Interview with a graduate

Mr. JINNO Chikara (First person on the far left)Kawasaki Heavy Industries, Ltd.

What is your utmost benefit from this project?

The benefit I gained from this project was to reconsider security strategies and tactics. Before working on the final project, I believed that the significance of enterprise security strategies is a broad and deep understanding of enterprise security guidelines. My most beneficial outcome is that I discovered that the essential aspect is the integrity of enterprise strategies. Another benefit is that I realized generative AI is an efficient tool to establish security strategies and tactics under time and resource constraints.

Methods for utilizing project outcomes

As organizations develop their internal security strategies and tactics, we encourage them to review the outcomes we have produced and conduct a self-check to verify whether personnel properly derived the strategies and tactics and appropriately applied the guidelines.

Also, when you struggle with how to utilize generative AI, I want you to use the outcomes as a reference.

This is unique to the ICSCoE

Firstly, I gained practical, grounded knowledge and skills through hands-on exercises using actual equipment; therefore, I cultivated the ability to apply knowledge to concrete measures effectively.

Secondly, I built strong, broad networks among the instructors and my colleagues. The fruitful and valuable experience I gained through the program is the exchange of insights with and consultations from the prestigious instructors and colleagues from other enterprises regarding a delicate subject, cybersecurity.

I believe that these experiences will enable me to propose more effective and persuasive strategies to strengthen my enterprise's cybersecurity.

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

IPA Better Life with IT

ICSCoE Industrial Cyber Security Center of Excellence

ICSCoE REPORT

8.29.2025

vol. 23

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

8th Core Human Resource Development Program Introducing Activities of Our Final Projects

An Approach to Enhancing Security Through Threat Intelligence

Backgrounds and Issues

The rapid adoption of advanced technologies, such as cloud computing, Internet of Things (IoT), and artificial intelligence (AI), has significantly increased accessibility and complexity of enterprise information systems in recent years. On the other hand, cyberattack techniques have become increasingly sophisticated; thus, defense models, which heavily rely on traditional tools and apply passive approaches, are proving complicated in responding to complex and varied threats.

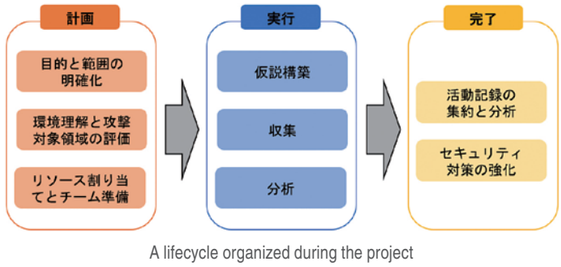
Moreover, the personnel of Security Operation Centers (SOCs) are under pressure to process massive logs and alerts daily and have been facing issues such as an increase in monitoring load and a shortage of human resources. As a result, the risks of overlooking signs of critical incidents have emerged. Furthermore, existing detection techniques often overlook malware campaigns masquerading as legitimate communications and cyberattacks using unknown tactics that cause delays in responses.

In light of these circumstances, the project focused on "Threat Hunting," an approach for proactively examining within systems and identifying signs of hidden threats. Threat Hunting has been gaining attention as an approach to complement and strengthen traditional defense models.

In this project, the team examined how to incorporate Threat Hunting into actual organizational operations from theoretical and practical perspectives.

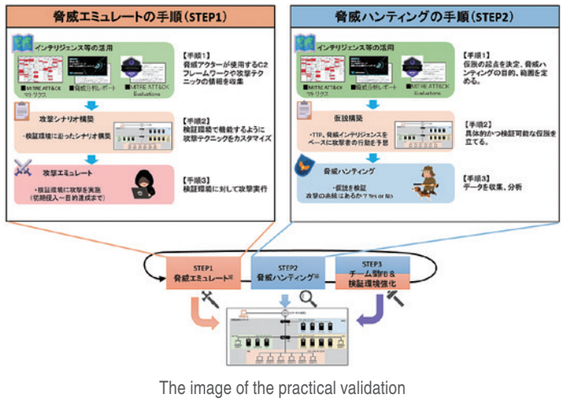
Issue-solving & Outcomes

The project began with literature reviews to deepen the understanding of the fundamental concept of Threat Hunting and the construction processes of hypotheses. The team analyzed existing hunting frameworks, organized major processes shared among them, and developed their unique lifecycle model as the next step, while focusing on understandability and versatility.



A lifecycle organized during the project

In addition, the team replicated their attack scenarios, bypassing the traditional security measures within simulated environments, and implemented and verified some hunting approaches to retrieve attack traces based on their hypotheses. As a result, the members obtained valuable insights applicable to practical operations, including considerable points to formulate hypotheses and the unique features of each approach.



The image of the practical validation

In the report compiling the above outcomes, named "Best Practices for Threat Hunting," the project team systematically organized fundamental concepts, practical methodologies, and key points for adopting threat hunting to enterprises. This report will support both the personnel considering the adoption of Threat Hunting and those seeking to review or refine their current operational practices.

Interview with a graduate

Mr. ONOUE Masayuki (2nd from the left in the front row)

What is your utmost benefit from this project?

My utmost benefit is that I realized the significance of having attackers' perspectives. By understanding how attackers infiltrate systems and attempt to evade detection technologies, I identified risks often overlooked when relying solely on a traditional defender's perspective. These insights and learnings are the most significant outcomes of this project, which I can effectively apply to strengthen the organization's security mechanism moving forward.

Methods for utilizing project outcomes

In addition to the fundamental concepts and procedures of Threat Hunting, we systematically compiled our insights and verifications obtained through the project activities. Through this report, we aim to provide a reference that enables readers to understand practical methodologies and their effectiveness.

In particular, we aim to provide content that offers concrete directions for practical implementation and effective insights for advancing security measures, especially for those considering adopting Threat Hunting or those who face challenges with the current monitoring systems.

This is unique to the ICSCoE

One year at the ICSCoE was a valuable experience, not merely acquiring knowledge - it allowed me to cultivate practical skills in thinking independently, experimenting, and turning ideas into practice. Through sharing insights with my colleagues from diverse backgrounds and receiving professional feedback from highly experienced instructors, I gained a multilateral perspective on cybersecurity.

In particular, the in-depth discussions during the final project provided me with a rare learning opportunity that is hard to achieve in my regular work environment. It offered me valuable experience in developing broader perspectives and adaptable approaches to problem-solving. I hope to apply those learnings to enhance security measures and foster human resource development within my organization.

Furthermore, with the growing significance of cybersecurity, I would like to proactively contribute to the advancement of the entire industry by applying the knowledge, skills, and insights that I gained through the ICSCoE program.

Individual organizations cannot address security challenges alone; thus, a collaborative approach across the industry and information-sharing are more essential than ever.

I want to continue engaging in efforts to strengthen security while keeping in mind this broader, industry-wide perspective for the future.

Developing security tactics based on corporate strategy: Considering generative AI and security guidelines

Backgrounds and Issues

As enterprises have been increasingly reliant on digital technologies, security has become a critical concern for the IT Department and management due to the growing sophistication of cyberattacks. However, the strategies and policies indicated by management tend to be abstract; therefore, in reality, many practitioners struggle to accurately understand their intents and identify and apply the appropriate guidelines.

Therefore, this project aims to create actionable recommendations for practitioners by examining how to develop security tactics more efficiently, leveraging the guidelines of the NIST Cybersecurity Framework (CSF) and generative AI.

Issue-Solving and Outcomes

In this project, firstly, the team clarified what security strategies and tactics are derived from.

As a result, we reconfirmed that we should develop security strategies in alignment with the overall missions, visions, and management strategies of enterprises, but not exist alone. We must derive security strategies from the business strategies and contribute directly to achieving organizational goals. We apprehended this relation, which crystallizes a hierarchical structure as follows: "Missions/Visions, and Management Strategies" at the top delivering concrete" Security Strategies," "Security Tactics," and "Security Plans." These elements must work together and maintain the integrity of upstream strategies and policies.

The team emphasizes that security strategies must support and promote the achievement of management strategies that derive from them; security tactics should ultimately contribute to the actualization of management strategies.

The Relationship between Corporate Strategy and Functional Strategies

Next, the team clarified the methods for utilizing the security guidelines.

A guideline is a framework that shapes the management and security strategies into concrete security tactics; it differs from merely a checklist.

Moreover, standardizing terminologies and concepts related to security helps encourage a shared understanding among internal and external stakeholders, facilitating smoother communication and contributing to enhanced external credibility.

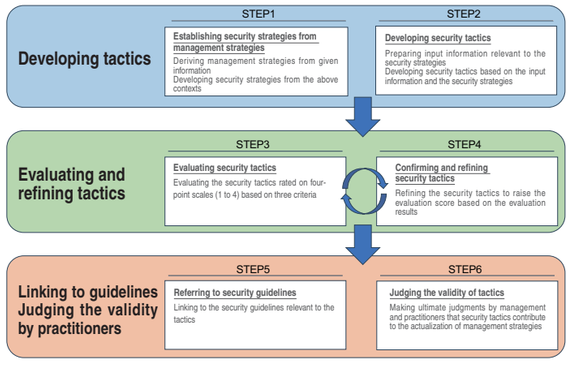
So far, the members have defined security strategies, tactics, and guidelines; however, they are dealing with a wide variety of management strategies and security guidelines in their real operations. In this context, the team utilized generative AI not only to reduce the time spent organizing/ understanding information but also to evaluate the validity of security tactics by third parties.

On this basis, the members examined the development of security tactics using generative AI. They took the approaches specifically as follows:

- **STEP 1 : Outputs from management strategies to security strategies**
- **STEP2 : Developing security tactics**
- **STEP3 : Evaluating security tactics**
- **STEP4 : Confirming and refining security tactics**
- **STEP5 : Referring to security guidelines**
- **STEP6 : Judging the validity of security tactics**

Through this project, the team confirmed that generative AI is efficient for creating drafted security tactics and bringing up new ideas.

In this manner, generative AI has proven that drafting security tactics is efficient and prompt, while it depends heavily on the given information due to the boundaries of imagination; thus, the team concluded that human judgment and refinement are essential to ensure accuracy and reliability.



The Examples of Applying Generative AI to Security Tactics Development Processes