International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0046
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 312 - 317

THREATINSIGHT: A Profile-Aware and Explainable Cyber Threat Intelligence System Using Real-Time Vulnerability Analysis

Mohamed Irfan M[1], Dr. P. Suriyakumar[2], Giridharan K[3], Logantharan S[4]
[1]Department of Information Technology, KPR Institute of Engineering and Technology, Coimbatore, India – 641407
[2]Department of Mathematics, KPR Institute of Engineering and Technology, Coimbatore, India - 641407
[3]Department of Information Technology, KPR Institute of Engineering and Technology, Coimbatore, India - 641407
[4]Department of Electrical and Electronics Engineering, KPR Institute of Engineering and Technology, Coimbatore, India - 641407
Emails: *mohamedirfan27521@gmail.com[1], suriyakumar.p@kpriet.ac.in[2], giridh4258@gmail.com[3], 22ee027@kpriet.ac.in[4]*

Abstract
This fast rate of publicly published software vulnerability disclosure, combined with the growing complexity of modern enterprise software environments, has created a strong need and requirement of an automated cyber threat intelligence system with the capacity to provide operational, contextally relevant risk information. Security practitioners regularly rely on generic vulnerability feeds, manual scanning, or host-based scanning tools, which often create too much noise, have little relevance to the environment and introduce privacy and governance issues. Besides, the use of opaque machine learning models of some of the available solutions limits the explainability, as well as auditability, of solutions in security decision-making.This report describes ThreatInsight, a profile-sensitive and interpretable Cyber Threat Intelligence System which provides deterministic vulnerability risk analysis using distinctively available threat intelligence information only. It takes input of vulnerability data over MITRE CVE, NVD, CISA KEV, and EPSS and compares vulnerabilities to user-provided environment profiles which describe what operating systems and application stacks are in use and therefore does not require host scanning or the use of user-specific telemetry. The risk prioritisation is calculated by the use of transparent and rule-based intelligence agents and the output of this calculated information is shared using a versioned REST API, a SOC-based dashboard, automated warnings, and reports, thereby showing a viable and credible solution to cyber threat intelligence in the real world.
Keywords: *Cyber Threat Intelligence; Vulnerability Analysis; Explainable Security Analytics; Profile-Aware Risk Assessment; Deterministic Threat Scoring; Privacy-Preserving Security Systems.*

1. Introduction
Software vulnerabilities reported publicly have significantly increased in number and the general use of highly complex and multi-layered software stacks has transformed the manner in which organizations address the issue of cyber risk. The modern business landscape relies on a heterogeneous combination of operating systems, applications, and third-party elements, which makes it hard to uniquely identify the vulnerabilities that are really relevant to the business circumstances of the security personnel. Lack of contextually applicable filtering system on publicly available repositories of vulnerabilities may lead to large and unsorted threat lists that overwhelm analysts and delay the creation of remediation. The intelligence of cyber threat is considered to be a strong determinant to successful vulnerability management, prevention of attacks and general improvement of security posture. Therefore, automated methods of testing vulnerabilities based on severity metrics, indicators of exploitability, and threat feeds have received more and more interest among both security practitioners and researchers.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0046
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 312 - 317

Most solutions that are out there use regulated machine-learning models or customized scoring systems to prioritize vulnerabilities. Although these methods prove effective in a controlled setting, they raise numerous practical issues: they are labour-intensive in data collection and annotation, and need specific configurations; they are often opaque in model performance, making it difficult to interpret; and black-box scoring models undermine security operations confidence and auditability. In addition, host-based scanning and constant telemetry gathering generate more privacy, compliance and operational issues In order to address these obstacles, the current paper proposes ThreatInsight, a profile-sensitive cyber threat intelligence platform that conducts deterministic vulnerability analysis based on publicly available and transparent rules and based on publicly available and only publicly available threat intelligence data. The system does not rely on automated asset discovery and opaque environmental learning models, which allows users the dynamism regarding how their operating systems and application stacks are explicitly configured through structured environmental profiles. The system produces vulnerability relevance, risk prioritisation, and remediation guidance by means of a rule-based explainable, rule-based intelligence engine that combines severity, exploitability indicators, exploitation status, and environmental context to generate a synthesis of these factors. Its general purpose is to equip a practical, interpretable, and privacy-generating cyber threat intelligence model, which can be operationalised in the context of normal security processes and with the assistance of compliance-friendly audits and audit policies.

2. Related Work

Historical methods of cyber threat intelligence and vulnerability assessment were largely based on fixed vulnerability databases, manual-based assessment, and universal scoring system, including the Common Vulnerability Scoring System (CVSS). the MITRE CVE and the National Vulnerability database (NVD) offer very useful data on the vulnerabilities, which are available publicly to perform security analysis, but their results are mostly generic and have no environment-specific operational environment. As a result, security teams are often faced with serious challenges in addressing the raw vulnerability data into executable remediation policies, especially in large, distributed, and heterogeneous enterprise software systems (Scarfone et al.,2010;Mell etal.,2007). As the scale of large-scale threat intelligence feeds and exploit datasets has grown, scholars have studied automated vulnerability prioritization based on exploitability indicators and machine learning. Other researchers apply the tool of supervised learning to forecast the probability of exploitation by using historical attack information and the availability of exploits (Sabottke et al., 2015; Allodi and Massacci, 2017). These methods, despite showing an improvement in prioritization accuracy in controlled tests, require large labeled datasets and have the drawback of requiring retraining on a regular basis. In addition, numerous systems based on learning are black box, which makes it hard to figure out how these systems made certain decisions and, hence, makes their use in operational security settings, where explainability and auditability are essential, challenging (Holzinger et al., 2017).

The recent trends in research focus on explainable security analytics, deterministic reasoning, and privacy preserving cyber threat intelligence enter as a way to solve the current limitations. Rule-based and hybrid intelligence systems have been used successfully to achieve greater transparency and less data and processing needs (Zhou et al., 2021; Behl and Behl, 2017). Still, most of the existing deployed systems still use either host-based scanning, vendor-specific telemetry, or discovery of default assets, which promotes numerous privacy and control issues. ThreatInsight can be viewed as a continuation of the trend, reaching the level of deterministic score of risk as well as profile-matching vulnerability, using only publicly available threat information intelligence data and, thus, can provide explainable and interpretable cyber threat intelligence without introducing invasive data gathering.

2.1.System Overview

ThreatInsight is an end-to-end, modular Cyber Threat Intelligence system offering environment-sensitive vulnerability risk analysis with just the public threat intelligence data and use it to assess the security. The

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0046
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 312 - 317

system is not based on a host scanning, agent deployment or private telemetry collection and is built on a clear user-declared profile of the environment and a completely deterministic risk-evaluation intelligence logic. Cyber threat analysis involves four major components making up the entire and integrated intelligence pipeline that is a part of the system architecture

- Public Threat Data Ingestion Module: Gathers vulnerability and exploitation information on a continuous basis (public sources, including MITRE CVE, NVD, CISA Known Exploited Vulnerabilities (KEV), and Exploit Prediction Scoring System (EPSS).
- Normalization of Threat Knowledge Module: Organizes raw vulnerability data in the form of CVE to Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC) to allow semantic interpretation of vulnerabilities and attack patterns.
- Deterministic Intelligence Engine: Uses rule-based analysis, risk scoring, and recommendation logic through a combination of severity measurements, exploitability measures, exploitation state and profile relevance to generate explainable risk outcomes.
- API and Visualization Module: Publishes intelligence products using a versioned REST API, a SOC-style web dashboard, automated notifications, and downloadable reports.

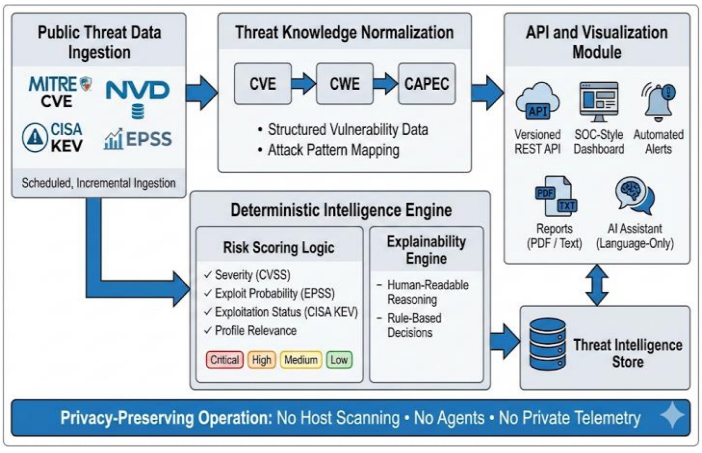

Figure 1 Flow Process

General structure of the suggested Threatinsight system that depicts the public threat data ingestion, normalized vulnerability, deterministic intelligence processing and SOC-like visualization and reporting. The modular architecture has allowed explainable risk assessment, vulnerability prioritization based on environment specifics, and high privacy due to lack of host scanning, agent deployment, or collection of telemetry, making the system appropriate to the real-world security operations.

3. Method

This part outlines how the proposed ThreatInsight cyber threat intelligence framework will be developed.

3.1.Public Threat Data Ingestion

The system takes vulnerability and exploitation data provided publicly available such as MITRE CVE, National Vulnerability Database (NVD), Cisaser Known Exploited Vulnerabilities (KEV) and Exploit Prediction Scoring System (EPSS). To guarantee freshness, consistency and traceability of the threat intelligence, data ingestion is conducted by means of scheduled and incremental collection scheme.

3.2.Threat Knowledge Extraction and Structuring

Based on the consumed information , ThreatInsight identifies structured vulnerability attributes and standardizes them into a single threat representation. The components obtained are the following:

- Vulnerability Identification (CVE): The vulnerabilities are identified using a unique identifier, the CVE identifier, and descriptive metadata and severity information.
- Weakness Classification (CWE): CVEs are assigned to categories in Common Weakness Enumeration to embody the software weakness underlying any given vulnerability.
- Attack Pattern Mapping (CAPEC): Mapped CWEs are relevant CAPEC attack patterns that characterize how vulnerabilities may be implemented in the attack scenarios.
- Exploitability Indicators: The scores of exploit prediction of EPSS and exploitation status of CISA KEV are used to state the real-world exploitation probability.
- Affected Product Context: Vendor and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0046
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 312 - 317

product data is rectified in the support of environment-flinty vulnerability matching.

3.3.Awareness of Profiles with Vulnerability Matching

Environment profiles are defined by the users and define operating systems and application stacks. These profiles are deterministically compared with vulnerabilities to determine the threats which are pertinent to the stated environment whilst eliminating the irrelevant vulnerabilities

3.4.Risk Scoring and Intelligence Fusion

The system obtains a final risk rating by a rule-based model that combines severity measures, exploitability measures, known exploitation measures and profile relevancy measures. The resultant scores are then translated to discrete risk levels, thus allowing the
prioritization to be uniform throughout the analytical process.

3.5.Explainability Mechanism

In case of every vulnerability evaluated, ThreatInsight generates a human understandable exposition through highlighting the prevailing factors which lead to the risk score. This strategy provides transparency and allows analysts to understand as well as audit all decisions of intelligence.

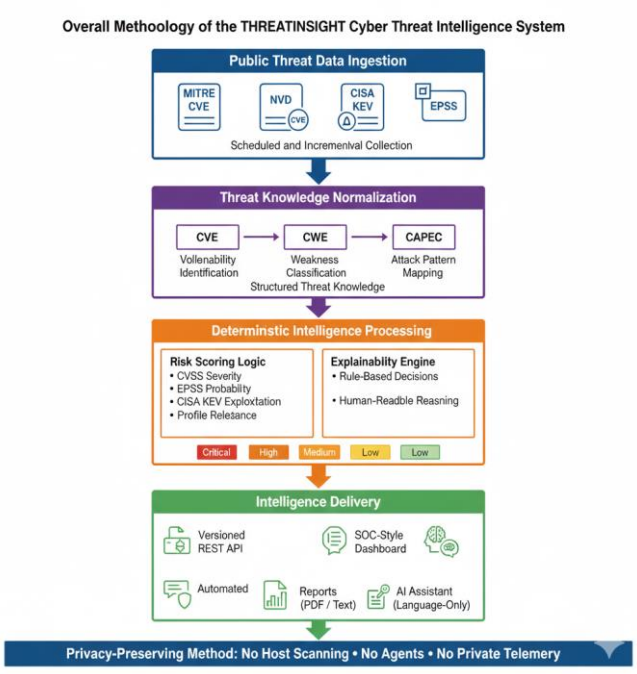

Figure 2 Methodology

General methodological process diagram of the ThreatInsight cyber threat intelligence system, depicting an end-to-end look at ingestion, normalization in a structured manner, deterministic intelligence calculation and provisioning of publicly available data. The sources of vulnerabilities such as CVE, NVD, CISA KEV, and EPSS are incrementally summarized and transformed into structured form of threat knowledge through CVE-to-CWE and CWE-to-CAPEC mappings. Deterministic risk scoring is the combination of severity, exploitability, exploitation status, and environment relevance, with explainable results, distributed via a versioned API, a SOC-style dashboard, alerts, and reports, and without host scanning or private telemetry. The methodology highlights transparency, reproducibility and risk prioritization based on the environment.

4. Results and Discussion

4.1.Results

The test of the suggested ThreatInsight system was conducted with a controlled analysis of its working behavior, using constantly ingested public vulnerability data and various user-defined profiles of the environment. The first one was aimed at assessing the general responsiveness of the system and the timeliness of data, the second at checking the similarity of the risk prioritization in the periodic updates, and the third at determining the practical usefulness of the intelligence products created in the real-world security analysis. The system had been able to receive real-time vulnerability reports of public sources and generate consistent and accurate risk scores after data modeling and intelligence merging. The matching profile based on the awareness was effective in eliminating irrelevant vulnerabilities, thus significantly reducing noise in the risk views. The dashboard and report deliverables allowed users to quickly spot high-risk vulnerabilities affecting their reported environments and have an understanding of the logic behind the prioritization decisions.

4.2.Discussion

The empirical results suggest that a rule-based, deterministic, and cyber threat intelligence approach can provide viable vulnerability prioritization and eliminates the need to use machine-learning models

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0046
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 312 - 317

or private telemetry. The system produces operational and explainable risk ratings by combining severity measures, exploitability measures, status of reported exploitations and environmental applicability, and is suitable to use in operational contexts. Even though the system does not imply asset discovery of unknown assets, and live system discovery, the privacy preservation and auditability is robust due to this conscious design choice. The profile-based intelligence paradigm proves to be effective in the situation when the key factors are trust, transparency, and adherence to rules, which explains the practical relevance of ThreatInsight in the security-related operations in the real world.

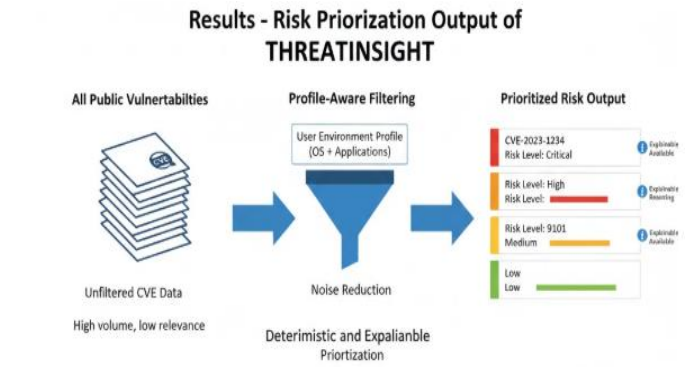

Figure 3 Result and Output

Graphical illustration of the ThreatInsight architecture defining profile-sensitive vulnerability filtration and deterministic risk prioritization. The figure illustrates the way of how large datasets of public vulnerabilities are systematically reduced to environment-specific risks, whereby the severity levels are well stratified and supported by explainable justifications, which can be used to make effective security decisions.

Conclusion

In this paper, the author introduces ThreatInsight, a profile-aware and explainable Cyber Threat Intelligence system, which supplies deterministic vulnerability risk analysis on the basis of publicly provided threat intelligence information alone. The system implements systematic vulnerability normalization, relevance matching against profiles, and rule-based intelligence logic to provide clear and operational risk prioritization and eliminate the need to scan the host, deploy agents, or use proprietary telemetry. ThreatInsight provides a way of reducing vulnerability noise through a combination of severity measures, exploitability measures, known exploitation measures, and contextual environmental measures, without losing the full explainability or auditability. Empirical evidence confirms that, with a deterministic, privacy-sensitive cyber threat intelligence methodology, operational security procedures can be effectively supported, and that this approach to vulnerability-management is most likely to be practical and reliable compared to an opaque vulnerability-management approach or intrusive approach.

Acknowledgements

The authors thank the faculty members of KPR Institute of Engineering and Technology and the management of this institution with the guidance, encouragement, and support they gave them in the process of developing this project..

References

[1]. P. Mell, K. Scarfone, and S. Romanosky, “A complete guide to the Common Vulnerability Scoring System version 2.0,” FIRST Forum of Incident Response and Security Teams, 2007.
[2]. K. Scarfone, A. Jansen, and M. Tracy, “Guide to General Server Security,” NIST Special Publication 800-123, National Institute of Standards and Technology, 2008.
[3]. MITRE Corporation, “Common Vulnerabilities and Exposures (CVE),” https://cve.mitre.org
[4]. National Institute of Standards and Technology, “National Vulnerability Database (NVD),” https://nvd.nist.gov
[5]. Cybersecurity and Infrastructure Security Agency (CISA), “Known Exploited Vulnerabilities Catalog,” https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[6]. J. Jacobs, “Exploit Prediction Scoring System (EPSS),” Forum of Incident Response and Security Teams (FIRST), 2021.
[7]. MITRE Corporation, “Common Weakness Enumeration (CWE),” https://cwe.mitre.org

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0046
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 312 - 317

[8]. MITRE Corporation, "Common Attack Pattern Enumeration and Classification (CAPEC)," https://capec.mitre.org
[9]. S. Allodi and F. Massacci, "Comparing vulnerability severity and exploitability using CVSS and exploit data," ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, 2014.
[10]. W. Sabottke, O. Suciu, and T. Dumitraș, "Vulnerability disclosure in the age of social media," USENIX Security Symposium, 2015.
[11]. A. Holzinger, C. Biemann, C. S. Pattichis, and D. B. Kell, "What do we need to build explainable AI systems?" arXiv preprint arXiv:1712.09923, 2017.
[12]. Z. Zhou, X. Chen, X. Li, J. Zeng, K. Luo, and Y. Zhang, "Explainable and robust AI for trustworthy systems," IEEE Intelligent Systems, vol. 36, no. 4, pp. 36–44, 2021.
[13]. M. Behl and K. Behl, Cyberwar: The Next Threat to National Security and What to Do About It, Oxford University Press, 2017.
[14]. S. Barnum, "Standardizing cyber threat intelligence information with the Structured Threat 15] OASIS, "Trusted Automated Exchange of Intelligence Information (TAXII) Version 2.1," OASIS Standard, 2021.
[15]. M. Angelelli and F. Militello, "A robust statistical framework for cyber-vulnerability analysis under uncertainty," Expert Systems with Applications, vol. 240, 2024.
[16]. P. Alaeifar, S. Achemlal, and C. Talhi, "Current approaches and future directions for cyber threat intelligence," Journal of Information Security and Applications, vol. 74, pp. 1–14, 2024.
[17]. G. Sunkara, "Explainable AI for cyber threat intelligence: enhancing analyst trust," Open Access Research Journal of Science and Technology, vol. 14, no. 02, pp. 029–040, Jul. 2025.
[18]. Y. Mujibur Sheikh et al., "RiskBridge: turning CVEs into business-aligned patch priorities," arXiv:2601.06201, Jan. 2026.