



IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

“iCTI: AN INTEGRATED CYBER RESILIENCE AND CYBER THREAT INTELLIGENCE ARCHITECTURE FOR PROACTIVE DEFENSE AND ENHANCED INCIDENT RESPONSE”

Kundan Kumar Mishra¹, Dr. Amaravathi Pentaganti²

^{1,2} Department of Computer Science and Engineering, NIILM University, Kaithal, Haryana, India

kundankumarmishra@gmail.com

ABSTRACT

Organizations can no longer rely on perimeter defenses and after-the-fact incident handling against attackers that grow more capable every year. This paper proposes iCTI, an integrated architecture that joins a cyber-resilience framework—risk management, identity and access management, incident response, business continuity and resilience metrics—with a cyber threat intelligence (CTI) pipeline that fuses social media, open-source intelligence (OSINT) and specialized feeds. The pipeline uses Zeek for network monitoring, Apache Kafka for ingestion and Apache Metron/Storm and Hadoop for real-time and batch analysis, and it enriches traffic with known threat indicators; adversary tactics, techniques and procedures (TTPs) drive proactive defense, and timely intelligence drives incident response. The resilience mechanisms were validated in a controlled AWS environment with SIEM, Apache Spark and OpenSearch, where 95% of simulated threats were detected with an average response time under five minutes. The iCTI architecture was then integrated with Wazuh, Suricata, OpenEDR, a Sophos firewall, Nessus and Splunk in a production-like environment and exercised with the Splunk Attack Range, which aligned the simulated activity to MITRE ATT&CK.

Key Words: Cyber Resilience, Cyber Threat Intelligence, Proactive Defense, Incident Response, TTP Analysis, SIEM, Zeek, Apache Metron, MITRE ATT&CK.

I. INTRODUCTION

Cyber resilience is the ability of an organization to protect its critical information assets, preserving their confidentiality, integrity and availability, while withstanding and recovering from cyber-attacks and continuing essential services. [1], [2] It has become a core element of enterprise risk management, yet organizations pursuing it face a scarcity of experienced security professionals, complex IT estates, fast-changing threats, limited budgets and regulatory obligations. [3]

Resilience, however, is only as good as the knowledge behind it. CTI, the systematic collection, analysis and use of information about potential cyber hazards, tells an organization which attackers, techniques and vulnerabilities matter most, so that defenses can be prepared before an attack and incident response can be tailored to the threat. [4], [5] Reactive defenses and generic response plans are frequently inadequate because they do not adapt to the threat landscape, and the absence of timely, actionable intelligence delays response, causing financial loss, data exposure and prolonged outages.

This paper therefore proposes iCTI, an integrated architecture that treats cyber resilience and CTI as one system. The contributions are:

- A cyber-resilience framework built on a CRAT-style assessment, identity and access management (IAM), incident response (IR) and measurable resilience metrics.

<https://www.ijrtsm.com> © International Journal of Recent Technology Science & Management

- A CTI architecture that integrates OSINT, social media and specialized intelligence channels with network telemetry, and turns adversary TTPs into proactive defense strategies.
- A CTI-driven incident-response capability that supplies timely, actionable intelligence, supports tailored response plans, prioritizes resources and allows intelligence sharing with trusted partners.
- Experimental validation in two environments: a controlled AWS cloud testbed and a production-like integrated security environment exercised with Splunk Attack Range v2.

Section II reviews related work. Section III presents the resilience methodology, Section IV the iCTI architecture, Section V the experiments and results, Section VI the challenges and limitations, and Sections VII and VIII the future scope and conclusions.

II. LITERATURE REVIEW

A. Cyber Resilience Frameworks

The discourse on cyber resilience has moved from a purely technical view to one that includes social, operational and organizational factors. [2], [6] The MITRE cyber-resiliency engineering framework, the seven-pillar (7Ps) model and a number of self-assessment tools such as CR-SAT for small and medium enterprises give organizations structured ways to design and assess resilience. [7], [8], [9] A systematic review of assessment frameworks and a survey of case studies nevertheless find practice fragmented and report few quantitative evaluations. [3], [10] Kott and Linkov argue that resilience can only be improved if it is measured, and Linkov *et al.* discuss metrics that make it measurable. [11], [12] Work on resilience engines for the Internet of Things and on digital twins for critical infrastructure shows the same concerns in specific domains. [13], [14]

B. CTI, Big Data and SOAR

CTI frameworks increasingly rely on big-data analytics. CTI-CORE analyzes large volumes of security data to identify and mitigate threats, and Bucur and Sgârciu survey big-data and machine-learning techniques for CTI. [15], [16] Zhang *et al.* integrate SOAR with CTI on big-data technologies to improve the efficiency of incident response, [17] while other work correlates CTI with sightings to assess and augment intelligence, computes over system provenance to detect threats, and predicts the risk of cyber incidents. [18], [19], [20] Anomaly detection over system logs with deep learning and exploratory security analytics are further building blocks. [21], [22] Deception technologies such as containerized honeypots add attacker-tracking intelligence. [23]

C. Research Gap

Resilience research and CTI research have developed largely in parallel. Resilience frameworks rarely specify where intelligence enters planning and response, and CTI systems rarely state how they raise measurable resilience. Few studies combine both, integrate diverse sources in a single architecture and validate it in operation. iCTI is designed to fill that gap.

III. RESEARCH METHODOLOGY: CYBER-RESILIENCE FRAMEWORK

A. Resilience Life Cycle

The proposed framework protects critical assets through a continuous loop (Fig. 1): identify critical assets, assess risk, deploy security controls, train and raise awareness, plan incident response, test and validate, and improve continually. Resilience is not a one-time achievement; the framework is refreshed as the threat landscape changes and is the shared responsibility of management, employees and partners, not of IT staff alone.



Fig. 1. Resilience life cycle for protecting critical assets against cyber threats.

B. Assessment, IAM and Incident Response

A Cyber Resilience Assessment Tool (CRAT) structures assessment into seven categories: governance, risk management, threat assessment, vulnerability management, incident management, business continuity and crisis management. Data are gathered through stakeholder interviews, review of policies and procedures, and analysis of technical controls; the results yield a roadmap that prioritizes improvements.

IAM regulates which digital identities may access which resources, through identification, authentication, authorization and accountability. It matters more as applications move to the cloud and users connect from many devices and locations. **IR** is the identification, analysis and management of security incidents. It relies on documented procedures, collaboration among IT, security and legal teams, and regular training and testing.

C. Resilience Metrics

Table 1 lists the metrics used to judge resilience. Good metrics are quantifiable, sensitive to change, relevant, adaptable, consistent, comprehensive and transparent. [11], [12] Two of them are computed from incident timestamps as in (1) and (2), and detection accuracy as in (3), where N is the number of incidents or simulated threats.

TABLE 1 Cyber-Resilience Metrics

Metric	What it measures
MTTD (mean time to detection)	Average time to identify an incident
MTTR (mean time to response)	Average response time after detection
RTO (recovery time objective)	Time to restore normal operations
RPO (recovery point objective)	Data loss tolerable before business impact
REF (risk exposure factor)	Business consequence given likelihood and severity
VD (vulnerability density)	Vulnerabilities relative to system size or complexity
Compliance assessment	Adherence to regulations and standards
User awareness	Security awareness among staff
Threat data coverage	Ability to detect emergent threats
IR effectiveness	Success of response plans in limiting impact

$$MTTD = \frac{1}{N} \sum_{i=1}^N (t_{\text{detect},i} - t_{\text{start},i})$$

(1)

$$MTTR = \frac{1}{N} \sum_{i=1}^N (t_{\text{respond},i} - t_{\text{detect},i})$$

(2)

$$DA = \frac{N_{\text{detected}}}{N_{\text{simulated}}} \times 100\%$$

(3)

IV. THE iCTI ARCHITECTURE

iCTI (Fig. 2) turns raw network telemetry and external intelligence into proactive defense and faster response. It is organized in six phases: data collection, data ingestion, data processing, CTI integration, threat analysis and visualization.

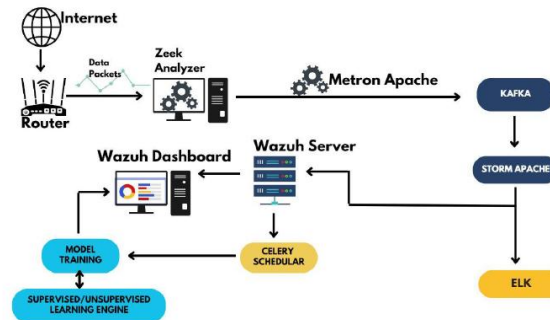


Fig. 2. The proposed iCTI architecture: Zeek, Kafka, Metron (Storm and Hadoop), Wazuh, ELK and a learning engine.

A. Collection, Ingestion and Processing

Collection. Zeek, a network security monitor, passively watches traffic and writes logs of IP addresses, protocols, ports, connection details and extracted files. **Ingestion.** Logs are partitioned across topics in Apache Kafka, a high-throughput, fault-tolerant, scalable pipeline that guarantees durable delivery. **Processing.** Apache Metron provides real-time threat detection and security analytics. Apache Storm topologies consume the Kafka streams in parallel to normalize, parse, enrich and extract features, while Apache Hadoop (HDFS) batch jobs support historical analysis, correlation and trend identification over larger data sets.

B. CTI Integration and Threat Analysis

Metron enriches the processed stream with CTI feeds of malicious IP addresses, domains, URLs and file hashes, so known indicators are matched in near real time. Anomaly detection, machine-learning algorithms and statistical analysis, supported by a supervised/unsupervised learning engine, then look for malicious patterns. Detections are prioritized by potential severity and impact and shown on dashboards (Wazuh and ELK) with reports, charts, graphs and alerts, so that analysts can decide and respond with context.

C. Intelligence Sources

The architecture draws on three source families. Social media provides real-time indicators of emerging threats and attack vectors, OSINT supplies publicly available information on vulnerabilities and hazards, and specialized feeds from trusted vendors or industry bodies provide contextualized, targeted intelligence. Aggregating them reveals prevalent attack vectors, emerging trends and the tools and techniques of adversaries.

D. Proactive Defense

Past attacks are studied for their TTPs, the recurring patterns, behaviors and indicators that characterize an adversary. Understanding them allows controls to be placed where they matter, for instance stronger e-mail filtering and staff training against phishing, intrusion detection and prevention systems, network segmentation and robust access controls. Security investment is aligned with the vulnerabilities and threats the data reveal, so the most critical assets receive the strongest protection.

E. Enhanced Incident Response

Collected intelligence is analyzed in the context of the organization's own infrastructure to identify the threats and weaknesses specific to it. This yields response plans tailored to attack scenarios, with predefined actions, responsibilities, communication protocols and escalation paths. For example, a plan may block command-and-control servers tied to a recent malware variant or refresh antivirus signatures. Real-time exchange of intelligence with trusted partners allows the organization to benefit from collective knowledge, and resources are allocated by risk, shortening detection and dwell time.

F. Novelty

Compared with the work reviewed in Section II, iCTI is distinguished by (i) integrating OSINT, social-media and specialized intelligence in a single framework; (ii) deriving proactive defenses from adversary TTPs; (iii) using specialized channels for context-specific intelligence; (iv) improving response with actionable and timely intelligence; (v) aligning security investment with identified vulnerabilities; (vi) supporting real-time sharing with reputable external entities; and (vii) remaining scalable and adaptable as threats and technologies change.

V. EXPERIMENTAL ANALYSIS AND RESULTS

A. Resilience Validation in a Controlled AWS Environment

Setup. A controlled environment resembling an organization's production setup was built on AWS: a virtual private cloud with public and private subnets, security groups and network ACLs. A SIEM solution, a big-data framework and OpenSearch were hosted on EC2 instances. Logs from CloudTrail, CloudWatch, EC2 instances and other security tools were processed with Apache Spark. Detection rules covered abnormal log-on attempts, suspicious network traffic and unusual file-access patterns; alerts were delivered through AWS SNS, with escalation procedures defined for each incident category. The OpenSearch cluster used TLS encryption, authentication and authorization, defined indices and mappings, and automatic retention and deletion policies.

Threats and workflow. Predefined tools generated simulated malware infections, phishing attacks and unauthorized access attempts. On detection, the SIEM raised an alert and started a response workflow with automated actions (blocking the IP address, disabling a compromised account, isolating the affected system) and manual actions (investigation, analysis and mitigation by analysts). Key performance indicators were detection accuracy (3) and response time, from detection to workflow initiation.

Results. The SIEM correctly identified 95% of the simulated threats, with an average response time of under five minutes. The response workflow contained the detected incidents and prevented further harm; OpenSearch indexed and searched the security data quickly enough for analysts to investigate promptly, and real-time alerts enabled immediate action. Fig. 3 shows infrastructure health during the attack period: processor load rose briefly (to about 0.01 per CPU at 02:31 PM) and then returned to near zero, disk activity varied between roughly 4 and 18 IOPS, and the primary network interface carried steady inbound traffic of about 96–97 units with negligible outbound traffic. No sustained resource exhaustion was seen, indicating that the mechanisms operated within the capacity of the environment.

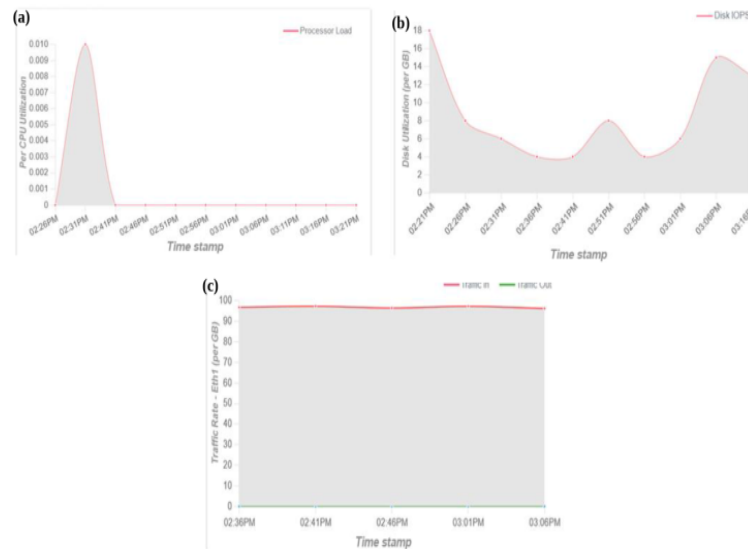


Fig. 3. Cloud infrastructure health during attack conditions: (a) processor load, (b) disk IOPS, (c) network traffic on the primary interface.

B. iCTI in a Production-Like Environment

Setup. iCTI was integrated into a representative production environment with servers, workstations, firewalls and intrusion detection. Intelligence was acquired continuously through automation and APIs from OSINT, social media (Twitter) and a SIEM feed, and analyzed in real time with machine-learning and anomaly-detection methods. Attack scenarios were generated with Metasploit, Nmap and Burp Suite. Table 2 lists the integrated security stack.

TABLE 2

Integrated Security Stack Used with iCTI

Function	Component
Network monitoring	Zeek
Streaming and processing	Apache Kafka, Storm, Metron, Hadoop
SIEM	Wazuh
IDS / IPS	Suricata (signature and behavioral)
Endpoint protection	OpenEDR
Network firewall	Sophos XG 210
Vulnerability assessment	Nessus
Threat-intelligence platform	Splunk
Attack simulation	Splunk Attack Range v2

Attack simulation. Splunk Attack Range v2 supplies isolated virtual machines with vulnerable applications, network configurations and attack scenarios, and records the events produced, which allows the architecture's detection and response to be assessed safely. The Splunk dashboard (Fig. 4) showed 11 simulations run, mapped to one MITRE ATT&CK tactic and one technique (T1003.002, OS credential dumping), and listed the attacking user name and target hosts. The Splunk Enterprise Security Content Update (ESCU, version 3.44.0) used for detection content (Fig. 5) contained 144 analytic stories and 916 detections spanning categories such as adversary tactics, cloud security, malware, privilege escalation and vulnerability.

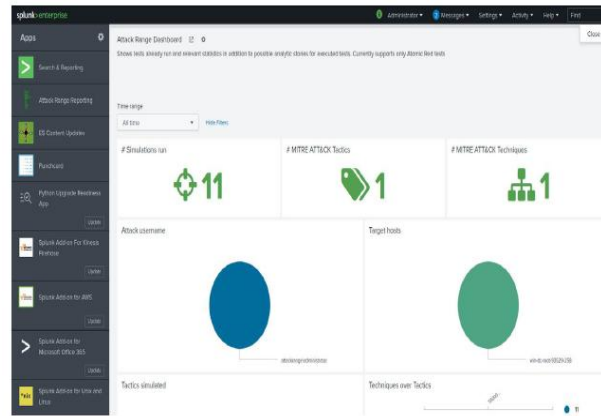


Fig. 4. Splunk Attack Range dashboard: simulations run, ATT&CK tactics and techniques, attacker user name and target hosts.

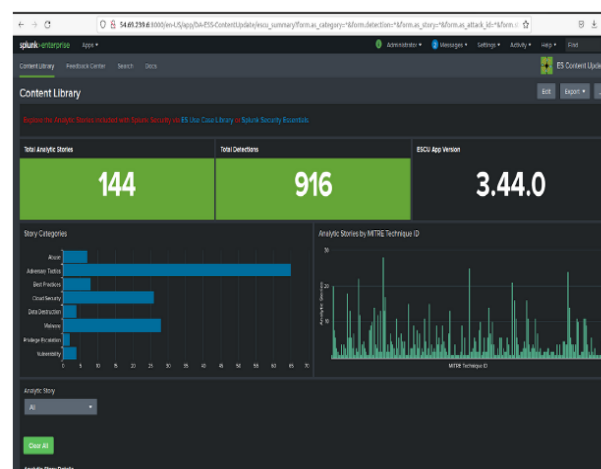


Fig. 5. Splunk ESCU content library: analytic stories, detections and stories by MITRE technique ID.

Suricata detected and alerted on the simulated attacks, and its alerts were visible in Splunk. Its effectiveness can be improved further by tuning thresholds and rule sets and by keeping threat-intelligence feeds current, which also reduces false positives. The dashboards let analysts trace compromised accounts and hosts and see which ATT&CK technique was in play, which supports both response and the refinement of defensive strategy.

TABLE 3

Summary of Experimental Findings

Environment	Evidence	Outcome
AWS resilience testbed	95% detection; response < 5 min	Incidents contained; alerts real time
AWS health monitoring	CPU peak ≈ 0.01 ; stable network	No sustained resource exhaustion
Attack Range v2	11 simulations; 1 tactic, 1 technique	Mapped to ATT&CK (T1003.002)
Suricata + Splunk	Alerts on simulated attacks	Detection shown; tuning advised

C. Discussion

Two complementary results emerge. In the AWS testbed the resilience mechanisms delivered a high, measurable detection rate with fast response, which confirms that detection and response workflows can be quantified through MTDD, MTTR and detection accuracy. In the integrated environment, iCTI demonstrated that threat data from several sources, network telemetry and a SOC toolchain can be combined, so that simulated attacks are detected, mapped to ATT&CK and presented to analysts with context. Together they support the thesis that intelligence makes resilience proactive: it turns TTP knowledge into controls and response plans before an incident occurs.

VI. CHALLENGES AND LIMITATIONS

A. Technical Challenges

Data quality, scalability of stream and batch processing, and computational cost are persistent concerns, as are false positives that burden analysts and adversarial evasion of learned detectors. [17], [24] Black-box models also limit trust, which makes explainable approaches attractive. [25]

B. Organizational and Ethical Challenges

A shortage of skilled staff, limited budgets, compliance requirements and change management slow adoption. Collecting and sharing intelligence raises privacy, fairness and transparency questions, and legal obstacles and a lack of standardization hinder exchange between organizations. [26]

C. Limitations of This Study

The experiments were run in controlled and production-like testbeds with simulated attacks, which cannot reproduce the complexity of real campaigns. The AWS evaluation reports a detection rate and an average response time but not the number of simulated threats, and the Attack Range run exercised a single ATT&CK technique. Quantitative detection and false-positive rates of the full iCTI pipeline against varied attack types were not measured and should be established in future work.

VII. FUTURE SCOPE

Future work includes proactive threat hunting on top of the iCTI pipeline, standardized sharing protocols and collaboration with external entities to build collective defense, richer visualization of intelligence, and privacy-preserving and ethical handling of shared data. Broader attack coverage (many ATT&CK tactics and techniques) with repeated runs and reported detection and false-positive rates, and the use of AI and blockchain to standardize and secure CTI collection and sharing, are further directions.

VIII. CONCLUSION

This paper presented iCTI, an architecture that integrates a cyber-resilience framework with a multi-source CTI pipeline to provide proactive defense and faster incident response. In a controlled AWS environment the resilience mechanisms detected 95% of simulated threats with an average response time below five minutes, and in a production-like environment the architecture worked with SIEM, IDS/IPS, endpoint, firewall, vulnerability and threat-intelligence tools while simulated attacks were detected and mapped to MITRE ATT&CK. By grounding defenses in adversary TTPs and supplying actionable intelligence during incidents, iCTI helps organizations prevent, detect and recover from attacks and make better-informed security investments. Broader, quantitatively reported evaluation is the next step.

REFERENCES

- [1] K. Hausken, "Cyber resilience in firms, organizations and societies," *Internet of Things*, vol. 11, 2020.
- [2] A. Annarelli, F. Nonino, and G. Palombi, "Understanding the management of cyber resilient systems," *Comput. Ind. Eng.*, vol. 149, 2020.

- [3] J. Pavão, R. Bastardo, D. Carreira, and N. P. Rocha, "Cyber resilience, a survey of case studies," *Procedia Comput. Sci.*, vol. 219, pp. 312–318, 2023.
- [4] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," arXiv:2103.03530, 2021.
- [5] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber threat intelligence sources, formats and languages," *Electronics*, vol. 9, no. 5, p. 824, 2020.
- [6] S. Colabianchi, F. Costantino, G. di Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Comput. Ind. Eng.*, vol. 160, 2021.
- [7] D. Bodeau, R. Graubart, J. Picciotto, and R. McQuaid, "Cyber resiliency engineering framework," The MITRE Corporation, 2011.
- [8] E. G. Carayannis, E. Grigoroudis, S. S. Rehman, and N. Samarakoon, "Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience," *IEEE Trans. Eng. Manag.*, vol. 68, no. 2, pp. 223–234, 2021.
- [9] J. F. Carías *et al.*, "Cyber resilience self-assessment tool (CR-SAT) for SMEs," *IEEE Access*, vol. 9, pp. 80741–80762, 2021.
- [10] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Comput. Secur.*, vol. 97, 2020.
- [11] A. Kott and I. Linkov, "To improve cyber resilience, measure it," *Computer*, vol. 54, pp. 80–85, 2021.
- [12] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environ. Syst. Decis.*, vol. 33, pp. 471–476, 2013.
- [13] E. Alvarenga *et al.*, "Cyber resilience for the Internet of Things: Implementations with resilience engines and attack classifications," *IEEE Trans. Emerg. Topics Comput.*, 2022.
- [14] A. Salvi, P. Spagnoletti, and N. S. Noori, "Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem," *Comput. Secur.*, vol. 112, 2022.
- [15] I. Alkinj, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "CTI-CORE: A cyber threat intelligence framework for big data analysis," *IEEE Access*, vol. 9, pp. 98404–98415, 2021.
- [16] D. Bucur and V. Sgârciu, "Big data analytics and machine learning for cyber threat intelligence: A survey," *Sensors*, vol. 21, no. 15, 2021.
- [17] L. Zhang, X. Yao, S. Liu, S. Liu, and H. Li, "A SOAR and CTI framework with big data technologies," *IEEE Access*, vol. 8, pp. 151379–151388, 2020.
- [18] P.-C. Lin *et al.*, "Correlation of cyber threat intelligence with sightings for intelligence assessment and augmentation," *Comput. Netw.*, vol. 228, 2023.
- [19] X. Shu *et al.*, "Threat intelligence computing," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 1883–1898.
- [20] L. Bilge, Y. Han, and M. Dell'Amico, "RiskTeller: Predicting the risk of cyber incidents," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 1299–1311.
- [21] M. Du, F. Li, G. Zheng, and V. Srikumar, "DeepLog: Anomaly detection and diagnosis from system logs through deep learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 1285–1298.
- [22] F. Pierazzi, S. Casolari, M. Colajanni, and M. Marchetti, "Exploratory security analytics for anomaly detection," *Comput. Secur.*, vol. 56, pp. 28–49, 2016.
- [23] V. S. Devi Priya and S. C. Sethuraman, "Containerized cloud-based honeypot deception for tracking attackers," *Sci. Rep.*, 2023.
- [24] M. Gopinath and S. C. Sethuraman, "A comprehensive survey on deep learning based malware detection techniques," *Comput. Sci. Rev.*, vol. 47, 2023.
- [25] K. Cho, J. Shin, and Y. Kim, "Enhancing cyber threat intelligence with explainable machine learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2047–2061, 2021.
- [26] N. Veerasamy, T. T. Mashiane, and K. J. Pillay, "Towards cyber incident response strategic planning," in *Proc. THREAT 2019 Cybersecurity Summit*, Sandton, South Africa, 2019.