CASE STUDY

ULTRARED

HOW JST STRENGTHENED SECURITY POSTURE AND MAINTAINED COMPLIANCE WITH ULTRA RED

Empowering Science, Inspiring Futures

Japan Science and Technology Agency (JST)

Industry: Government / Research & Innovation
Headquarters: Saitama, Japan
Employees: 1,546 (as of April 2025)
Website: www.jst.go.jp/EN/

For Japan, a country driven by science and technology, enhancing research and development capabilities has become a critical national priority. Faced with global challenges such as climate change, resource and energy shortages, food insecurity, and pandemics, the nation increasingly relies on scientific innovation to deliver effective solutions.

The **Japan Science and Technology Agency (JST)** plays a central role in this mission. Acting as a catalyst for innovation, JST funds diverse R&D projects, conducts policy-driven research, and promotes public understanding of science and technology.

KEY CHALLENGES

JST operates hundreds of critical information systems supporting national research and innovation. As a government agency, it must comply with Japan's **"Unified Cybersecurity Standards for Government Agencies"** while defending against increasingly sophisticated cyberattacks.

Frequent, high-volume attacks
As a major R&D funding body, JST is a high-value target for advanced cyber threats.

Compliance pressure
Government mandates require JST to meet strict security standards, continuously updated to reflect the latest attack trends.

Manual testing bottlenecks
Testing cycles for hundreds of systems stretched to **2–3 years,** resulting in infrequent assessments of individual systems.

Emerging attack surfaces
Growth in cloud adoption and external-facing assets created additional blind spots.

JST was conducting vulnerability assessments and penetration tests manually even before unified standards mandated them. However, with hundreds of systems under its management and diverse business operations, testing frequency soon became inconsistent. Tests were typically run sequentially, and completing a full cycle for all systems often took two to three years. It became clear that this approach was not sustainable.

GOAL

JST aimed to modernize its security testing and adopt an **"attacker's-eye view"** of its digital environment to:

- **Continuously identify and validate** vulnerabilities in real time.
- **Automate penetration testing** to shorten testing cycles from years to days.
- **Ensure compliance** with government cybersecurity standards.
- **Improve collaboration** between security teams and system owners to remediate issues quickly.

> **Security controls are essential to protect JST's mission, but our goal is also to maximize research efficiency. We needed a solution that balances both."**
>
> ***Tsutomu Kurosawa, JST***

EVALUATION OF SOLUTIONS

In November 2023, JST conducted a PoC, looking for a solution capable of:

- Automating penetration testing and exposure validation.
- Simulating **real-world attacker techniques** at high frequency.
- Integrating latest threat intelligence to detect emerging risks.
- Scaling across hundreds of systems with minimal operational burden.

After a comprehensive evaluation of proposals from multiple vendors, **ULTRA RED** was selected, as it was determined to meet the requirements defined in the government agency's unified standards, leading to its adoption following a formal bidding process.

> **ULTRA RED met our key requirements and provided a unified platform, robust detection and automation capabilities."**
>
> ***Tsutomu Kurosawa, JST***

WHY ULTRA RED

ULTRA RED was chosen for its ability to deliver a **Continuous Threat Exposure Management (CTEM)** program through an agentless SaaS platform that integrates three essential capabilities:

1 EASM

External Attack Surface Management

Continuously discovers and monitors exposed IT assets.

2 ABAS

Automated Breach & Attack Simulation

Runs realistic penetration tests based on the latest attack techniques.

3 CTI

Cyber Threat Intelligence

Continuously updates testing techniques to reflect emerging attacker behaviors.

SELECTION CRITERIA FULFILLED BY ULTRA RED:

- ☑ **Daily testing and exposure validation** across all monitored domains.
- ☑ **Meets key requirements** of the Japanese government cybersecurity standards.
- ☑ **Threat-driven simulations** with continuously updated attack patterns.
- ☑ **Clear risk prioritization** and actionable remediation guidance.

IMPLEMENTATION

PROJECT START:

November 2023 – PoC completed successfully.

DEPLOYMENT:

ULTRA RED was rolled out in **July 2024.**

FREQUENCY:

Weekly automated intrusion simulations, expanding toward continuous testing.

PROCESS INTEGRATION:

- ULTRA RED integrates with JST's existing SOC, CSIRT, and security workflows.
- Results are shared directly with system owners for rapid remediation.
- Dashboards provide real-time visibility into vulnerabilities and threat exposures.

> **ULTRA RED highlights vulnerabilities, ranks them by business risk, and facilitates collaboration between security and system owners."**
>
> ***Satoshi Yanagida, Systems Lead, JST***

OUTCOMES & BENEFITS

By implementing automated testing, JST was able to reduce operational costs while strengthening its overall security posture — without the need to expand its team. According to Tsutomu Kurosawa, replicating ULTRA RED's testing coverage manually would have required enormous resources, and the solution has contributed to operational efficiency within JST.

Faster Testing Cycles

- Automated simulations now run **weekly,** with capability to scale to **daily** tests.

Improved Threat Visibility

- Full mapping of external-facing assets.
- Real-time detection of vulnerabilities and exposures.

Higher Operational Efficiency

- Reduced manual workload for security teams.
- Automatic prioritization of vulnerabilities based on **business impact.**

Compliance Achieved

- JST successfully passed an external audit.
- ULTRA RED supports JST's efforts to stay aligned with Japan's evolving security standards.

LOOKING AHEAD

JST is exploring further use of technologies such as **VITA AI,** an AI-powered security assistant designed to:

- Accelerate detection and classification of threats.
- Automate analysis and response prioritization.
- Further reduce mean time to remediation (MTTR).

AT A GLANCE

BEFORE ULTRA RED	WITH ULTRA RED
○ Manual testing, inconsistent cycle	☑ Automated scanning, weekly (scalable to daily)
○ 2–3 years per testing cycle	☑ Continuous testing, real-time insights
○ No risk prioritization	☑ Threats prioritized by business impact
○ Limited attack coverage	☑ Constantly updated attack scenarios
○ High costs expected	☑ Lower cost, high ROI