CASE STUDY

ULTRARED

HOW OPEN HOUSE GROUP SECURES ITS EXPANDING ATTACK SURFACE WITH ULTRA RED

OPEN HOUSE GROUP

Open House Group Co., Ltd.

Head Office: Tokyo, Japan
Founded: 1997
Industry: Real Estate, Property Investment
Website: openhouse-group.co.jp

Background

Open House Group is a leading real estate company based in Tokyo, Japan, with operations spanning residential development, property investment, and financing. Since its founding in 1997, the company has grown rapidly through acquisitions and partnerships, reaching over 1 trillion yen in annual revenue by 2023.

This growth has introduced an increasingly complex IT landscape. With numerous subsidiaries operating across different environments, maintaining visibility and control over the group's digital footprint has become a growing challenge. Recognizing the rising risk of external threats and the need to stay ahead of attackers constantly scanning for vulnerabilities, Open House Group turned to ULTRA RED to help reduce its attack surface across the entire group.

Challenges

- Limited visibility across subsidiaries
- Unintentional exposure of assets during frequent infrastructure changes
- Difficulty prioritizing and mitigating threats in a complex environment

Outcomes

- Increased asset visibility and control
- Clear risk prioritization
- Improved collaboration across teams
- Faster threat triage and remediation

Use Cases

- Attack surface management
- Continuous monitoring and risk reduction
- Compliance with government security guidance

The Need for Attack Surface Management

As part of its digital transformation efforts, Open House Group has embraced cloud technologies and a zero trust security model. But rapid growth through mergers and acquisitions created a fragmented and complex IT environment. A wake-up call came when an internal test environment was externally accessed just days after setup — highlighting how quickly attackers can exploit exposed assets.

Motivated by this incident and the 2023 attack surface management guidelines published by Japan's Ministry of Economy, Trade and Industry, Open House Group launched a proactive strategy to improve visibility and reduce external risk.

Selecting ULTRA RED: Going Beyond Vulnerability Detection

Open House Group began exploring attack surface management solutions in 2020, but the 2023 guidelines from Japan's Ministry of Economy, Trade and Industry accelerated efforts. A dedicated project team was launched in April 2024 to lead the evaluation.

After testing multiple products, the team selected ULTRA RED for its unique, validation-first approach. Unlike traditional tools that rely on CVE scores or software versions, ULTRA RED focuses on **actual attack vectors:** the specific, exploitable gaps attackers could realistically use.

WHY ULTRA RED

- **High detection accuracy**
- **Identifying vulnerabilities that other solutions miss**
- **Automated validation of exploitability**
- **Detailed proof of exploitability (PoC)**

> ULTRA RED detected vulnerabilities other products missed. Not only was the detection accuracy high, but it also stood out by **validating whether the vulnerabilities could actually be exploited** — from the attacker's point of view. It even listed specific request/response samples used in verification, offering high resolution and better understanding of the issue."
>
> *Hayato Masuzawa, Security Analyst at Open House Group.*

This attacker-centric view gave the team the clarity needed to prioritize and remediate threats faster.

CASE STUDY

ULTRARED

Implementation & Impact

Continuous Monitoring and AI-Driven Triage with ULTRA RED

Open House Group now uses ULTRA RED to monitor systems across 300 locations and over 14 group companies. By prioritizing risk-based attack vectors, the security team can respond faster and more effectively.

Soon after implementation, ULTRA RED flagged an exposed internal subdomain in an exploitable state. The team quickly worked with the relevant department to fix it — a reminder of the risks tied to forgotten or legacy assets and the need for continuous monitoring.

With varying security maturity across subsidiaries, gaining visibility across the group is critical. ULTRA RED helps surface unknown or untracked assets and validate real risk automatically.

"ULTRA RED's continuous asset discovery has been a huge advantage — helping us uncover related domains and associated risks across a complex environment."

Hear It From the Customer
Watch the Video!

The team also leverages **VITA AI, ULTRA RED's generative AI assistant,** to speed up triage and improve communication across teams — enabling faster, more informed responses.

Looking Ahead:

Strengthening Security with ULTRA RED

At Open House Group, security is seen as an ongoing, company-wide effort. The team plans to expand use of ULTRA RED's CTEM platform beyond the core security team — fostering shared responsibility across departments.

As the business grows in size and complexity, Open House Group will continue leveraging ULTRA RED to cover more areas, including cloud posture management and brand/domain protection — helping the company stay ahead of evolving threats while supporting secure growth.

Discover What ULTRA RED Can Do for You — Book a Free Demo.

About ULTRA RED

ULTRA RED is a pioneer and leading provider of Continuous Threat Exposure Management (CTEM) solutions, built on a validation-first approach. Our CTEM platform helps security teams confidently reduce threat exposure by continuously identifying, validating, and prioritizing gaps across the entire attack surface. Learn more at **www.ultrared.ai**.