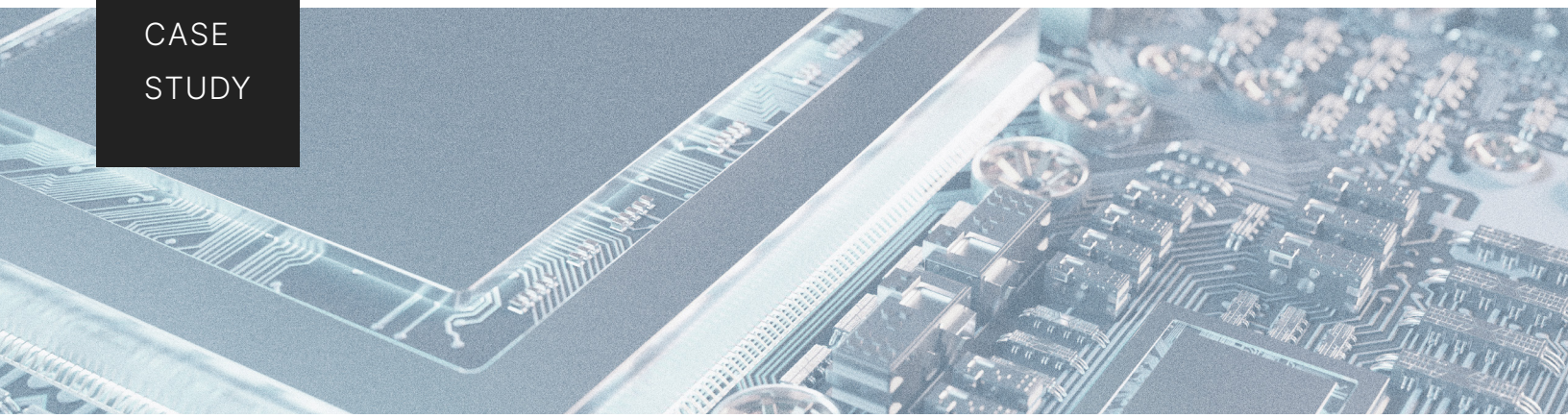
CASE STUDY



Intelligence: The Cornerstone of Toshiba's Aggressive Security Transformation

Recorded Future's intelligence powers Toshiba's advanced security strategy

TOSHIBA

Toshiba, the multinational conglomerate technology company headquartered in Japan, drives their advanced security strategy and transformation through their Cyber Security Center. At the core of the Cyber Security Center's strategy is their "intelligence-centric" approach, for which they depend on Recorded Future Intelligence Platform to help inform how they protect their business.

Manufacturers providing products and services in the digital age must strengthen security in two areas: first, information security, which protects internal systems and data to facilitate business operations; and second, product security, which enhances the security of the products and services they provide to protect customers and partners to defend against cyber attacks.

Given Toshiba's wide range of businesses operating globally, including manufacturing, energy, infrastructure-related systems, and electronic devices, they have seen the need to bolster their security posture. The company established the Cyber Security Center in 2017, which is responsible for protecting their global operations from both an information and product security standpoint with a consolidated and streamlined approach to security.

Intelligence plays a critical role in this process. From the establishment of the Cyber Security Center to its current day operations, how did the company succeed in its efforts to strengthen security, including the transformation of its structure? We talked to the leaders of the Cyber Security Center to find out.

Proactive Intelligence: Essential for Risk-Based Countermeasures

Toshiba's Cyber Security Center focuses on and promotes three main objectives:

Governance, establishing regulations and guidelines, developing systems, and collaborating with external parties.

Operations, based on the concept of security lifetime protection, which consists of design and protection, monitoring and detection, response and recovery, and evaluation and verification.

Training for all Toshiba Group employees and security specialists.

With the establishment of the Cyber Security Center, Toshiba has changed its approach to be proactive "risk-based security management" basing decisions to invest in security solutions according to the level of protection a solution can provide for Toshiba's assets.

Takashi Amano,
General Manager of Cyber Security Technology Center, Toshiba

“We realized that in order to take risk-based countermeasures, we needed to shift our focus from reactive to proactive protection," recalls Takashi Amano. As a result, he came to the conclusion that "to support our proactive approach to security, we needed to invest in threat intelligence to prepare us for cyber attacks before they happen. Recorded Future’s wide coverage and volume of information led to our initial evaluation of their intelligence, and later to choosing Recorded Future as our intelligence provider.”

Kenji Kojima,
Senior Manager of Cyber Security Technology Center, Toshiba

After evaluating a range of intelligence vendors that provide IoCs (Indicator of Compromise) and threat intelligence, Toshiba chose Recorded Future. The deciding factor was Recorded Future’s superiority in both breadth of information coverage and volume of information. Kenji Kojima said, "Recorded Future accumulates a wide range of data to provide us with the most useful intelligence. Moreover, we can set alerts within the Recorded Future Intelligence Platform that trigger when specific keywords are found on the web. We most appreciated the fact that Recorded Future's intelligence has accumulated a wide range of past information and delivers relevant information based on its own engine once keywords are set.”

"Rather than handling IoC feeds such as harmful IP addresses or malware hash values in pieces, the Recorded Future Intelligence Platform presents a dashboard of IoCs tied to specific threats and the attackers who use them. We found it easy to use in that it displays a large amount of information in a structured manner, rather than in isolation," Kojima said.

In parallel to the introduction of Recorded Future, the Cyber Security Center established a team of analysts to utilize intelligence. The analyst team helps to respond to inquiries from the Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT), which are responsible for incident response in the field.

Intelligence also contributes to two-way collaboration, for example, when the results of dashboard investigations are given to the CSIRT, enabling them to ask deeper questions related to threats. “As we mature, we are building strong processes around intelligence, digging deeply into our alerts with the help of relevant threat intelligence," Kojima said.

The Cyber Security Center also uses Recorded Future’s Brand Intelligence solution to ascertain whether any intellectual property or confidential information related to Toshiba has been leaked on the dark web, and gather context around that leak. By setting keywords such as the Toshiba brand name, alerts fire to notify the Cyber Security Center when relevant information has been detected.

Strengthening global governance and raising the level of security across Toshiba’s entire group of companies is also a major challenge that the Cyber Security Center is addressing with intelligence. The Chief Information Security Officers (CISOs) of Toshiba Group companies meet regularly to share company-wide threat trends obtained through intelligence and to communicate with the CSIRTs of individual companies regarding alerts related to their own operations. Kojima says, "We have been able to achieve a good balance between top-level information sharing and field-level information sharing.”

"Intelligence-centric" Security in Combination with SOAR

The Cyber Security Center aims to be an "intelligence-centric" operation that detects and responds to threats by collecting a variety of internally available logs and event information in addition to external threat information from the Recorded Future Intelligence Platform (***see Figure 1***).

Automation of incident response through a Security Orchestration, Automation and Response (SOAR) has been critical to the Cyber Security Center’s operations. Toshiba has integrated intelligence into their SOAR and utilizes it in the Security Operation Center (SOC) and CSIRT, which monitor Toshiba Group's security.

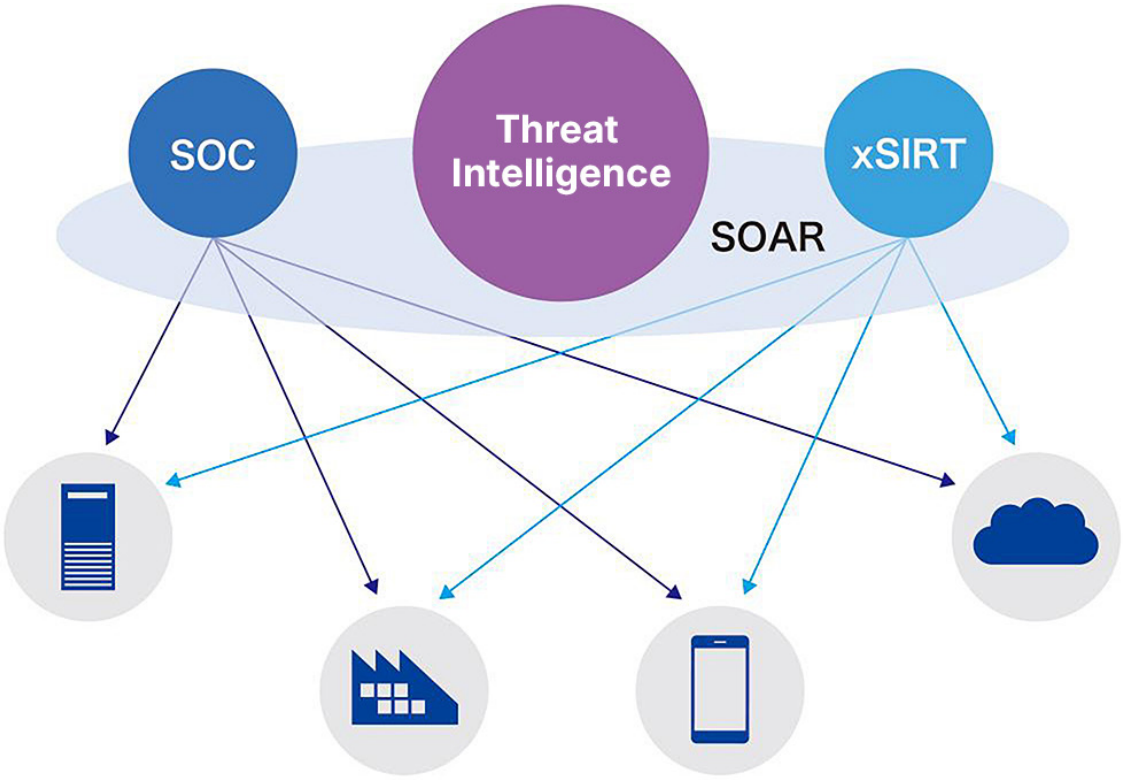


Figure 1. *Diagram showing how Toshiba's Cyber Security Center's security operations function with intelligence at its core (**Source:** Toshiba Corporation)*

By automating the process of obtaining and enriching threat information and incorporating threat intelligence into the process, Toshiba is attempting to turn tacit knowledge of personnel into formal knowledge and achieve intelligence-centric operations.

Incident handling tends to rely on personal knowledge and abilities. When a device alerts, it is necessary to examine the reputation and risk of the IP address communicating with that device, and to check for devices or suspicious processes communicating with the same IP address.

To support this response, Toshiba augments their SOAR through an API (application programming interface) with their Recorded Future integration. By automating the process of obtaining and enriching threat information and incorporating threat intelligence into the process, Toshiba is attempting to turn tacit knowledge of personnel into formal knowledge and achieve intelligence-centric operations. For example, when handling an incident, experienced personnel used to have to search for the necessary information themselves, but after switching to a system that automatically retrieves relevant threat information, the need for such work, which requires reliance on human skills, was reduced.

Amano has noticed that "Recorded Future's intelligence has reduced the time required to respond to incidents. In the future, we plan to visualize the effects and quantify the effectiveness of using intelligence to prevent damage before it occurs, and present this information to management."

Becoming a "Trusted Partner" Through Enhanced Product Security

Toshiba's Cyber Security Center's leaders are also enthusiastic about various future applications of Recorded Future's intelligence in their security infrastructure. The company plans to integrate Recorded Future with their Endpoint Detection and Response (EDR) solution, which has been introduced globally, to visualize the status of devices through EDR and compare it with threat intelligence, thereby enabling a comprehensive understanding of potential threats and the presence of malware.

Further, Toshiba expects that intelligence will be used in a wider range of situations in zero-trust security, which is being implemented in phases. As the transition from perimeter defense to zero-trust security progresses, the number of targets to be monitored by their SOC, including authentication, will increase. "In the transformation from perimeter security to zero-trust security, we will consider how to best make use of intelligence," said Amano.

A key initiative unique to the manufacturing industry, the company intends to use intelligence not only to protect its internal infrastructure, but also to protect the products and services it provides to its corporate customers. "There is a possibility that we ourselves will have to become intelligence providers for Toshiba's products and services," said Amano.

Toshiba is developing an internal vulnerability management platform to manage which products and services are affected by vulnerabilities discovered on a daily basis. By utilizing the Vulnerability Intelligence provided by Recorded Future, Toshiba intends to build a system that not only confirms the existence of vulnerabilities, but also prioritizes them based on risk scores.

From left to right: Mr. Kojima, Mr. Amano

The manufacturing industry is facing a major turning point. Toshiba is also working to promote digital transformation (DX) and increase corporate value by combining its manufacturing technology and experience with the latest technologies. To do so, the foundation of trust is essential.

Amano expresses trust using the formula "value divided by risk.” This means that trust can be enhanced not only by increasing value, but also by reducing risk. “We want to strengthen trust by increasing value and reducing risk at the same time," said Amano. “In an age when we are connected to our customers and partners in the digital world, what is most important is trust. We will continue to strive to enhance Toshiba's value as a connected partner through continued investment in security measures," said Amano.