SWIMLANE

CASE STUDY

Toshiba Automates, Centralizes, and Streamlines Security Operations by Deploying a Modern SOAR

Toshiba Group has long been engaged in the social infrastructure business based on its business philosophy "Committed to People, Earth and Future." Three elements, "People," "Earth," and "Future" are included in this management philosophy, which expresses the Group's desire to create a better world in which "humanity" and "Earth" are in perpetual balance, rather than a world in which only humanity benefits. And today, they have been developing their business with the mission of supporting social infrastructure through cyber-physical system technology that combines the physical technology the Group has cultivated since its founding as a manufacturing company, with cyber technology centered on information and AI.

TOSHIBA

Challenges

Toshiba now has a division called the Cyber Security Center, which was established in 2017 in response to the recent rise in information security risks. The organization's mission is to support Toshiba Group's overall security, which covers not only information security but also product security for its products, systems, and services. The Cyber Security Center promotes risk-based security measures, and "Our challenge was how to efficiently monitor and operate security while properly understanding company-wide risks and utilizing threat intelligence," recalls Kenji Kojima, Chief Specialist, Security Strategy Group, Cyber Security Center, Corporate Technology Planning Div. of Toshiba Corporation.

While threats have become more complex and sophisticated in recent years, and incidents have increased, IT environments and security methods have also become more complex. How to effectively manage them has become an important issue for the immediate future. In addition, there is a staffing shortage of security professionals with sufficient knowledge and skills, so it was necessary to consolidate and visualize knowledge with a limited number of people to ensure SecOps efficiency.

At the Cyber Security Center, "We had been consolidating and managing information on security incidents that had occurred, but we thought it was necessary to strengthen management using this information for more efficient operations. We also thought that one of the keys was to enhance the integration between systems" said Toshimichi Ohashi, Chief Specialist, Managed Security Department, Cyber Security Technology Center, Corporate Research & Development Center of Toshiba Corporation. "In security, it is important to learn from past mistakes and lead to proper improvements, so we needed to change our management structure" (Kojima).

Solution

The Cyber Security Center began to consider countermeasures to solve these issues, and since SOAR (Security Orchestration, Automation and Response) products were just starting to appear in the Japanese market, the team created an initial list of five SOAR vendors to review. The Center then narrowed down its selection to three companies for a detailed evaluation of each platform's

Kenji Kojima
Chief Specialist
Security Strategy Group
Cyber Security Center
Corporate Technology Planning Div.
Toshiba Corporation

Toshimichi Ohashi
Chief Specialist
Managed Security Dept.
Cyber Security Technology Center
Corporate Research & Dev. Center
Toshiba Corporation

Future

Since there are various use cases that can be automated in the operations of the Cyber Security Center, the team is currently consolidating incident information and gradually incorporating it into Swimlane. They plan to expand automation to even more use cases in the future.

Kojima commented, "Since there is a very wide range of security products and it is important to easily integrate with various products, we hope to build out integrations with our extensive security products and groupware in the future."

"Our center covers product security as well as information security. The key to product security is to quickly identify which part of your products are affected by newly discovered vulnerabilities. We hope to use Swimlane for product security in the near future."

functions. The security team then conducted a PoC (proof-of-concept) as a part of the product selection process to confirm that the SOAR solutions would meet the Center's requirements. While considering the SOAR vendors, the Center placed importance on the ability to integrate with external products and services, ease of operation, vendor support system, and customizability. In particular, as they moved forward with proactive security measures, they believed that the integration with threat intelligence was especially important, so the team focused on whether it would be easy to properly integrate threat intelligence into SOAR and utilize it within security.

Deployment

In the end, the SOAR vendor selected by the Cyber Security Center was Swimlane. "The most important aspect of SOAR is that we can build the playbook the way we want it and we're able to share the operational results on the dashboard. Swimlane's playbooks and dashboards are highly customizable, which was the biggest reason for our selection," explained Kojima. Swimlane offers the advantage of dashboards that can be freely reconfigured to easily display the KPIs you want to see. "With other companies' products, the playbooks come pre-installed as defaults, but with Swimlane, I was able to customize the task-flow of the various playbooks myself flexibly" (Ohashi).

When implementing Swimlane, the security team not only conducted a desk study in advance, but also a PoC. One of the key points the Center worked on was to define the use cases they wanted to automate with the SOAR platform in advance and visualize the procedures properly, which made the implementation in Swimlane relatively smooth.

Benefits

By consolidating incident information in the Swimlane platform, the current alert status could be quickly ascertained, and by managing the information in dashboards, it became easier to achieve a common understanding of security processes and procedures within the company.

In addition, the Center was now able to quickly identify current KPIs and improve its security operations based on the visualized metrics. In the Center's operations, Swimlane and threat intelligence tools are actively integrated, so if a suspicious IoC is found, it is automatically investigated and fed back to operations to smoothly facilitate incident response. By streamlining each of these tasks in this way, they have succeeded in reducing the overall work time and have been able to allocate the saved resources to other tasks.

"For example, we obtain information on security-sensitive URLs and IP addresses from various sources from time to time, and we need to investigate logs showing that Toshiba employees have accessed these URLs. Before the introduction of Swimlane, these tasks were done by manually going to the logs of each network device and entering commands for searching. After deploying Swimlane, we can check for the corresponding access log by simply entering the IP address, and the results can be viewed in Swimlane, greatly improving the speed and time required for the work" (Ohashi).