Recorded Future®

CASE STUDY

Okinawa Institute of Science and Technology Protects Education Excellence with Security Intelligence

Okinawa Institute of Science and Technology (OIST) is a graduate university located in Okinawa Prefecture, Japan, that is rapidly gaining recognition in the worldwide academic community as a model for excellence in education and research.

USE CASE

- SIEM alert triage and threat detection

CHALLENGE

- Resource constraints and limited access to external threat data create security blind spots

SOLUTION

- Security Intelligence integrated into IBM® Security QRadar® Security Information and Event Management (SIEM)

OUTCOMES

- 3-4x improvement in security monitoring accuracy and operational efficiency
- 25% reduction of false positive QRadar® offenses

Higher Ed is a High-Value Target

Universities maintain a wealth of sensitive data – from valuable research to protected health information. A security breach can result in severe consequences that ripple far beyond an institution's walls.

"One of my main objectives is to detect and respond to threats in real time, while providing a flexible IT environment for research staff," explains OIST chief information security officer Keita Nagase. "This dual pursuit of effective security systems and speed is a priority."

The team relies on an IBM® Security QRadar® SIEM system to detect and correlate security event logs across the University's security stack — comprising vulnerability management, penetration testing, and intrusion detection systems and other tools — however, they lacked visibility into external context on the threats that could be targeting them.

"With so many security events coming out of the SIEM, it was difficult to determine which ones presented critical risk," he explains. **"Our internal team doesn't have the resources or specialized expertise to collect and analyze every relevant threat. Our challenge was to improve our threat detection capabilities and prioritize threats with a greater degree of accuracy."**

> "Today, security intelligence from Recorded Future is an indispensable part of our security operations. It improves the quality of analysis in security monitoring, aids in information sharing, and serves as a repository of intelligence for incident response,"
>
> *Keita Nagase*
> *Chief Information Security Officer*

Photo: OIST/Kenji Togo

Real-Time Security Intelligence Drives Automation and Balances Resource Constraints

"Recorded Future's ability to enrich SIEM data, along with its accessibility to closed sources and dark web forums, drove our interest," says Mr. Nagase. **"But the quality of information and advanced automation capabilities were what ultimately led us to select the platform over a managed security operations service."**

The Recorded Future Security Intelligence Platform combines analytics with human expertise to unite an unrivaled variety of open source, dark web, technical sources, and original research. A seamless integration with QRadar enables the OIST team to:

- Correlate and enrich QRadar offenses with external threat data, significantly reducing time to verdict
- Proactively block threats using Recorded Future intelligence in correlation rules
- Enhance threat hunting capabilities via on-demand enrichment of IPs, domains, hashes, and vulnerabilities
- Automate processes to streamline workflows and boost team efficiency and confidence

Full Visibility, Streamlined Operations and Executive-Level Support

"Today, security intelligence from Recorded Future is an indispensable part of our security operations. It improves the quality of analysis in security monitoring, aids in information sharing, and serves as a repository of intelligence for incident response," says Mr. Nagase.

> "Stakeholders have been impressed by our ability to make threat intelligence actionable with Recorded Future's reports and detailed cyber threat information and analysis."
>
> *Keita Nagase*
> *Chief Information Security Officer*

He continues, "We have access to a much broader set of external threat sources that we didn't have before due to tool and resource limitations. **By integrating intelligence into our existing IBM® Security QRadar® system and workflows, and automating analysis, we believe we have improved the accuracy and operational efficiency of security monitoring by a factor of three to four."**

University leadership has taken notice. **"Stakeholders have been impressed by our ability to make threat intelligence actionable with Recorded Future's reports and detailed cyber threat information and analysis."** With these insights, Mr. Nagase and team can report on the impact of similar attacks in the industry, cite trends from the dark web that often indicate whether the University is likely to be targeted by cybercriminals, and respond quickly, and with confidence, to disrupt adversaries.