EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 1, Bulan Juni, Tahun 2025, Hal 33-42
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i1.58567

pISSN 2615-0646
eISSN 2614-8595

Enhancing IT/OT Security Posture Against Erlang/OTP SSH Exploits Through Threat Campaign Assessment

Nabila Latifa Tullaili[1], Ridwan Satrio Hadikusuma[2], Aries Suharso[3]

[1],[3]Department of Information System, Faculty of Science and Technology, University of Singaperbangsa Karawang, Karawang, 41361, Indonesia
[2]Department of Interdisciplinary Engineering, Universitas Indonesia, Depok, Indonesia

[1]2410631250065@student.unsika.ac.id
[2]ridwan.satrio@ui.ac.id
[3]aries.suharso@unsika.ac.id

ARTICLE INFORMATION

Submitted : 06-11-2024
revised : 03-01-2025
Accepted : 05-05-2025
Published : 30-06-2025

ABSTRACT

The convergence of Information Technology (IT) and Operational Technology (OT) infrastructures exposes organizations to new risks, particularly when facing critical vulnerabilities. This research evaluates the security posture of IT/OT environments against CVE-2025-32433, a severe vulnerability in Erlang/OTP's SSH daemon that allows unauthenticated remote code execution. The assessment was conducted in a real environment using the Keysight Threat Simulator, where simulated threats were injected from the darkcloud, passed through a Palo Alto Networks firewall, and targeted a host system (Windows Server 2016) with Keysight Agent version 25.7.3-1751647889 and ATI version 25.5.4181.502994. This campaign involving seven malware scenarios using remote hosts and DNS callbacks. The results showed 43 prevention outcomes, 0 detection events, and 9 security recommendations. While the firewall prevented part of the attacks, the detection capability at the host level failed entirely, indicating potential blind spots in monitoring and response.The study concludes that proactive threat simulation is essential for identifying prevention gaps and detection weaknesses in converged IT/OT networks. Recommendations include strengthening host-based detection, improving IT/OT segmentation, and enhancing monitoring of DNS traffic to mitigate exploitation risks.

Keywords : Erlang/OTP Vulnerability; Keysight Threat Simulator; Malware Campaign; SSH Exploits; Zero Trust Security;

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 1, Bulan Juni, Tahun 2025, Hal 33-42
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i1.58567
pISSN 2615-0646
eISSN 2614-8595

INTRODUCTION

The convergence of Information Technology (IT) and Operational Technology (OT) has introduced significant advantages in terms of efficiency (Bhole et al., 2025), connectivity (Cho & Kim, 2025), and real-time monitoring within modern enterprises (Caviglia, 2025). However, this integration also creates new attack surfaces that are frequently exploited by threat actors (Lee & Choi, 2025), particularly through critical vulnerabilities in widely deployed protocols such as Secure Shell (SSH) (Azzahri et al., 2024; Mining Threat Intelligence from Billion-Scale SSH Brute-Force Attacks, 2025). One such vulnerability, CVE-2025-32433, discovered in Erlang/OTP's SSH daemon, allows unauthenticated remote code execution and has already been observed in active exploitation campaigns (Mining Threat Intelligence from Billion-Scale SSH Brute-Force Attacks, 2025).

Industries with high levels of digital transformation (Garg, 2025), including healthcare (Oyeniyi & Oyeniran, 2025), education (Cyber Security Breaches in Corporate Networks, 2025), and high technology (Metibemu et al., 2025), are particularly exposed due to weak segmentation between IT and OT systems (Kolli et al., 2024; Caviglia, 2025). This highlights an urgent need to assess and strengthen cybersecurity measures in converged environments (Framework for Assessing Information System Security Posture Risks, 2025; Dalal, 2025).

Previous studies on OT cybersecurity have primarily focused on theoretical risk assessments (Cho & Kim, 2025), patch analysis (Redavid, 2024; Bölin & Van Daele, 2024), or evaluations of intrusion detection systems (Yulianto et al., 2025). While these approaches contribute valuable insights (Nair, 2025), they often lack practical validation of how real-world attacks unfold in operational settings (Bhole et al., 2025).

In contrast, breach and attack simulation (BAS) platforms offer the capability to replicate real attack vectors and evaluate both prevention and detection mechanisms under realistic conditions (Yulianto et al., 2025). This type of proactive validation provides organizations with measurable data on their resilience against emerging threats (Ofili et al., 2025), beyond traditional vulnerability scans or penetration tests (Securing Against Advanced Cyber Threats, 2025).

Several studies have investigated the security challenges of IT/OT environments and the exploitation of SSH-based vulnerabilities. Research by Kolli et al. (2024) emphasized that weak segmentation between IT and OT systems remains a primary factor enabling adversaries to gain footholds in industrial networks. Other works, such as Bölin and Van Daele (2024), highlighted that remote code execution vulnerabilities in industrial control systems are often underreported, yet they pose significant risks due to the critical functions these systems support. With regard to SSH security, prior studies have mainly concentrated on analyzing protocol weaknesses and recommending patch management strategies (Azzahri et al., 2024) rather than demonstrating live exploitation in operational contexts. Furthermore, investigations into defense technologies such as intrusion detection and prevention systems have shown limited detection capabilities

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 1, Bulan Juni, Tahun 2025, Hal 33-42
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i1.58567
pISSN 2615-0646
eISSN 2614-8595

when attackers employ advanced persistence techniques (Yulianto et al., 2025).

In recent years, breach and attack simulation (BAS) tools have emerged as an approach to continuously validate security posture. Several authors have argued that BAS can complement penetration testing by providing automated and repeatable adversarial scenarios (Yulianto et al., 2025). However, most reported works applying BAS have been conducted in controlled laboratory settings (Nair, 2025), focusing largely on IT infrastructures while leaving OT environments underexplored (Bhole et al., 2025). This gap illustrates the need for empirical validation in realistic IT/OT scenarios, especially concerning newly disclosed vulnerabilities such as CVE-2025-32433.

Unlike earlier research, the present study contributes novelty by applying Keysight Threat Simulator to emulate real-world attack campaigns in a converged IT/OT environment, thus offering more practical insights into both prevention and detection mechanisms. By simulating live malware campaigns and analyzing both prevention and detection outcomes, this study introduces a novel perspective compared to prior works that largely remain at conceptual or laboratory scale. The findings highlight current weaknesses in IT/OT segmentation and host-based detection while providing concrete recommendations for enhancing defense strategies. This novelty bridges the gap between theoretical vulnerability analysis and real-world threat validation, offering actionable insights for organizations facing the challenges of converged IT/OT security.

RESEARCH METHODS

The research methodology followed a structured process as illustrated in the flowchart at Figure 1. The study began with an extensive review of the literature to identify the relevance of CVE-2025-32433 and its implications for IT/OT security. This step ensured a solid theoretical foundation and provided insights into existing approaches to vulnerability exploitation and defense strategies. Afterward, the topology was designed and the required hardware was installed, consisting of a physical server running Windows Server 2016 that served as the target host. On this host, the Keysight Agent version 25.7.3-1751647889 and ATI version 25.5.4181.502994 were deployed to enable communication with the Threat Simulator platform.

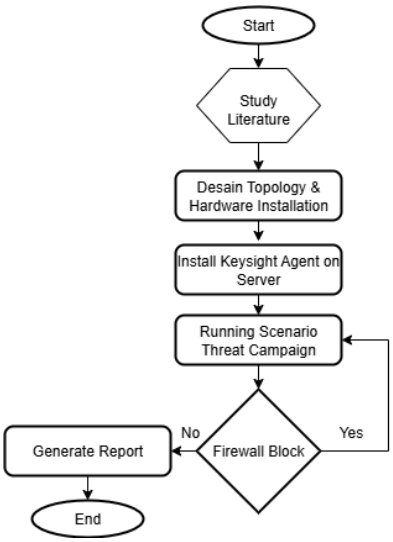

Figure 1. Research Methods

Following the setup, the predefined threat campaign ASSESSMENT: Keys to the Kingdom – Erlang/OTP SSH Vulnerability Analysis and Exploits Observed in the Wild was executed. This campaign included seven specific attack scenarios designed to exploit SSH vulnerabilities and simulate real-world adversarial behavior. The scenarios involved connections to malicious IP addresses and domains, namely 194.165.16.71,146.103.40.203,146.103.40.203:6667, as well as multiple DNS-based

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 1, Bulan Juni, Tahun 2025, Hal 33-42
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i1.58567
pISSN 2615-0646
eISSN 2614-8595

callbacks such as d09idt23pgl3db0en3dgeam6i45tpc6bg.dns.outbound.watchtowr.com, dns.outbound.watchtowr.com, d0a3qn23pglekp6ckgtge8xxfd14a8ouk.dns.outbound.watchtowr.com, and d0am3pi3pgl6h3t9mkp0qt3zn9p1izwso.dns.outbound.watchtowr.com. These attack vectors represent common tactics used by threat actors to establish remote access, maintain persistence, and evade detection. The scenarios were executed automatically using the Keysight Threat Simulator, which provided the advantage of replicating real-world malware campaigns in a controlled and repeatable environment. Once the attacks were launched, their traffic passed through a Palo Alto Networks firewall configured with “any” measurement. The firewall’s response was observed to determine whether the attack traffic was blocked or allowed. Based on the outcome, two conditions were considered: if the firewall blocked the traffic, the simulation proceeded to verification and continued with further scenarios; if not, the system proceeded to generate a comprehensive report.

At the conclusion of the process, the Threat Simulator automatically generated a detailed report consisting of three primary output metrics: Prevention Result, Detection Result, and Recommendations. The Prevention Result measured the effectiveness of the firewall and endpoint defenses in blocking malicious traffic before it reached the target host. The Detection Result evaluated whether the malicious activity was identified or flagged by existing monitoring tools during execution. Finally, the Recommendations section provided actionable guidance for addressing weaknesses, including configuration adjustments, improved segmentation, and enhanced monitoring of DNS traffic. This output format ensured that the research not only assessed the current level of security but also highlighted practical steps for strengthening the IT/OT security posture against emerging SSH-based exploits.

RESULT AND DISCUSSION

Before executing the simulation scenario, the network topology was first designed to ensure controlled attack traffic flow. As illustrated in Figure 2, the Keysight Threat Simulator Dark Cloud acts as the attack source, generating malicious traffic intended to mimic real-world threat campaigns. This traffic is directed through the Palo Alto Networks security tools, which function as the primary defense layer to prevent and detect malicious activities. Any traffic that passes through the firewall will then be forwarded to the designated server, where a Threat Simulator agent has been installed, as shown in Figure 2. This setup enables the evaluation of both prevention and detection capabilities of the security tools under realistic adversarial conditions.

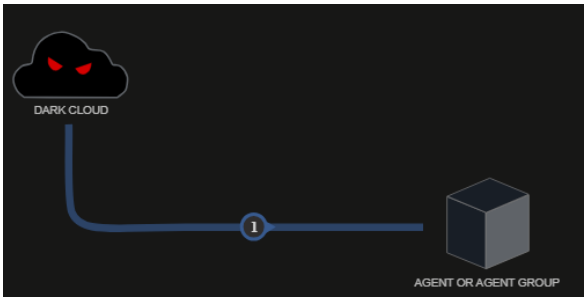

Figure 2. Threat Simulation Topology using Keysight Threat Simulator and Palo Alto Networks

The results in Table 1 of the threat simulation revealed that out of seven attack scenarios executed, only three were successfully prevented by the firewall, while four scenarios were allowed to bypass existing security controls. Specifically, the attacks involving direct connections to malicious IP addresses such as 194.165.16.71 and

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 1, Bulan Juni, Tahun 2025, Hal 33-42
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i1.58567
pISSN 2615-0646
eISSN 2614-8595

146.103.40.203:6667 were effectively blocked, demonstrating adequate prevention against known IP-based threats. However, the scenarios involving DNS-based callbacks, including d09idt23pgl3db0en3dgeam6i45tpc6bg.dns.outbound.watchtowr.com and other variants, were not blocked, resulting in failed prevention.

Table 1. Simulation Results of Malware Campaign Execution

Audit Name	Expected Result	Result	Prevention	Primary Tecnique	Started On
Malware Campaign - Visit Remote Host: 194.165.16.71	Blocked, None	Passed	Blocked	N.A	8/17/24. 4:17 PM
Malware Campaign - Visit Remote Host: d09idt23pgl3db0en3dgeam6i45tpc6bg.dns.outbound.watchtowr.com	Blocked, None	Failed	Allowed	T1071.001	8/17/24, 4:17 PM
Malware Campaign - Visit Remote Host: dns.outbound.watchtowr.com	Blocked, None	Failed	Allowed	T1071.001	8/17/24, 4:17 PM
Malware Campaign - Visit Remote Host: 146.103.40.203	Blocked, None	Passed	Blocked	T1071.001	8/17/24, 4:18 PM
Malware Campaign - Visit Remote Host: d0a3qn23pglekp6ckgtge8xxfd14a8ouk.dns.outbound.watchtowr.com	Blocked, None	Failed	Allowed	T1071.001	8/17/24. 4:18 PM
Malware Campaign - Visit Remote Host: d0am3pi3pgl6h3t9mkp0qt3zn9p1izwso.dns.outbound.watchtowr.com	Blocked, None	Failed	Allowed	T1071.001	8/17/24, 4:19 PM
Malware Campaign - Visit Remote Host: 146.103.40.203:6667	Blocked, None	Passed	Blocked	T1095	8/17/24, 4:19 PM

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 1, Bulan Juni, Tahun 2025, Hal 33-42
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i1.58567
pISSN 2615-0646
eISSN 2614-8595

Based on the simulation results at Figure 3, The test generated a total of 43 prevention attempts, of which several were successfully blocked (green/“Passed”), while a notable portion failed (red/“Failed”), meaning the system allowed malicious traffic to bypass controls. This indicates that while preventive mechanisms are in place, they are not fully reliable in mitigating all simulated threats. On the detection side, the result is more concerning: 0 successful detections were recorded, with all attempts marked as failed. This suggests that the environment lacks sufficient monitoring or alerting capability to identify attacks once they penetrate the initial prevention layer.

Figure 3. Threat Simulation Analysis Results – Prevention vs Detection

The assessment reveals several critical gaps, showing that prevention is still inconsistent as many attacks managed to bypass existing controls, while detection capabilities are completely absent, leaving the system unable to recognize post-breach activities. Without adequate detection and response, the organization is at high risk of undetected compromise, highlighting the urgent need to strengthen threat visibility and implement more integrated defense strategies. The 9 recommendations provided in the summary represent actionable insights to strengthen security posture as shown at Table 2.

Table 2. Table of Security Recommendations

No	Recommendation	Description
1	Improve Prevention Signatures/Policies	Refine security policies and rules to reduce failed blocking attempts.
2	Enhance Detection Coverage	Deploy or optimize detection tools to ensure threats are identified post-breach.
3	Update Threat Intelligence Feeds	Regularly synchronize with updated threat intelligence for accurate classification.
4	Fine-Tune System Configurations	Adjust security configurations to follow industry best practices.
5	Implement Layered Defense Strategies	Combine network, endpoint, and application

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 1, Bulan Juni, Tahun 2025, Hal 33-42
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i1.58567
pISSN 2615-0646
eISSN 2614-8595

		controls for stronger resilience.
6	Review Endpoint Controls	Strengthen endpoint protection to complement network-level defenses.
7	Improve Log Analysis and SIEM Integration	Enhance visibility by correlating logs and alerts with SIEM platforms.
8	Conduct Continuous Testing & Validation	Perform regular red-teaming, penetration testing, and breach simulations.
9	Apply Patches and Security Updates	Close vulnerabilities by applying timely system and application updates.

Most recommendations focus on enhancing intrusion prevention and traffic inspection, which directly respond to the high number of failed prevention attempts observed during testing. Several points emphasize the need for improved detection and monitoring, aiming to close the visibility gap that left all detection attempts unsuccessful. Additionally, recommendations related to policy enforcement and configuration hardening suggest that current controls are not fully optimized, allowing threats to bypass existing defenses. Overall, the recommendations highlight that the environment requires not just stronger preventive measures, but also robust detection and response capabilities to achieve a balanced and resilient security posture.

CONCLUSION

Based on the analysis and recommendations, it can be concluded that the current security posture is not sufficient to withstand sophisticated threats such as Erlang/OTP SSH exploits. Although preventive controls were able to block a number of attacks, many still bypassed the defenses, and the complete absence of detection highlights a serious visibility gap. The 9 recommendations generated, ranging from strengthening intrusion prevention, enhancing monitoring capabilities, to improving policy enforcement, emphasize the need for a more integrated and layered security approach. Therefore, implementing these recommendations is crucial to improving both prevention accuracy and detection capability, ultimately ensuring stronger resilience against future threat campaigns.

REFERENCES

A blended approach of static binary mining and exploratory data analysis to obtain the security posture of embedded systems firmware. (2025). International Journal of Information and Computer Security. https://www.inderscienceonline.com/doi/abs/10.1504/IJICS.2025.145105

Azzahri, M. N., et al. (2024). The application of Cowrie honeypot to analyze attacks on SSH and Telnet protocols. In 2024 IEEE 2nd International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT) (pp. 290–295).

https://doi.org/10.1109/ICEECIT63698.2024.10859786

Bhole, M., Sauter, T., & Kastner, W. (2025). Enhancing industrial cybersecurity: Insights from analyzing threat groups and strategies in operational technology environments. IEEE Open Journal of the Industrial Electronics Society, 6, 145–157. https://doi.org/10.1109/OJIES.2025.3527585

Bölin, O., & Van Daele, P. (2024). Penetration testing of one-time password authentication. https://urn.kb.se/resolve?urn=urn:nbn:se:bth-26640

Caviglia, R. (2025). Novel approaches to standard-based cybersecurity risk management in OT environments (Doctoral dissertation). https://tesidottorato.depositolegale.it/handle/20.500.14242/200922

Cho, H., & Kim, S. (2025). Threat modeling for the defense industry: Past, present, and future. IEEE Access, 13, 53276–53304. https://doi.org/10.1109/ACCESS.2025.3550337

Cyber security breaches in corporate networks: A literature review on recent threats and their impact. (2025). Theseus. https://www.theseus.fi/handle/10024/887316

Dalal, A. (2025). Designing zero trust security models to protect distributed networks and minimize cyber risks. Social Science Research Network. https://doi.org/10.2139/ssrn.5268092

Easttom, C. (2025). A study of North Korea's cyber warfare: Actors, tactics, and AI integration. EBSCOhost. https://openurl.ebsco.com/contentitem/gcd:184729845

Fojude, M. (2025). Insider threat agent: A behavioral-based zero trust access control using machine learning agent (Doctoral dissertation, Georgia Southern University). https://digitalcommons.georgiasouthern.edu/etd/2942

Framework for assessing information system security posture risks. (2025). ProQuest. https://www.proquest.com/openview/5e0312b388937340d2f316706f3b4223/1

Garg, P. (2025). Cloud security posture management: Tools and techniques. Social Science Research Network. https://doi.org/10.2139/ssrn.5357921

Hussain, M., & Rahbi, F. (2025). Strengthening cloud security: Innovations in posture management tools and techniques (Unpublished manuscript). https://doi.org/10.13140/RG.2.2.24821.90082

Koli, L., Kalra, S., Thakur, R., Saifi, A., & Singh, K. (2025). AI-driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection. arXiv. https://doi.org/10.48550/arXiv.2505.03796

Kolli, R. K., Priyanshi, E. R., & Vashishtha, P. S. (2024). Palo Alto firewalls: Security in enterprise networks. International Journal of Engineering

Development and Research, 12(3), 1–13.

Lee, I., & Choi, C. (2025). MuCamp: Generating cyber campaign variants via TTP synonym replacement for group attribution. IEEE Transactions on Information Forensics and Security, 20, 6162–6174. https://doi.org/10.1109/TIFS.2025.3578233

Metibemu, O. C., Adesokan-Imran, T. O., Ajayi, A. J., Tiwo, O. J., Olutimehin, A. T., & Olaniyi, O. O. (2025). Developing proactive threat mitigation strategies for cloud misconfiguration risks in financial SaaS applications. Journal of Engineering Research and Reports, 27(3), 393–413. https://doi.org/10.9734/jerr/2025/v27i31442

Mining threat intelligence from billion-scale SSH brute-force attacks. (2025). IDEALS. https://www.ideals.illinois.edu/items/115715

Nair, R. R. (2025). Evaluating the effectiveness of AI-driven threat intelligence systems: A technical analysis. Journal of Computer Science and Technology Studies, 7(3), 514–524. https://doi.org/10.32996/jcsts.2025.7.3.58

Ofili, B. T., Erhabor, E. O., & Obasuyi, O. T. (2025). Enhancing federal cloud security with AI: Zero trust, threat intelligence and CISA compliance. World Journal of Advanced Research and Reviews, 25(2), 2377–2400. https://doi.org/10.30574/wjarr.2025.25.2.0620

Osholake, S. F., Umealajekwu, C., Edohen, A., Majekodunmi, A. O., & Evans-Anoruo, U. (2024). Human–AI collaborative security operations: Optimizing SOC analyst cognitive load through augmented intelligence frameworks (Unpublished manuscript).

Oyeniyi, J. O., & Oyeniran, O. A. (2025). Optimizing information security in cloud environments. Journal of Cybersecurity and Emerging Research Practices. https://digitalcommons.kennesaw.edu/jcerp/vol2025/iss1/8

Redavid, F. (2024). Exploiting race conditions to break the OTP authentication mechanism in web applications (Master's thesis, Politecnico di Torino). https://webthesis.biblio.polito.it/33225

Securing against advanced cyber threats: A comprehensive guide to phishing, XSS, and SQL injection defense. (2025). Neliti. https://www.neliti.com/publications/589857

Security challenges and mitigation strategies in multi-cloud environments: A comprehensive analysis. (2025). Scholars Repository. https://eprint.scholarsrepository.com/id/eprint/2287

Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2025). Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration. Cyber Security Applications, 3, 100077. https://doi.org/10.1016/j.csa.2024.100077