CASE STUDY

ULTRARED

FOCUSING ON REAL ATTACK VECTORS MISSED BY TRADITIONAL VULNERABILITY MANAGEMENT

パーソル キャリア
PERSOL

PERSOL CAREER

Industry: Recruitment services & HR consulting
Headquarters: Tokyo, Japan
Founded: 1989
Website: www.persol-career.co.jp

PERSOL CAREER is a core company within the PERSOL Group (Japan) focused on HR and career services. With the mission "Empowering people to own their work," PERSOL CAREER provides a wide range of services including job placement, recruitment advertising, and new graduate hiring support. The company operates popular services such as the career-change platform **"doda"** and high-level recruitment service **"doda X."**

In response to the rising tide of cyberattacks, the company has been implementing various security measures, such as vulnerability assessments, patch management, and installation of security appliances. However, recognizing the importance of understanding the *real risks* present in live operational environments, the company decided to adopt **ULTRA RED.**

INTRODUCTION

Any publicly facing asset can become an attacker's initial entry point

Even with initiatives to strengthen system security — including vulnerability assessments, patch management, and security device deployment — it's difficult to ensure comprehensive coverage for all publicly accessible assets. Assets not listed in management inventories — such as independently published sites by overseas branches or temporary campaign sites — can easily be overlooked, leaving them outside the scope of existing security measures. Mr. Atsuo Sakurai, responsible for IT security strategy and implementation at PERSOL, had recognized that they were continuing operations without fully grasping what kinds of security risks existed in real environments, which gave him a strong sense of urgency.

> **From an attacker's perspective, it doesn't matter whether administrators have proper management in place or even know about the asset — any externally exposed asset can be a target for initial intrusion. If attackers can reach critical assets afterward, the initial entry point doesn't need to hold sensitive data directly. That's reason enough for attackers to exploit it."**
>
> ***Mr. Sakurai***

Sakurai began considering what to prioritize:

> **We should certainly strive to bring existing security measures as close as possible to 100%, but it's unrealistic to achieve complete coverage or maintain it daily. Instead, I decided that we should prioritize understanding the *actual risks* in the operational environment — including both known and unknown assets, regardless of whether vulnerability management or publication intent exists."**
>
> ***Mr. Sakurai***

ASM COULDN'T FULFILL WHAT WE NEEDED.

With general ASM, only a part of what you want to do can be realized

Initially, Sakurai thought of **ASM (Attack Surface Management)** solutions and began evaluating several. However, he soon noticed limitations.

According to the Ministry of Economy, Trade and Industry's guidelines, ASM frameworks typically include:

Discovery → **Information Gathering** → **Risk Assessment** → **Risk Response**

While this seemed aligned with their goals, the guidelines also noted that some tools only *collect OS/software version data and display potential vulnerabilities based on that,* rather than verifying actual vulnerabilities.

> **Typical ASM tools point out exposed version information and list possible CVEs associated with them — but that's about it. They don't test whether the vulnerability can actually be exploited, and vulnerabilities without version data remain undetected."**
>
> ***Mr. Sakurai***

Even if software has known vulnerabilities, exploitation often depends on specific configurations or enabled services. Without executing real attack code, it's impossible to confirm if the vulnerability is exploitable. Moreover, ASM tools relying on version info cannot detect vulnerabilities in internally developed applications, and application-layer weaknesses are often out of scope.

> **In short, most ASM platforms assess risks without confirming whether actual attacks would succeed. But attackers don't care whether a flaw is in the OS, middleware, or application — if it's exploitable, it's a valid entry point. Through our research, we found that ASM tools couldn't fully achieve what we wanted to do."**
>
> ***Mr. Sakurai***

SELECTION CRITERIA

Beyond Vulnerability Detection: Real Cyberattack Simulation

Sakurai then clarified the goal: to continuously detect and respond to exploitable vulnerabilities across *all* externally exposed assets — regardless of whether they were known or unknown, or which layer (OS, application) they existed on — by testing under the same conditions as real external attackers. The focus was on identifying and eliminating attack risks that could slip through existing vulnerability and patch management processes.

Through proof-of-concept trials, **ULTRA RED** emerged as the best fit.

What particularly impressed Sakurai was **ULTRA RED's "Automated Breach & Attack Simulation (ABAS)",** which performs simulated cyberattacks using actual exploit code. This allows risks to be quantified and prioritized effectively.

USING ULTRA RED TOGETHER WITH VULNERABILITY ASSESSMENTS

How does ULTRA RED differ from penetration testing or vulnerability assessments that also perform attacks? PERSOL CAREER compared them internally (see Fig. 1).

FIGURE 1. ULTRA RED VS. GENERAL ASM VS. VULNERABILITY ASSESSMENT

CATEGORY	ULTRA RED	GENERAL ASM	VULNERABILITY ASSESSMENT
Asset Discovery	Yes	Yes	No
Attack Verification	Yes	No	Yes
Detection Method	Version info + attack verification	Primarily version information	Version info + attack verification
Frequency	Daily *(configurable)*	Daily *(configurable)*	Ad hoc or periodic
Scope	All discovered assets	All discovered assets	Only assets specified by the customer
Coverage Layer	OS / Middleware / Application	OS / Middleware	OS / Middleware / Application
Pre-configuration Required	Generally not required	Generally not required	WAF / IPS exclusion settings, test environments, test IDs required
Manual Deep Dive	No	No	Yes *(service-dependent)*

> **ULTRA RED conducts verification using real attack code and covers the application layer as well, aligning much more closely with our objectives,"**
>
> ***Mr. Sakurai***

While traditional vulnerability assessments can determine whether a vulnerability exists, they typically require specifying targets — meaning unknown assets are excluded.
However, Sakurai still recognizes the advantages of manual, in-depth assessments:

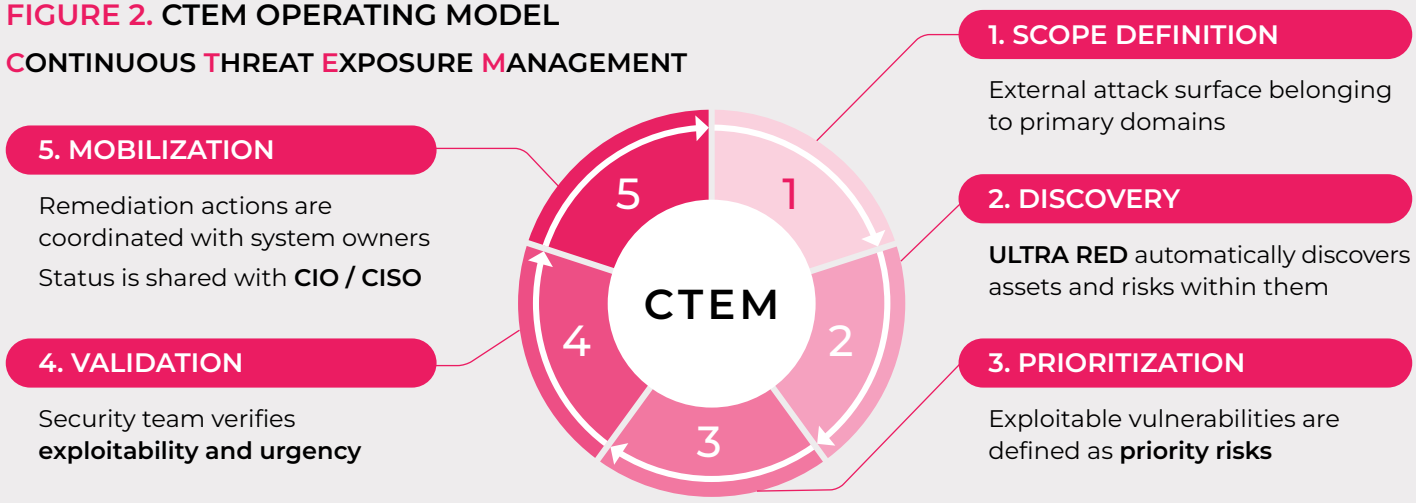
> **We don't consider ULTRA RED a replacement for vulnerability assessments. We plan to continue both — using ULTRA RED to quickly address the most urgent risks in parallel."**
>
> *Mr. Sakurai*

OPERATING WITHIN THE CTEM FRAMEWORK

ULTRA RED was initially applied in a small-scale rollout, targeting only PERSOL CAREER's key domains. The focus is on identifying assets and risks, then prioritizing those with confirmed successful attack scenarios.
Operations are aligned with the **CTEM (Continuous Threat Exposure Management)** framework (see Fig. 2):

FIGURE 2. CTEM OPERATING MODEL

CONTINUOUS THREAT EXPOSURE MANAGEMENT



> **We don't open ULTRA RED directly to system administrators. Instead, our security team logs in daily, reviews findings, and if an actually exploitable vulnerability is detected, we immediately notify the system management team — treating it with the same priority as a system outage."**
>
> *Mr. Sakurai*