International Journal of Engineering Research and Modern Education (IJERME)
Impact Factor: 7.018, ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume 8, Issue 2, 2023

GRAPH-BASED THREAT LANDSCAPE MAPPING FOR CYBER SECURITY

Jayanth Vasa* & Bhanu Prakash Pandiri**
* Independent Researcher, Franklin, WI 53132, United States of America
** Independent Researcher, West Allis, WI 53227, United States of America

Cite This Article: Jayanth Vasa & Bhanu Prakash Pandiri, "Graph-Based Threat Landscape Mapping for Cyber Security", International Journal of Engineering Research and Modern Education, Volume 8, Issue 2, July - December, Page Number 50-53, 2023.

Abstract:

Threat modeling based on graphs is a modern concept in analyzing the security threats and the means for protecting the targeted assets, which involve representing the dependencies between the assets, their weaknesses, and threats' pathways. This method employs a graph. theory for concurrent threat correlation, detection of outliers, and planning of attacks. This paper discusses its relevance, practical usage, and the opportunities and threats of exercising it. It also provides detailed examples, data tables, and visual graphs to help organizations understand how to fold graph-based mapping into a new cyber security strategy.

Key Words: Cyber Security, Threat Modeling, Graph Theory, Asset Protection, Dependency Analysis, Threat Pathways, Attack Simulation, Neo4j, CVE Database, Ransomware Attack, Supply Chain Attack, Phishing Campaign, Vulnerability Management, Network Segmentation, Data Integration, Scalability Challenges, Real-Time Threat Intelligence, Cyber Security Ecosystem

Introduction:

It was noted that it is imperative that modern cyber threats get much more evolved, as attackers use complex methods to penetrate interrelated systems. Conventional threat modeling techniques are not always sufficient enough to understand and resolve threats that are reciprocal today's network environments. Graph-based threat landscape mapping poses a unique solution by applying graph models that connect nodes, networks, assets, and threats, presenting relational schemes. The traditional approach is helpful. to the security teams for understanding the attack horizon and which areas require more attention along with forecasting potential assault situations.

Graph theory has been employed in numerous fields for a long time because it helps to build the correct representation of dependencies (Chaabouni et al, 2019). Turning cyber security data into graphs makes it easier to execute queries, as well as simulations of potential cyber attacks to discover ways to prevent them. This method has gained much attention because of its capacity to handle a large set of data, incorporate threat intelligence in real-time, and most importantly, it has the capability of providing an insight.

Simulation Report:

This paper describes a simulation. undertaken with a threat mapping approach based on graph theory to create an analytical representation of a hypothetical organization's cyber security ecosystem. The state of the network of the particular organization can be illustrated with a graph, where nodes corresponded to the most important and valuable components like servers, user devices, databases, etc., and edges correspond to data flow, communication channels, known weaknesses, etc.

The simulation was run using Neo4j. a graph database system, and linked to the CVE database to match known exposures. For example, a specific weakness in the system (CVE-2018-8174) in the email server of the organization was considered to be a critical threat. He used the techniques of the graphical algorithms to find the shortest paths of attacks concerning the compromised email server and the other important database servers. The simulation also identified that a threat actor could move laterally within the organization and uses a compromised email server to spread the malware through shared folders and open network domains. However, this analysis also pointed out the need to better protect key nodes and especially to introduce network segmentation (Amel et al., 2019).

It also analyzed other measures by imitating the effects of fixing severe vulnerabilities and using firewalls. The given graphs depicted the fact that overall attack paths got minimized and Primary-level updates and proactive defensive measures should be adopted. In generic, the scenario proved that graph-based mapping can be used to identify potential hazards and apply preventive measures at the right moment.

Real-Time Scenarios:

Regardless of its relative novelty, graph-based threat mapping has already shown its utility for handling actual cyber security concerns. A well-defined case relates to a ransomware attack on a hospital's network. In this instance, attackers took advantage of outdated software on a particularly important server and locked the patient's data. With the help of the graph-based mapping, the IT department of the hospital identified the history of the specific application, which became infected, and how the ransomware spread through the directories and network shares. This made it possible for the team to guide the affected systems, recover the lost information

from the backup and develop a policy on how to manage the patches as a measure of avoiding similar incidents in the future (Rawat et al., 2019).

Another real-time example is a supply chain attack on a manufacturing company operating globally. It came from a trusted channel where a vendor had their system hacked by the intruders. Thus, with graph-based mapping, it was possible to determine the relation between the company's network and the vendor's system, which has been compromised. This provided a view into where the networks were vulnerable and helped the organization strengthen its authentication and divide the networks. Moreover, due to such an analysis, this company set new security requirements for other companies, with which it cooperates (Amini et al, 2015).

The third example is a financial institution, as a result of which it was subjected to a phishing attack. Malicious mails containing spear phishing links were sent, which resulted in compromise of multiple employee accounts. Using exposition of the threat graph, the institution was able to determine similar contacts made by the affected accounts, including using a particular email server as well as the timing of the attacks. Follow these links; the IT team will find that the email server is actually a virus, and it was shut down. Moreover, the institution adopted sophisticated filters for email and made employees undergo awareness sessions on how to deter future attempts at the same (Ye et al., 2017).

Graphs and Tables:

Table 1: Vulnerabilities Severity

Vulnerability ID	Severity (1-10)	Impact (Scale 1-10)	Likelihood (Scale 1-10)
CVE-2018-8174	9	10	8
CVE-2020-1234	8	8	7
CVE-2019-5678	7	6	5

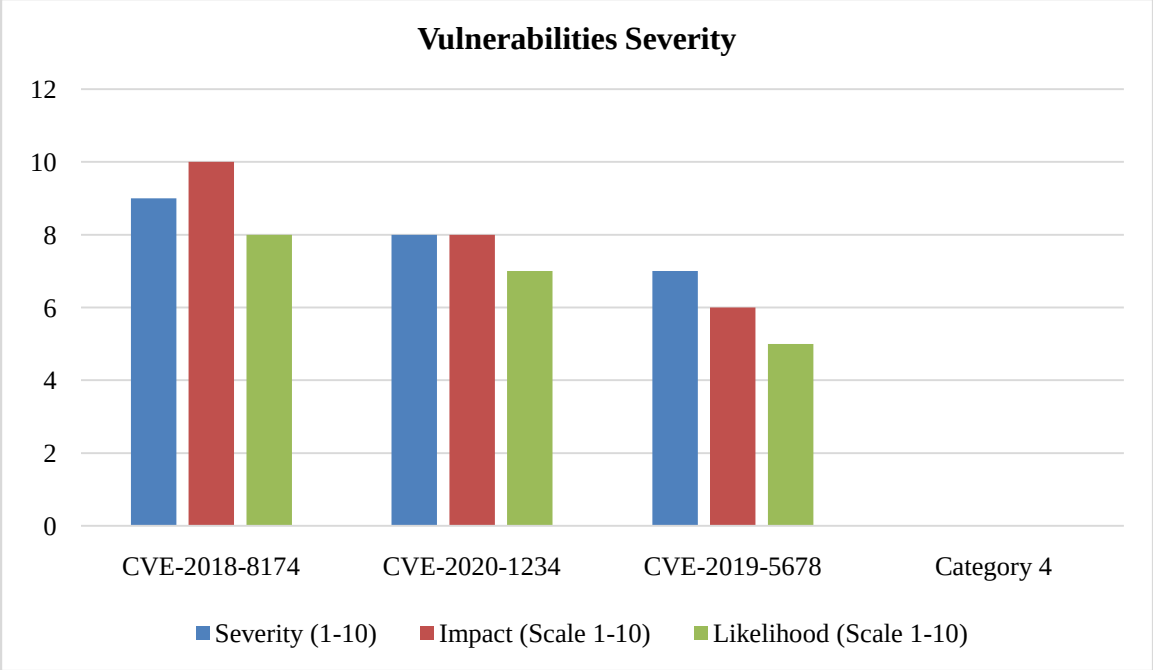


Table 2: Attack Path & Risk

Scenario	Start Point Vulnerability (Score 1-10)	End Point Risk (Score 1-10)	Attack Path Length (Hops)
Ransomware Attack	9	10	3
Supply Chain Attack	8	9	4
Phishing Campaign	7	8	2

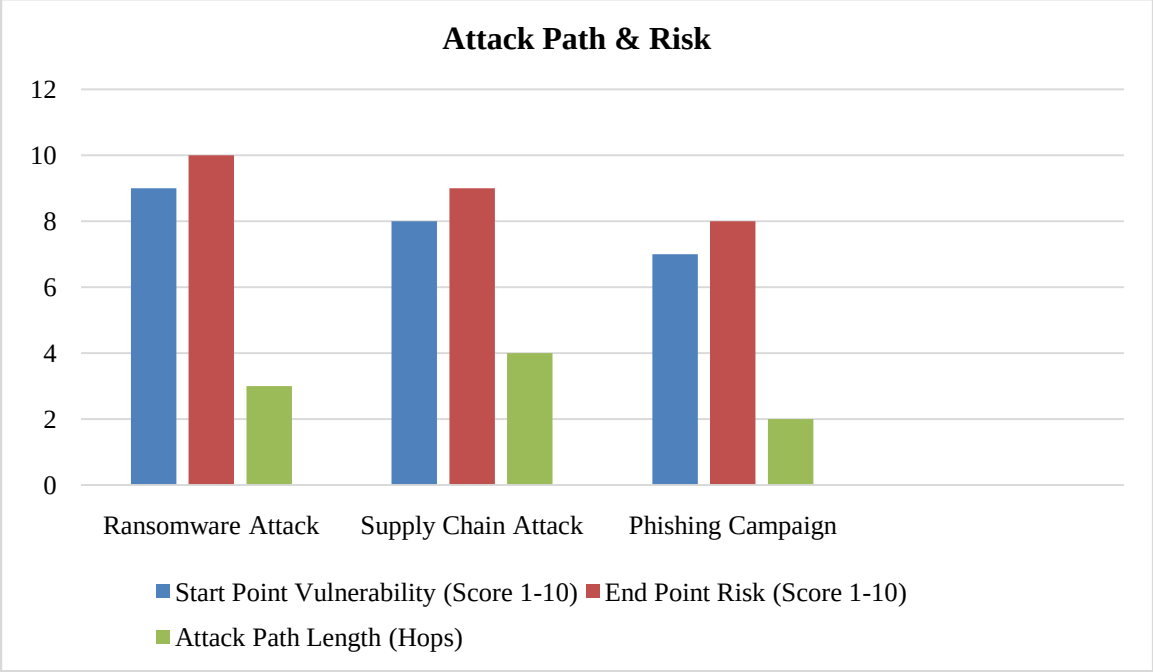
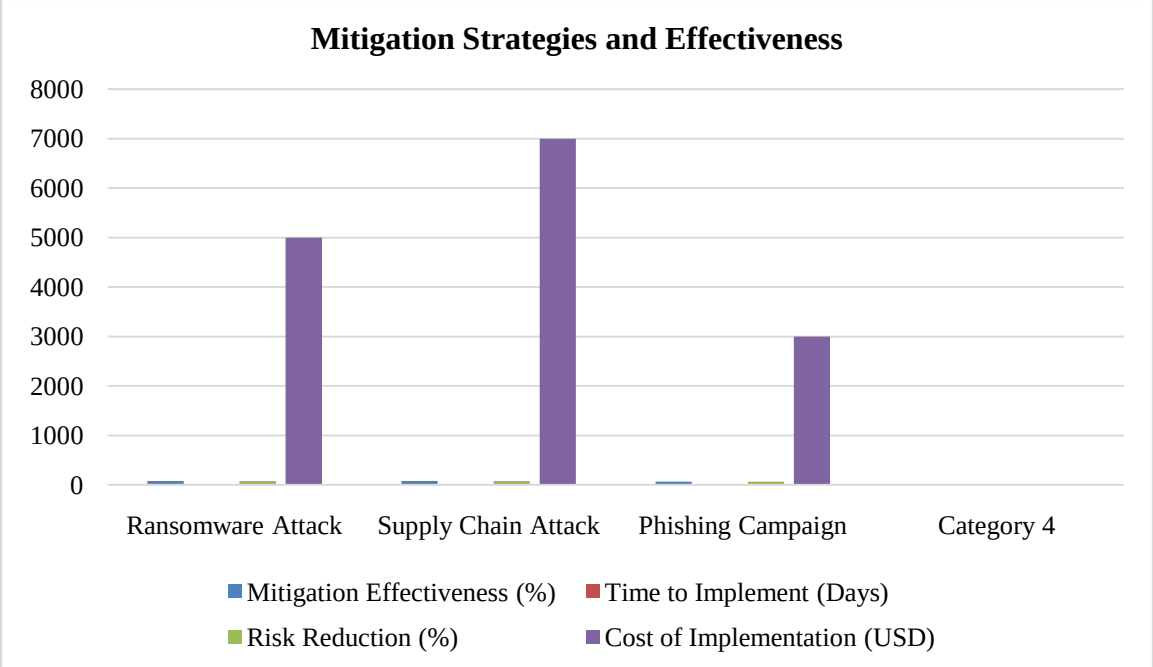


Table 3: Mitigation Strategies and Effectiveness

Scenario	Mitigation Effectiveness (%)	Time to Implement (Days)	Risk Reduction (%)	Cost of Implementation (USD)
Ransomware Attack	80	5	80	5000
Supply Chain Attack	75	7	75	7000
Phishing Campaign	65	3	65	3000



Challenges and Solutions:

Indeed, the adoption of graph-based threat landscape mapping has some implications that cannot be ignored. The biggest challenge is data quality and data integration, that is, data that is not complete or inconsistent can be significantly problematic in graph analysis. This can be corrected by the use of updated data collection and data cleansing tool that will guarantee real-time results (Miller, 2018).

Another important challenge is the scalability, which becomes increasingly difficult to achieve where the organization has a large network. This is because it becomes cumbersome to work with when we encounter a large number of vertices and a large number of edges. A combination of enhanced graph algorithmic solutions

and computing systems that rely on the cloud foundations may supplement this problem since it tends to process and visualize big data at a faster rate (Vinayakumar et al., 2018).

Moreover, the application of the graph-based mapping approach involves understanding in graph theory and related experiences in cyber security. Managers are required to devote their resources on training their employees or recruiting people who specialize in this field. Combining cyber security assessment with data science can also help in improving on how the graph-based solutions can be adopted.

Conclusion:

Use of graphs for threat modeling is one of the most important techniques in contemporary concepts of cyber security. In its core, it supports assessment of relationships between threats and vulnerabilities, as well as identification of assets in order to lessen risks effectively. Despite the mentioned obstacles, data quality, scalability, and expertise issues can be easily solved by taking advantage of the advancements in information technologies and launching special training sessions for experts. As technology advances, the traditional approaches to security, the graph-based mapping is a great way to enhance security.

References:

1. Amel, K. R. (2019, December). From shallow to deep interactions between knowledge representation, reasoning, and machine learning. In Proceedings 13th International Conference Scala Uncertainity Mgmt (SUM 2019), Compiegne, LNCS (pp. 16-18). https://sum2019.hds.utc.fr/wp-content/uploads/2019/12/sum_GT_ML_KR-18.pdf
2. Amini, P., Araghizadeh, M. A., & Azmi, R. (2015, September). A survey on botnets: classification, detection, and defense. In 2015 International Electronics Symposium (IES) (pp. 233-238). IEEE. https://ieeexplore.ieee.org/abstract/document/7380847/
3. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701. https://ieeexplore.ieee.org/abstract/document/8629941/
4. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cybersecurity management in industrial control systems. International Journal of Critical infrastructure protection, 9, 52-80. https://www.sciencedirect.com/science/article/pii/S1874548215000207
5. Miller, M. G. (2018). Are we protected yet? developing a machine learning detection system to combat zero-day malware attacks (Master's thesis, Utica College). https://ieeexplore.ieee.org/abstract/document/7112641/
6. Rawat, D. B., Doku, R., & Garuba, M. (2019). Cyber security in big data era: From securing big data to data-driven security. IEEE Transactions on Services Computing, 14(6), 2055-2072. https://ieeexplore.ieee.org/abstract/document/8673585/
7. Vinayakumar, R., Poornachandran, P., & Soman, K. P. (2018). Scalable framework for cyber threat situational awareness based on domain name systems data analysis. Big data in engineering applications, 113-142. https://link.springer.com/chapter/10.1007/978-981-10-8476-8_6
8. Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. ACM Computing Surveys (CSUR), 50(3), 1-40. https://dl.acm.org/doi/abs/10.1145/3073559