yuichiro (6th Cohort)
West Japan Railway Company

Three trainees from the sixth cohort, Mr. KAMIIKE, Mr. KANEKO, and Mr. FUKUDA, presented "How to Deal with Configuration Errors of Cloud Security." First, Mr. KAMIIKE said, "The members had not had enough knowledge of security before participating in this project, but we could produce the outcomes by pushing toward as the sixth cohort trainees."

The background of this project is that cloud services have become advanced and a necessary foundation to promote enterprise DX while many security incidents have occurred in the Cloud environment. 95% of the security incidents Most of the causes of those security incidents are simple configuration errors, accounting for 95 percent in 2020, and they assumed it would be 99 percent in 2025. Thus, Mr. KAMIIKE said, "The approaches to prevent the incidents caused by configuration errors of the Cloud services are urgent."

This project aimed to establish guidelines describing the crucial points for the philosophy of configuration errors and effective countermeasures and to create educational content for hands-on training to learn the risks and measures for configuration errors. The project members explored the literature, interviewed the enterprises utilizing solutions, verified technologies, derived their best practices through discussions among the members, and summarized the guidelines and educational contents as their outcomes. In the guide, the project members stated, "Configuration errors are human errors and challenging to prevent; thus, the mechanisms to accept occurring issues and detect and remedy them are crucial." Based

Mr. KANEKO Eiji (6th Cohort)
Mitsubishi Electric Corporation

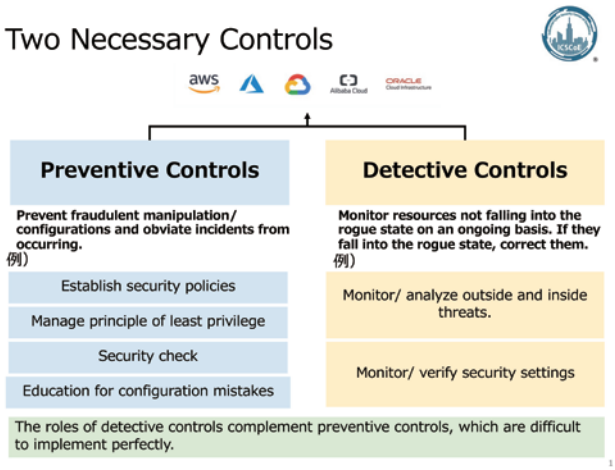
Mr. FUKUDA Tetsuya (6th Cohort)
OPTAGE Inc.

on this philosophy, the members marshal the subjects from two fields, such as preventive controls and detective controls, and describe the points to implement CCoE, CSPM, and IaC*.

Also, for the educational content, the members developed the guardrail-typed security leveraging preventive and detective controls and a training environment to understand the risks caused by configuration errors in the Cloud as a true-life experience. This educational content is a form to obtain practical techniques through hands-on exercises and groupworks.

Mr. KAMIIKE said, "Through this final project, the members established a Cloud environment for exercises, which enables them to verify practical techniques and develop the guidelines and educational content."

*CCoE:Cloud Center of Excellence, CSPM:Cloud Security Posture Management, IaC:Infrastructure as Code



Demonstration of The World's First 800GbE Interoperability Experiment

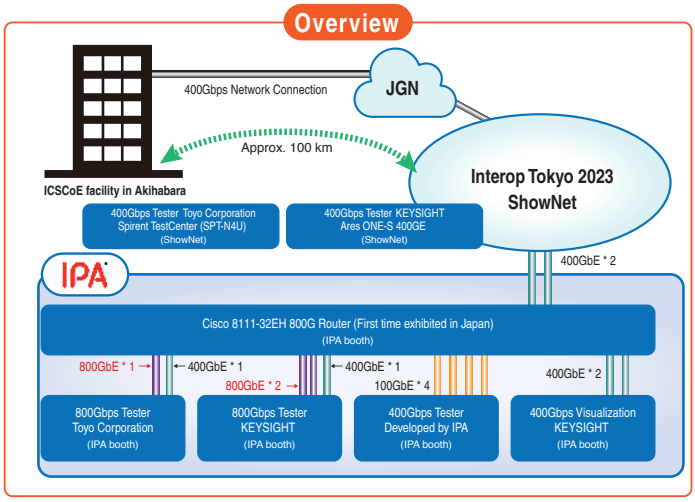
At Interop Tokyo 2023 (3 days from June 13, 2023), the ICSCoE partnered with multiple vendors to demonstrate the world's first 800GbE interoperability experiments.

The ICSCoE led this experiment in collaboration with Cisco Systems, Inc. (providing Cisco 8111-32EH), Keysight Technologies, Inc. (providing Keysight AresONE 800G), and SpirentCommunications, Inc. and Toyo Corporation (providing SpirentB2 800G ethernet appliance), we were able to gather the latest 800GbE equipment, which is still under development, at the IPA booth. We realized network interoperability among various equipment and conducted security-focused assessment and verification. This was a symbolic demonstration to show exactly what Interop is about.

The ICSCoE established a 400G network connection between our facility in Akihabara and the IPA booth at the Interop venue using 400G IOWN* demonstration networks developed by the NTT group via ShowNet. We also conducted security experiments to generate and control 400Gbps traffic using the traffic generator developed by the ICSCoE. It was the first experiment using IOWN (Open APN) 400G network connection open to the public. This experiment also contributed to APN (All-Photonics Network) advocated by NTT.
*IOWN: Innovative Optical and Wireless Network

Moreover, the ICSCoE collaborated with Keysight Technologies, Inc. and Spirent Communications, Inc./ Toyo Corporation for their experiments. Each company installed devices at ShowNet sight and at the IPA booth and established network connections between them. We used the network connections to carried out a performance assessment of the devices.

For the experiments we conducted, received positive feedback from the Executive Committee and Awards Committee members of Interop Tokyo 2023 and won four awards. As a result, we obtained comments from the four cooperating companies, stating that they achieved satisfying experimental outcomes. The ICSCoE will continue to work to provide new value by making full use of our knowledge and technology for the future.



ICSCoE Engineer's Comment

At the ICSCoE, we have been working to enhance cybersecurity measures against cyber attacks that are becoming increasingly severe. To tackle this, we have been collaborating with manufactures and installed state-of-the-art technologies in our facilities, and built a secure environment for testing security measures and product verification using actual equipment. We are also focusing on nurturing talent in this field.
At Interop Tokyo 2023, these efforts were recognized, and we were able to gather the cutting-edge 800G Ethernet devices which are still under development. It was the first time in the world to conduct performance and security assessments with devices developed by multiple manufacturers. We acknowledge that our commitment is to persist in these efforts and their outcomes, and we will endeavor to strengthen our relationships with manufacturers and continue to create new value.

MATSUMOTO Satoshi
Cyber Technology Laboratory, ICSCoE

The Core Human Resource Development Program for 6th Cohort was Completed

In June 2023, the ICSCoE held the sixth graduation ceremony for the Core Human Development Program: forty-eight trainees graduated from our one-year program, and they took the first step as Industry Cybersecurity experts.

Ms. MURAKAMI Yuka
OPTAGE Inc.

Remarks from the Graduate Representative

This one year was a turning point in my professional life and a fruitful moment with various opportunities to grow and learn.

Since the impacts of COVID-19 stabilized, many trainees could participate in overseas deployment exercises during the sixth term program.

I participated in the France deployment exercise and realized the latest trends in France that became a factor of self-improvement. I absorbed valuable experience by participating in the overseas forum and hearing firsthand opinions about the reality of security abroad that it's hard to experience at a company.

In addition, through the ordinal training, we thought of risks from the attacker's perspective and obtained various security insights by learning step-by-step in environments similar to actual sites.

Cybersecurity is a constantly evolving area - as technologies develop and become more complex, new threats emerge - we must keep developing security measures to respond to this rapid change. Leveraging the connections built through one year and gathering information is essential. I want to cherish those connections as the most valuable assets.

From now on, we will utilize the knowledge and skills absorbed through the program and strive to support Japan's critical infrastructures from the security perspective as our mission. Also, we will value the connections among the instructors, seniors, and colleagues and pursue our further growth and learning. Thank you very much for your support throughout the year.

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan
Bunkyo Green Court Center Office,
2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591
TEL 03-5978-7554 FAX 03-5978-7513

R60 古紙パルプ配合率 60%再生紙を使用
リサイクル適性Ⓐ この印刷物は、印刷用の紙へリサイクルできます。