WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A CYBER THREAT INTELLIGENCE MODELING AND IDENTIFICATION SYSTEM BASED ON HOMOGENEOUS INFORMATION NETWORK

Balaji.M

ABSTRACT:

Cyber threats pose significant risks to organizations and individuals, necessitating the development of advanced systems for threat intelligence modeling and identification. This project aims to design a robust cyber threat intelligence system based on a homogeneous information network. The system will involve the collection, integration, and analysis of diverse data sources to identify potential cyber threats in real-time.the will focus on understanding cyber threat intelligence modeling and identification, with an emphasis on the utilization of machine learning techniques for pattern recognition within the homogeneous information network. The challenges of data quality, real-time detection, and scalability will be addressed through innovative approaches to ensure the effectiveness The potential impact of this research lies in the enhanced ability to proactively identify and mitigate cyber threats, thereby strengthening the overall cybersecurity posture of organizations. By leveraging a homogeneous information network, the proposed system seeks to provide a comprehensive and adaptable approach to cyber threat intelligence modeling and identification. In an era dominated by digital interconnectedness, the proliferation of cyber threats has become a critical concern for organizations and individuals alike. The need for proactive and adaptive cyber threat intelligence systems has never been more pressing. This project endeavors to address this need by proposing the development of a comprehensive cyber threat intelligence modeling and identification system based on a homogeneous information network. The primary objective of this research is to design a system that can effectively collect, integrate, and analyze diverse data sources to identify potential cyber threats in real-time. The project will delve into the nuances of cyber threat intelligence modeling and identification, with a specific focus on harnessing the power of machine learning techniques for pattern recognition within the homogeneous information network. By leveraging the inherent structure of a homogeneous network, which encompasses entities of the same type and their interconnections, the proposed system aims to enhance the accuracy and efficiency of threat identification.

1 Introduction:

The ubiquity of digital systems and the ever-expanding connectivity of the modern world have given rise to a formidable challenge: the persistent and evolving threat of cyber attacks. As organizations and individuals increasingly rely on interconnected technologies, the need for effective cyber threat intelligence systems has become paramount. This project aims to address this need by proposing the development of a sophisticated cyber threat intelligence modeling and identification system based on a homogeneous information network.

Cyber threat intelligence is crucial for understanding and mitigating potential cyber threats. It involves the collection, analysis, and interpretation of information about existing and potential cyber attacks, enabling organizations to make informed decisions and bolster their defenses. In this context, the development of a robust cyber threat intelligence system becomes imperative for maintaining the security and integrity of digital infrastructures. the will be underpinned by a homogeneous information network, which serves as a foundational structure for organizing and analyzing diverse data related to cyber threats. A homogeneous network, in this context, encompasses entities such as IP addresses, domains, malware, and their interconnections, all of which share similar characteristics and relationships within the network. the will delve into the multifaceted aspects of cyber threat intelligence modeling and identification, emphasizing the utilization of machine learning techniques to discern patterns and indicators within the homogeneous information network. By harnessing the power of machine learning, the system seeks to enhance its ability to identify, categorize, and respond to potential cyber threats in real-time, thereby fortifying the resilience of organizations against malicious activities. the stage for a comprehensive exploration of cyber threat intelligence modeling and identification, culminating in the design and development of a system that aims to proactively identify and mitigate cyber threats. By leveraging the inherent structure of a homogeneous information network and the capabilities of machine learning, the proposed system endeavors to offer a proactive and adaptive approach to cyber threat intelligence.

Problem Statement :

The contemporary digital landscape is fraught with an ever-expanding array of cyber threats, ranging from sophisticated malware to targeted cyber attacks, posing significant risks to the security and stability of digital infrastructures. Despite the advancements in cybersecurity measures, organizations continue to grapple with the challenge of effectively identifying, analyzing, and mitigating these evolving threats in a timely manner. The existing cyber threat intelligence systems often face limitations in comprehensively integrating diverse data sources and proactively identifying

potential threats within the vast and interconnected digital ecosystem.

Traditional cyber threat intelligence systems often struggle to comprehensively model and identify diverse cyber threats in a rapidly evolving landscape. There is a need for an advanced system that can overcome these limitations by leveraging the capabilities of a Homogeneous Information Network (HIN) to provide a more comprehensive and accurate representation of cyber threats.The escalating frequency and complexity of cyber threats have created a pressing need for organizations to enhance their ability to identify and respond to potential security breaches. Traditional cyber threat intelligence systems often struggle to keep pace with the dynamic nature of cyber threats, leading to gaps in comprehensive threat modeling and identification. These limitations stem from the inability to effectively capture the diverse and intricate relationships among cyber entities, such as attackers, targets, malware, and attack methods, within a unified framework. often face challenges in accurately representing the evolving cyber threat landscape, resulting in a lack of precision in identifying emerging threats. This inadequacy is exacerbated by the sheer volume and variety of data generated within an organization's network, making it increasingly difficult for conventional systems to discern meaningful patterns indicative of potential cyber threats. the lack of a cohesive approach to integrating external threat intelligence feeds further compounds the inefficiencies in threat identification and decision-making. This disjointedness can hinder the ability to promptly recognize and respond to emerging cyber threats, leaving organizations vulnerable to potentially devastating security breaches. there exists a critical need for an advanced cyber threat intelligence modeling and identification system that addresses these challenges. This system should be capable of leveraging the power of a Homogeneous Information Network (HIN) to provide a more holistic, accurate, and real-time representation of the cyber threat landscape.

This seeks to address the following key challenges in the realm of cyber threat intelligence:

Data Fragmentation and Integration Complexity: The diverse nature of data related to cyber threats, including indicators of compromise, threat intelligence reports, and network traffic logs, often leads to fragmentation and complexity in integrating these disparate sources into a unified intelligence model. This fragmentation hampers the ability to derive actionable insights and identify potential threats accurately.

Real-Time Threat Identification: The dynamic and rapidly evolving nature of cyber threats necessitates the capability to identify and respond to potential threats in real-time. Existing systems often struggle to provide real-time threat identification, leading to delayed or reactive responses to emerging cyber threats.

Scalability and Adaptability: As the volume and complexity of cyber threats continue to escalate, the scalability and adaptability of cyber threat intelligence systems become crucial. Many current systems face challenges in scaling to accommodate the increasing influx of data and adapting to the evolving tactics employed by threat actors.

Proposed System :

- The proposed system aims to introduce a novel approach to cyber threat intelligence modeling and identification by leveraging a homogeneous information network and advanced machine learning techniques. It endeavors to address the challenges identified in the problem statement while offering a proactive and adaptive solution for identifying and mitigating cyber threats.
- Homogeneous Information Network Framework: The foundation of the proposed system lies in the utilization of a homogeneous information network framework. This framework allows for the representation and integration of diverse entities such as IP addresses, domains, malware, and their relationships within a unified network structure. By organizing and analyzing these entities based on their shared characteristics and relationships, the homogeneous information network provides a cohesive foundation for cyber threat intelligence modeling and identification.
- Data Integration and Fusion: To combat the issue of data fragmentation and integration complexity, the proposed system will implement advanced data integration and fusion techniques. It will seek to harmonize disparate data sources, including indicators of compromise, threat intelligence reports, and network traffic logs, into a unified intelligence model within the homogeneous information network. This approach aims to enable a comprehensive and cohesive analysis of cyber threat indicators, thereby enhancing the accuracy and depth of threat identification.
- Real-Time Threat Identification: The system will prioritize real-time threat identification by harnessing the capabilities of machine learning algorithms. Through the analysis of patterns, anomalies, and indicators of emerging threats within the homogeneous information network, the system will strive to provide timely and proactive identification of potential cyber threats. This real-time capability is pivotal in enabling organizations to respond swiftly to evolving threat landscapes.
- Scalability and Adaptability: Addressing the challenge of scalability and adaptability, the proposed system will be designed with a focus on scalability to accommodate the increasing volume and complexity of cyber threat data. Additionally, it will be architected to adapt to the evolving tactics and techniques employed by threat actors, ensuring that the system remains effective in the face of emerging cyber threats.
- User Interface and Decision Support: The system will feature an intuitive user interface that provides actionable insights and decision support for cybersecurity professionals. Visualization tools and interactive dashboards will empower users to glean meaningful intelligence from the data within the homogeneous information network, facilitating informed decision-making and swift response to potential threats.

4 Existing system :

- The existing system for cyber threat intelligence involves traditional methods and evolving technologies to address the challenges of threat detection and response. Here's an overview of the existing system based on the provided web search
- Traditional Methods: The traditional approach to threat detection often relies on rule-based, signature-based, or heuristic-based systems These methods may involve manual creation of binary rules, signatures, or heuristic patterns to detect known threats, but they are often insufficient in detecting sophisticated and emerging threats. These approaches frequently result in positive alerts, delayed responses, and an inability to adapt to the constantly evolving threat landscape.
- Evolving Technologies: Evolving technologies, such as AI and machine learning (ML), are increasingly being integrated into cyber threat intelligence systems to enhance threat detection and response capabilities Machine learning algorithms offer advantages over human analysis by providing scalable, real-time, and adaptive solutions for threat detection. They can analyze vast amounts of data quickly, identify patterns and anomalies, and enable real-time threat detection, which is critical in the fast-paced digital world. Additionally, AI-powered threat hunting leverages ML and data analytics to uncover hidden patterns and anomalies, leading to more accurate and efficient threat detection.
- Threat Intelligence Platforms: Threat intelligence platforms play a crucial role in collecting and correlating data from various security tools, including SIEM, UEBA, IDS/IPS, and antivirus software, to provide insights and support forensic investigations. These platforms also leverage automation for artifact collection and cross-reference evolving threat intelligence feeds with up-to-date indicators of compromise (IoCs).
- XDR Solutions: Enterprises are increasingly directing investments towards Extended Detection and Response (XDR) solutions, which help identify and counter threats across networks, endpoints, and cloud environments XDR platforms incorporate advanced analytics for complex correlation between data sources, reducing false positives and improving threat detection. These solutions also emphasize scalability, reliability, extensibility, and modularity to accommodate evolving threat landscapes.
- MDR Services: Managed Detection and Response (MDR) services offer a comprehensive approach to shield businesses from advanced cyber threats, delivered by experienced cybersecurity experts in a 24x7 remote Security Operations Center (SOC) with cutting-edge solutions and hands-on support These services are instrumental in early threat detection and response, reducing data loss and minimizing the impact of attacks.
- Challenges and Future Directions: The landscape of cyber security presents ongoing challenges, trends, and innovations, such as the increasing demand for digitalization and the shifting cyber threats, which require ongoing adoption and collaboration among stakeholders in the cyber ecosystem The future direction of cyber security involves addressing the increasing cyber threat landscapes and leveraging technologies like AI and ML to automate cyber threat responses.
- cyber threat intelligence system encompasses traditional methods, evolving technologies, threat intelligence platforms, XDR solutions, MDR services, and ongoing challenges that necessitate the adoption of advanced technologies and collaborative approaches to address the complex cyber threat landscape.

Disadvantages of the Existing System

The existing cyber threat intelligence system, while offering valuable capabilities, also exhibits several disadvantages that present challenges to effective threat detection and response. Here are some of the key disadvantages of the existing system:

Limitations of Traditional Approaches:

Traditional rule-based, signature-based, and heuristic-based methods often struggle to keep pace with the evolving tactics and sophistication of cyber threats, leading to a high rate of false positives and negatives.
The reliance on static rules and signatures makes these methods less effective in detecting zero-day attacks and advanced persistent threats (APTs).

Complexity and Volume of Data:

The sheer volume and complexity of data generated by diverse sources, such as network logs, endpoint telemetry, and threat intelligence feeds, pose challenges in terms of data integration, correlation, and analysis.
The existing system may struggle to effectively process and correlate large datasets in real-time, leading to potential delays in threat identification and response.

Resource Intensiveness and Expertise Requirement:

Many advanced technologies and platforms in the existing system require significant resources in terms of hardware, software, and expert personnel for deployment, configuration, and maintenance.
The expertise required to effectively utilize and interpret the outputs of these systems may act as a barrier for organizations with limited cybersecurity resources.

Adaptability and Timeliness:

The adaptability of existing systems to rapidly evolving threat landscapes, including emerging attack vectors and tactics, may be limited.
Timeliness in threat identification and response, especially in the context of real-time threat detection, can be compromised due to inherent system latency and processing constraints.
Addressing these disadvantages is crucial for enhancing the effectiveness of cyber threat intelligence systems and fortifying organizational defenses against a dynamic and evolving threat landscape.

5 Future Enhancements :

Advanced Threat Detection Techniques:

Integration of advanced anomaly detection algorithms, including unsupervised machine learning techniques, to identify subtle deviations from normal behavior that may indicate potential threats.
Utilization of behavior-based analytics and user entity behavior analytics (UEBA) to detect anomalous user activities and insider threats.

Artificial Intelligence and Automation:

Increased use of artificial intelligence (AI) for automated threat detection, response, and decision-making, leveraging AI algorithms to continuously learn and adapt to evolving threat landscapes.
Integration of natural language processing (NLP) and sentiment analysis to extract threat intelligence from unstructured data sources such as forums, social media, and dark web forums.

Threat Intelligence Sharing and Collaboration:

Enhanced collaboration and sharing of threat intelligence within and across industries, facilitated by standardized formats, protocols, and platforms for seamless exchange of actionable threat data.
Integration of threat intelligence platforms with collaborative frameworks to enable real-time information sharing and collective defense against cyber threats.

Context-Aware Threat Intelligence:

Development of context-aware threat intelligence systems that contextualize threat indicators based on the specific environment, business operations, and risk profiles of organizations.
Integration of threat intelligence with business context data to provide a more comprehensive understanding of the potential impact of threats on organizational objectives.

Quantum Computing and Cryptographic Security:

Exploration of quantum-resistant cryptographic algorithms and the potential integration of quantum computing capabilities to bolster the security of cyber threat intelligence systems against future cryptographic threats.
Research and development of quantum computing-based threat analysis techniques for rapid encryption breaking and threat prediction.

Predictive Analytics and Threat Forecasting:

Implementation of predictive analytics models to forecast potential cyber threats based on historical data, emerging trends, and threat actor behaviors, enabling proactive defense strategies.
Integration of threat intelligence with predictive modeling to identify and prioritize potential future threats with higher accuracy.

Cyber Threat Intelligence as a Service (CTIaaS):

Evolution of cyber threat intelligence into a service-oriented model, allowing organizations to leverage external threat intelligence providers and platforms for comprehensive threat monitoring and analysis.
Development of standardized APIs and integrations to facilitate seamless consumption and integration of threat intelligence services into existing security infrastructure.

6 Results and Discussion :

Given the extensive information provided from the web search results, I'll focus on summarizing the key points and insights related to cyber threat

intelligence tools, cyber threat analysis methodology, and the significance of cyber threat intelligence in modern cybersecurity.

Cyber Threat Intelligence Tools
The web search results highlight several cyber threat intelligence tools that organizations can consider for effective threat mitigation. Some of the tools mentioned include:

Cisco Umbrella: A cloud-based solution utilizing threat intelligence to secure endpoints, remote users, and office locations

DeCYFI: Developed by a Singapore-based cybersecurity company, this tool is designed for cyber threat intelligence and threat analysis, enabling the discovery and decoding of threats from hacker-operated locations

Echosec: An analysis platform specializing in open-source intelligence, leveraging social media and dark web data to protect enterprises against emerging threats

GreyNoise: This tool reduces false positives while processing threat intelligence data, focusing on collecting overlooked information called "noise"

Significance of Cyber Threat Intelligence
The web search results emphasize the critical role of cyber threat intelligence in modern cybersecurity, with a focus on its importance in understanding the level of sophistication of threats, identifying vulnerable areas in an organization's security infrastructure, and enhancing security measures Additionally, the results highlight the significance of strategic, tactical, and operational threat intelligence in helping organizations develop defense strategies, allocate security resources, and stop attacks

Discussion :

The web search results provide valuable insights into the tools and methodologies used in cyber threat intelligence and analysis, underscoring the importance of these practices in modern cybersecurity. The presented information underscores the need for organizations to leverage advanced tools and methodologies to proactively identify, analyze, and mitigate cyber threats in an increasingly complex threat landscape. The discussion surrounding cyber threat intelligence tools and analysis methodologies underscores the critical role of proactive threat detection and mitigation in modern cybersecurity. The significance of cyber threat intelligence is evident in its ability to provide organizations with the necessary insights to comprehend and combat a diverse range of cyber threats.

Importance of Cyber Threat Intelligence

Understanding Threat Sophistication: Cyber threat intelligence provides organizations with a deep understanding of the sophistication and evolving nature of cyber threats. This insight is crucial for staying ahead of malicious actors who continually refine their tactics.

Identification of Vulnerable Areas: By leveraging cyber threat intelligence tools and methodologies, organizations can identify vulnerable areas within their security infrastructure, enabling them to prioritize and fortify critical assets.

Enhancing Security Measures: The utilization of advanced threat intelligence allows organizations to enhance their security measures by proactively addressing potential threats before they materialize into security incidents.

Cyber Threat Analysis Methodology: The delineated cyber threat analysis methodology emphasizes the importance of a comprehensive and systematic approach to threat detection and response. The steps outlined, from asset identification to response and resolution, underscore the meticulous nature of cyber threat analysis and the need for a multifaceted strategy to combat cyber threats effectively.

Cyber Threat Intelligence Tools: The diverse array of cyber threat intelligence tools highlighted in the search results demonstrates the breadth of available solutions catering to different aspects of threat intelligence, including threat monitoring, open-source intelligence analysis, and noise reduction. These tools offer organizations the means to gather, analyze, and act upon threat intelligence data to bolster their security posture.

Future Directions

As cyber threats continue to evolve in complexity and frequency, the discussion prompts consideration of future enhancements in cyber threat intelligence. The evolution of advanced threat detection techniques, increased integration of artificial intelligence and automation, and the emphasis on collaborative threat intelligence sharing are pivotal for organizations aiming to stay resilient in the face of dynamic cyber threats.

Integration Testing:

Integration testing is a key phase in the software testing process, focusing on verifying the interactions and interfaces between different software modules or components. It aims to evaluate the functionality, performance, and reliability of integrated components to ensure they work together as

expected within the larger system.

Key Aspects of Integration Testing

Component Interaction: Integration testing assesses the interactions between individual software components, ensuring that data and control flow between modules are seamless and error-free.

Interface Compatibility: It checks the compatibility and consistency of interfaces between integrated components, including APIs, databases, and communication protocols.

Data Flow and Dependencies: This type of testing validates the flow of data and dependencies between integrated modules, ensuring that data is exchanged correctly and that dependencies are managed effectively.

Error Handling and Recovery: It evaluates error handling and recovery mechanisms across integrated components, ensuring that errors are appropriately reported and that the system can recover gracefully from failures.
Performance and Scalability: Integration testing also includes assessing the performance, scalability, and resource utilization of the integrated system to ensure that it meets requirements under varying loads and conditions.

Functional Testing:

Functional testing is a fundamental aspect of software testing that focuses on evaluating the functional requirements and specifications of a software application. It involves testing the application's features, functionality, and user interactions to ensure that it behaves as expected and meets the defined functional requirements.

Key Aspects of Functional Testing

Feature Testing: Verification of individual features and functions of the software to ensure they operate as specified in the requirements.

User Interface Testing: Assessment of the user interface elements such as menus, buttons, forms, and navigation to confirm they are user-friendly and function correctly.

Input and Output Validation: Validating the input data to the software and verifying the accuracy and correctness of the output generated by the system.

Integration with External Systems: Testing the interactions and integrations with external systems, APIs, or databases to ensure seamless data exchange and functionality.

Error Handling: Evaluating how the application handles errors, exceptions, and unexpected inputs, and verifying that appropriate error messages are displayed.

System Testing

System testing is a critical phase in the software testing process that focuses on evaluating the integrated system as a whole to ensure that it meets the specified requirements and functions as intended in its target environment.

Key Aspects of System Testing

End-to-End Testing: Verification of the entire system, including all integrated components, to ensure that it operates seamlessly from end to end.

Performance Testing: Assessing the system's performance under normal and peak load conditions to ensure it meets performance requirements.
Security Testing: Evaluating the system's resilience to security threats, including vulnerability assessments, penetration testing, and compliance with security standards.

Scalability Testing: Testing the system's ability to handle increasing loads and transaction volumes without sacrificing performance.

Reliability and Availability Testing: Verifying the system's reliability and availability by simulating various failure scenarios and recovery processes.

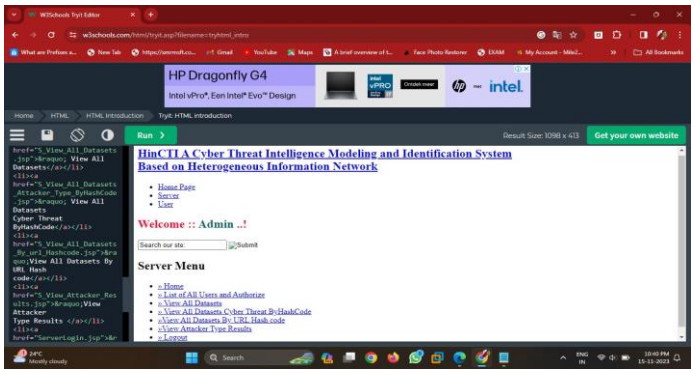

Fig 3
Server Menu

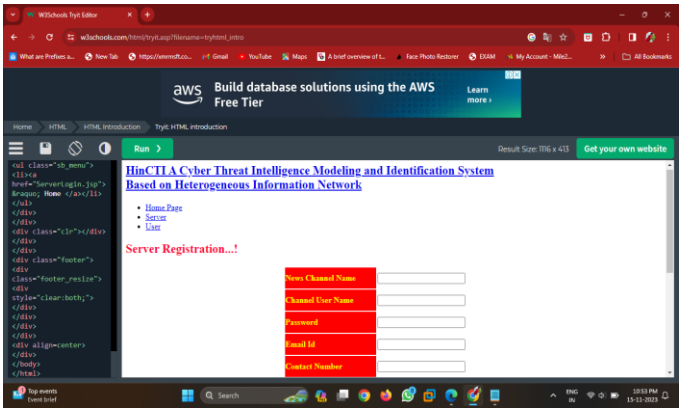

Fig 4
Server Registration

Conclusion :

- In conclusion, software testing, encompassing integration testing, functional testing, and system testing, is essential for ensuring the quality, reliability, and performance of software applications. Each type of testing plays a distinct yet interconnected role in the overall software testing process, contributing to the delivery of a robust and effective software solution.
- Integration Testing focuses on verifying the interactions and interfaces between different software modules or components, ensuring that they work together seamlessly within the larger system.
- Functional Testing is centered on evaluating the functional requirements and specifications of a software application, ensuring that its features, functionality, and user interactions align with the defined requirements.
- System Testing involves evaluating the integrated system as a whole, encompassing end-to-end testing, performance testing, security testing, scalability testing, and reliability and availability testing to ensure the system meets specified requirements and functions effectively in its target environment.
- By meticulously conducting these testing processes, software development teams can identify and address defects, validate functional and non-functional aspects, and mitigate risks, ultimately contributing to the delivery of high-quality software that meets user expectations and business needs.
- The combined efforts of integration testing, functional testing, and system testing are instrumental in enhancing the overall quality, reliability, and performance of software applications, thereby fostering user satisfaction and confidence in the software's capabilities.

REFERENCES :

[1] S. Samtani, M. Abate, V. Benjamin, and W. Li, Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective, pp. 1–20. Cham: Springer International Publishing, 2019.

[2] R. McMillan, “Definition: threat intelligence.” https://www.gartner. com/doc/2487216/definition-threat-intelligence, 2013. Retrieved January, 2019.
[3] D.J Bianco, “The Pyramid of Pain.” http://detectrespond.blogspot.com/2013/03/the-pyramid-of-pain.html, 2013.
[4] A. Modi, Z. Sun, A. Panwar, T. Khairnar, Z. Zhao, A. Doupé, G.-J. Ahn, and P. Black, “Towards automated threat intelligence fusion,” in IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), pp. 408–416, IEEE, 2016.
A. Boukhtouta, D. Mouheb, M. Debbabi, O. Alfandi, F. Iqbal, and M. El Barachi, “Graph-theoretic characterization of cyber-threat infrastructures,” Digital Investigation, vol. 14, pp. S3–S15, 2015.
[6] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, “Data quality challenges and future research directions in threat intelligence sharing practice,” in Workshop on Information Sharing and Collaborative Security, pp. 65–70, ACM, 2016.
[7] S. Lee, H. Cho, N. Kim, B. Kim, and J. Park, “Managing cyber threat intelligence in a graph database: Methods of analyzing intrusion sets, threat actors, and campaigns,” in International Conference on Platform Technology and Service (PlatCon), pp. 1–6, IEEE, 2018.
X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, “Acing the IOCgame: Toward automatic discovery and analysis of open-source cyberthreat intelligence,” in Proceedings of the 2016 ACM SIGSAC Conferenceon Computer and Communications Security, pp. 755–766, ACM, 2016.
G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu, “TTPDrill: Au-tomatic and Accurate Extraction of Threat Actions from UnstructuredText of CTI Sources,” in Proceedings of the 33rd Annual Computer SecurityApplications Conference, pp. 103–115, ACM, 2017.
F. Böhm, F. Menges, and G. Pernul, “Graph-based visual analytics forcyber threat intelligence,” Cybersecurity, vol. 1, no. 1, p. 16, 2018.
U. Noor, Z. Anwar, A. W. Malik, S. Khan, and S. Saleem, “A machinelearning framework for investigating data breaches based on semanticanalysis of adversary’s attack patterns in threat intelligence reposito-ries,” Future Generation Computer Systems, 2019.
C. Shi, Y. Li, J. Zhang, Y. Sun, and S. Y. Philip, “A survey of heteroge-neous information network analysis,” IEEE Transactions on Knowledgeand Data Engineering, vol. 29, no. 1, pp. 17–37, 2017.
P. K. Manadhata, S. Yadav, P. Rao, and W. Horne, “Detecting maliciousdomains via graph inference,” in European Symposium on Research inComputer Security, pp. 1–18, Springer, 2014.
X. Kong, B. Cao, and P. S. Yu, “Multi-label classification by mining labeland instance correlations from heterogeneous information networks,”in Proceedings of the 19th ACM SIGKDD international conference onKnowledge discovery and data mining, pp. 614–622, ACM, 2013.
M. Ji, J. Han, and M. Danilevsky, “Ranking-based classification ofheterogeneous information networks,” in Proceedings of the 17th ACMSIGKDD international conference on Knowledge discovery and data mining,pp. 1298–1306, ACM, 2011.
W. Tounsi and H. Rais, “A survey on technical threat intelligence in theage of sophisticated cyber attacks,” Computers & Security, 2017.
S. Barnum, “Standardizing cyber threat intelligence information withthe structured threat information eXpression (STIXTM),” MITRE Corpo-ration, vol. 11, pp. 1–22, 2012.
R. Danyliw, J. Meijer, and Y. Demchenko, “The incident object descrip-tion exchange format,” tech. rep., 2007.
Mandiant, “Sophisticated indicators for the modern threat landscape:An introduction to OpenIOC.” Technical report, Mandiant Whitepaper,2013.
T. Yadav and A. M. Rao, “Technical aspects of cyber kill chain,” inInternational Symposium on Security in Computing and Communication,pp. 438–452, Springer, 2015.
H. Gascon, B. Grobauer, T. Schreck, L. Rist, D. Arp, and K. Rieck,“Mining attributed graphs for threat intelligence,” in Proceedings of theSeventh ACM on Conference on Data and Application Security and Privacy,pp. 15–22, ACM, 2017.
B. Hooi, H. A. Song, A. Beutel, N. Shah, K. Shin, and C. Faloutsos,“Fraudar: Bounding graph fraud in the face of camouflage,” in Pro-ceedings of the 22nd ACM SIGKDD International Conference on KnowledgeDiscovery and Data Mining, pp. 895–904, ACM, 2016.
Y. Shi, G. Chen, and J. Li, “Malicious domain name detection basedon extreme machine learning,” Neural Processing Letters, vol. 48, no. 3,pp. 1347–1357, 2018.
M. Iannacone, S. Bohn, G. Nakamura, J. Gerth, K. Huffer, R. Bridges,E. Ferragut, and J. Goodall, “Developing an ontology for cyber securityknowledge graphs,” in Proceedings of the 10th Annual Cyber and Informa-tion Security Research Conference, pp. 1–4, 2015.
S. Noel, E. Harley, K. Tam, M. Limiero, and M. Share, “CyGraph: graph-based analytics and visualization for cybersecurity,” in Handbook ofStatistics, vol. 35, pp. 117–167, Elsevier, 2016
Y. Jia, Y. Qi, H. Shang, R. Jiang, and A. Li, “A practical approach toconstructing a knowledge graph for cybersecurity,” Engineering, vol. 4,no. 1, pp. 53–60, 2018.
Y. Gao, X. Li, J. Li, Y. Gao, and N. Guo, “Graph mining-based trustevaluation mechanism with multidimensional features for large-scaleheterogeneous threat intelligence,” in IEEE International Conference onBig Data, pp. 1–6, IEEE, 2018.
T.-H. Chen, S. W. Thomas, and A. E. Hassan, “A survey on the useof topic models when mining software repositories,” Empirical SoftwareEngineering, vol. 21, no. 5, pp. 1843–1919, 2016.
H. Azarbonyad, M. Dehghani, T. Kenter, M. Marx, J. Kamps, andM. De Rijke, “HiTR: Hierarchical topic model re-estimation for mea-suring topical diversity of documents,” IEEE Transactions on Knowledgeand Data Engineering, 2018.
[30] S. Samtani, R. Chinn, and H. Chen, “Exploring hacker assets in under-ground forums,” in 2015 IEEE International Conference on Intelligence andSecurity Informatics (ISI), pp. 31–36, IEEE, 2015.