CYCRAFT

User Case of Education:

Advanced Network and Cybersecurity Laboratory of Kyushu University

Preface

Preemptive Defense: Strengthening Academic Research and Cybersecurity Structure with Attack Surface Management

With the rapid evolution of AI, the methods and scale of cyberattacks have become increasingly complex and sophisticated. For defenders, this necessitates a shift from traditional "reactive detection and response" to "predictive defense," an approach that adopts an attacker's perspective to identify and mitigate risks in advance. A fundamental concept of this preemptive defense is Attack Surface Management (ASM), which provides visibility into external assets and their associated risks.

In recent years, the Japanese government has been promoting measures to strengthen cybersecurity, including external network environments. For instance, the Ministry of Economy, Trade and Industry (METI) has released ASM-related guidelines, positioning it as a foundational measure for organizational cybersecurity management. Furthermore, the Ministry of Education, Culture, Sports, Science and Technology (MEXT), in its "Information Security Policy Guidelines for Educational Settings," (教育情報セキュリティポリシーに関するガイドライン) noted that risks faced by educational institutions are no longer confined to internal systems. These risks now encompass public domains, services, and research systems, emphasizing the importance of digital asset inventory and vulnerability management—concepts that align directly with ASM.

Based on these technological trends and policy regulations, higher education institutions like universities—which manage numerous research units and decentralized IT systems—find that maintaining continuous visibility of assets and risks from an external perspective is not only vital for strengthening defense but is also becoming a cornerstone for the credibility of research and education.

Background

Cybersecurity Governance in Open Academic Environments

Due to the diverse needs of academic research, university campus networks are often more complex and fragmented than corporate environments. Take Kyushu University, a leading Japanese national university, as an example: the campus manages over 2,000 FQDNs (Fully Qualified Domain Names). Almost all domains are managed independently by individual colleges and laboratories, resulting in highly decentralized systems. While this architecture fosters flexibility for research and education, it makes it difficult for cybersecurity administrators to maintain real-time visibility of the overall exposure. This expands the External Attack Surface, creating blind spots that can become breaches in the institution's cyber resilience.

Moreover, for higher education institutions, cybersecurity risk is not just an IT department issue; it can cause substantive disruption to research and teaching. A major challenge in cybersecurity education and research is how to accurately inventory observable risks, and even allow students and researchers to interact with real-world vulnerabilities, without infringing on internal systems, disrupting academic activities, or hindering existing operations.

To address this, Professor Koji Okamura (岡村耕二), the CISO of Kyushu University and head of the Advanced Network and Cybersecurity Laboratory (先端ネットワーク研究室), introduced CyCraft's XCockpit EASM solution primarily for research purposes. This initiative aims to apply professional security tools within an academic setting, bridging the gap between theoretical research and practical campus defense.

Implementation Scenarios

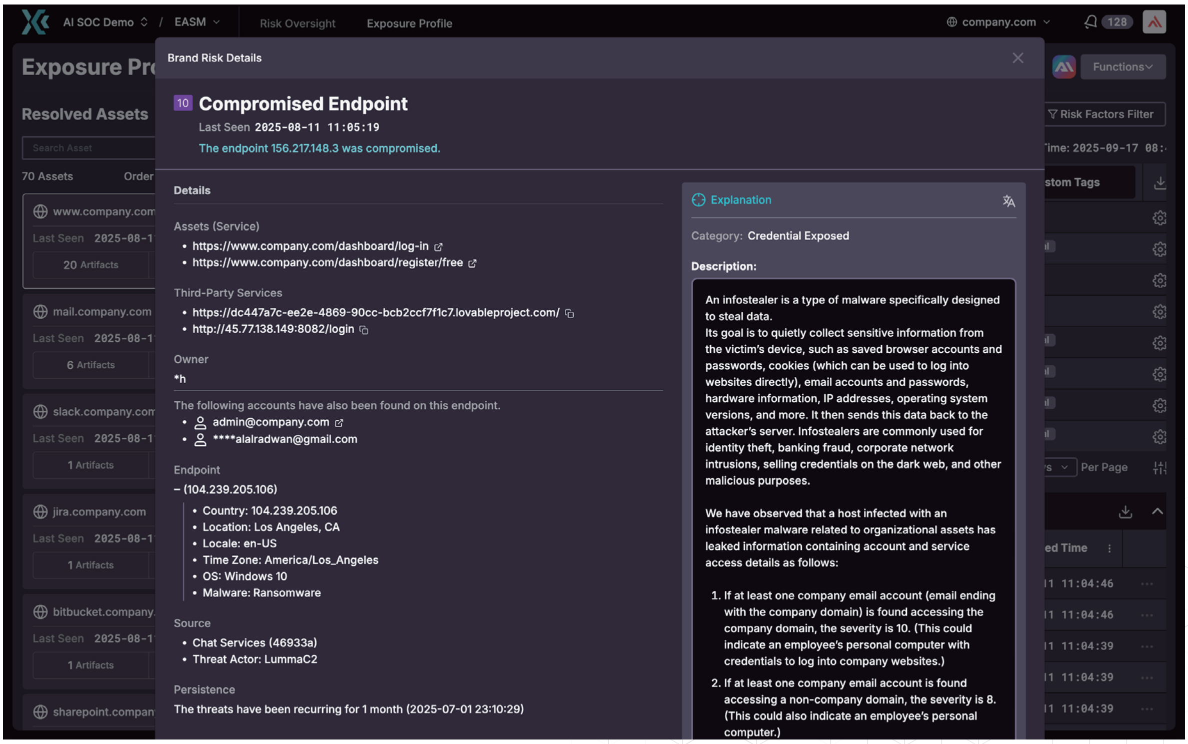
Real-World Applications: "Seeing" Cybersecurity Risks

By implementing XCockpit EASM as a research tool, students in the laboratory can observe and interact with real-world vulnerability data within the university's domains, moving beyond abstract concepts. This data has become essential material for academic theses. Several students in the Advanced Network Laboratory have already utilized XCockpit EASM data as the analytical foundation for their graduate projects or master's theses. Research topics include "Prioritizing Vulnerability Response via Diverse Evaluation Methods," "Transforming Decentralized Big Data into Intuitive Visualizations," and "Classifying and Consolidating Risks Related to Certificates."

CyCraft's XCockpit automatically scans four major categories of digital assets: Domains, URLs, IPs, and accounts. From asset inventory and risk quantification to supply chain management, it provides a comprehensive grasp of an organization's external exposure. Furthermore, XCockpit utilizes non-intrusive, agentless collection technology, ensuring no interference or additional load on research networks or system operations. This allows users to obtain authentic attack surface intelligence without impacting academic activities—a significant advantage for educational settings that prioritize system stability and research ethics.

According to Professor Okamura, students log into the XCockpit platform almost daily for data verification and analysis. By engaging with actual vulnerabilities within their own university's network, their understanding of exposure, vulnerabilities, and severity is no longer limited to textbooks. They gain a profound understanding of the complexity of real-world risks. This process of interacting with real vulnerabilities under safe conditions is crucial training for students transitioning from theory to practice.

> *"XCockpit is a SaaS product; you simply get an account, change the password, and set up MFA to start. The onboarding is incredibly lightweight. Even though this was our first time using an ASM product, the manuals and Academy videos provided by CyCraft made it easy to visualize the system's output, which was very helpful for initial understanding. The interface is intuitive—once you know what information is available, it's very easy to use. Even students without prior practical security experience found no technical barrier to entry."*
>
> ***— Professor Koji Okamura, CISO of Kyushu University***



Brand Risk Details

10 **Compromised Endpoint**

Last Seen 2025-08-11 11:05:19

The endpoint 156.217.148.3 was compromised.

Details

Assets (Service)

- https://www.company.com/dashboard/log-in
- https://www.company.com/dashboard/register/free

Third-Party Services

- https://dc447a7c-ee2e-4869-90cc-bcb2ccf7f1c7.lovableproject.com/
- http://45.77.138.149:8082/login

Owner

*h

The following accounts have also been found on this endpoint.

- admin@company.com
- ****alalradwan@gmail.com

Endpoint

– (104.239.205.106)

- Country: 104.239.205.106
- Location: Los Angeles, CA
- Locale: en-US
- Time Zone: America/Los_Angeles
- OS: Windows 10
- Malware: Ransomware

Source

- Chat Services (46933a)
- Threat Actor: LummaC2

Persistence

The threats have been recurring for 1 month (2025-07-01 23:10:29)

Explanation

Category: Credential Exposed

Description:

An infostealer is a type of malware specifically designed to steal data.
Its goal is to quietly collect sensitive information from the victim's device, such as saved browser accounts and passwords, cookies (which can be used to log into websites directly), email accounts and passwords, hardware information, IP addresses, operating system versions, and more. It then sends this data back to the attacker's server. Infostealers are commonly used for identity theft, banking fraud, corporate network intrusions, selling credentials on the dark web, and other malicious purposes.

We have observed that a host infected with an infostealer malware related to organizational assets has leaked information containing account and service access details as follows:

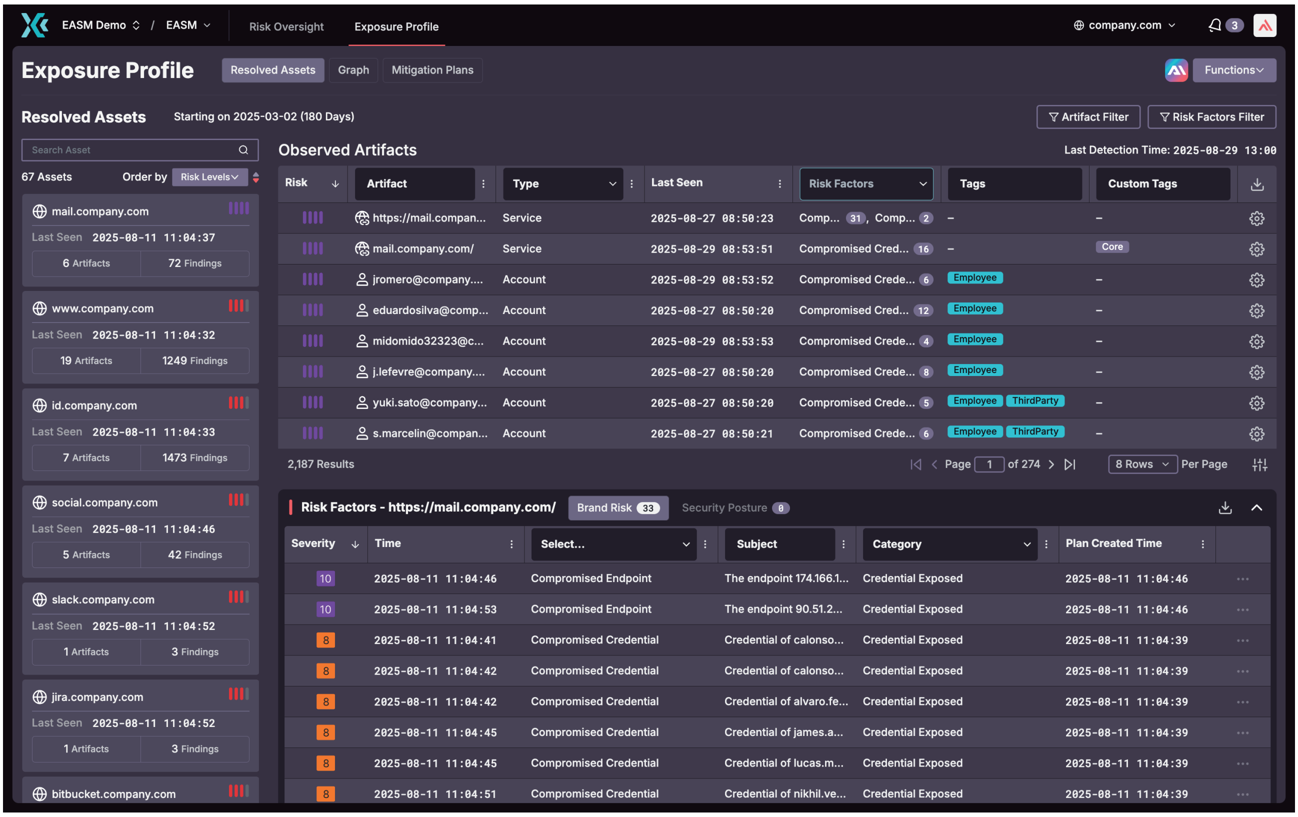
1. If at least one company email account (email ending with the company domain) is found accessing the company domain, the severity is 10. (This could indicate an employee's personal computer with credentials to log into company websites.)
2. If at least one company email account is found accessing a non-company domain, the severity is 8. (This could also indicate an employee's personal computer.)

Leveraging XCockpit EASM to monitor real-world vulnerabilities in support of academic research and education.

Synergy Between Research and Campus Cybersecurity Governance

Beyond providing vulnerability or weakness data for the laboratory, another key value XCockpit EASM brings to Kyushu University is visibility into Dark Web leaks. The Dark Web hides in grey zones where leaked credentials, account data, and confidential information are traded—often serving as the initial entry point for attackers. XCockpit EASM automatically monitors multiple Dark Web sources to identify potential threats. Professor Okamura noted that Dark Web intelligence, such as leaked IDs related to the university, is a highly valuable source that was previously difficult to obtain. This was one of the primary features that initially drew him to CyCraft's solution.

To maintain the boundary between research and practice and adhere to risk control principles, Dark Web data is not accessible to students. Instead, Professor Okamura, in his capacity as CISO, collaborates directly with the university's incident response center to hand over this intelligence for investigation and remediation. In this model, the laboratory focuses on analyzing vulnerabilities for research, while Dark Web monitoring serves as a critical reference for the university's governance and incident response. This clear division of labor ensures that XCockpit EASM supports both educational and the institution's actual security framework. Currently, the Kyushu University CSIRT is actively evaluating the formal adoption of XCockpit EASM to further strengthen campus-wide resilience.



Resolved Assets Starting on 2025-03-02 (180 Days)

67 Assets

mail.company.com
Last Seen 2025-08-11 11:04:37
6 Artifacts 72 Findings

www.company.com
Last Seen 2025-08-11 11:04:32
19 Artifacts 1249 Findings

id.company.com
Last Seen 2025-08-11 11:04:33
7 Artifacts 1473 Findings

social.company.com
Last Seen 2025-08-11 11:04:46
5 Artifacts 42 Findings

slack.company.com
Last Seen 2025-08-11 11:04:52
1 Artifacts 3 Findings

jira.company.com
Last Seen 2025-08-11 11:04:52
1 Artifacts 3 Findings

bitbucket.company.com

Observed Artifacts

Last Detection Time: 2025-08-29 13:00

Risk	Artifact	Type	Last Seen	Risk Factors	Tags	Custom Tags
	https://mail.compan...	Service	2025-08-27 08:50:23	Comp... 31, Comp... 2	–	–
	mail.company.com/	Service	2025-08-29 08:53:51	Compromised Cred... 16	–	Core
	jromero@company....	Account	2025-08-29 08:53:52	Compromised Crede... 6	Employee	–
	eduardosilva@comp...	Account	2025-08-27 08:50:20	Compromised Cred... 12	Employee	–
	midomido32323@c...	Account	2025-08-29 08:53:53	Compromised Crede... 4	Employee	–
	j.lefevre@company....	Account	2025-08-27 08:50:20	Compromised Crede... 8	Employee	–
	yuki.sato@company...	Account	2025-08-27 08:50:20	Compromised Crede... 5	Employee ThirdParty	–
	s.marcelin@compan...	Account	2025-08-27 08:50:21	Compromised Crede... 6	Employee ThirdParty	–

2,187 Results Page 1 of 274 8 Rows Per Page

Risk Factors - https://mail.company.com/ Brand Risk 33 Security Posture 0

Severity	Time	Select...	Subject	Category	Plan Created Time
10	2025-08-11 11:04:46	Compromised Endpoint	The endpoint 174.166.1...	Credential Exposed	2025-08-11 11:04:46
10	2025-08-11 11:04:53	Compromised Endpoint	The endpoint 90.51.2...	Credential Exposed	2025-08-11 11:04:46
8	2025-08-11 11:04:41	Compromised Credential	Credential of calonso...	Credential Exposed	2025-08-11 11:04:39
8	2025-08-11 11:04:42	Compromised Credential	Credential of calonso...	Credential Exposed	2025-08-11 11:04:39
8	2025-08-11 11:04:42	Compromised Credential	Credential of alvaro.fe...	Credential Exposed	2025-08-11 11:04:39
8	2025-08-11 11:04:45	Compromised Credential	Credential of james.a...	Credential Exposed	2025-08-11 11:04:39
8	2025-08-11 11:04:45	Compromised Credential	Credential of lucas.m...	Credential Exposed	2025-08-11 11:04:39
8	2025-08-11 11:04:51	Compromised Credential	Credential of nikhil.ve...	Credential Exposed	2025-08-11 11:04:39

XCockpit EASM identifies hidden risks in the campus environment for use in investigation and remediation.

XCOCKPIT
EASM

Key Highlights of Kyushu University User Case:

> Real-World Data for Practical Research:

Labs can use live vulnerability data from campus domains as an analytical foundation, allowing students to understand risk assessment and mitigation from a practical perspective.

> Comprehensive Autonomous Asset Inventory:

XCockpit EASM provides a non-intrusive, external view to automatically inventory decentralized digital assets. No agents are required, ensuring zero disruption to campus systems while maintaining a complete attack surface profile.

> Strengthening Governance via Dark Web Monitoring:

Continuous monitoring of Dark Web markets helps the institution capture critical leak intelligence that was previously out of reach, integrating it into governance and incident response workflows.

Conclusion

Under the policy direction emphasized by MEXT, External Attack Surface Management is more than a defensive tactic—it is a foundation connecting academia, education, and governance. As seen in the case of Professor Okamura's lab at Kyushu University, XCockpit EASM serves as a powerful research aid, allowing students to engage with real-world risks without affecting operations. Simultaneously, it provides high-risk alerts, such as Dark Web leaks, to the university's security center to support decision-making and response.

Through this dual-purpose model, XCockpit EASM serves research, education, and campus governance alike. It has become a pivotal tool for academic institutions facing an ever-changing threat landscape, helping to deepen academic content while building a more resilient overall security posture.

About CyCraft

CyCraft Technology (7823.TW) — Taiwan's first AI-native cybersecurity company to list on the TWSE Innovation Board — is dedicated to automating cybersecurity with AI, shifting defense from reactive firefighting to proactive, scalable dominance. Delivering protection that is faster, easier, safer — and smarter on cost, CyCraft empowers defenders to scale. With a proven track record serving top-tier government agencies, leading financial institutions, and semiconductor giants, CyCraft is building Asia's most advanced AI-driven joint defense ecosystem — dramatically shortening dwell time, reducing breach impact, and strengthening enterprise digital resilience worldwide.

CYCRAFT
www.cycraft.com