Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(6):101-107

Research Article ISSN: 2394 - 658X

Auto-Isolation: Enhancing Cybersecurity Resilience through Automated Network Segmentation in Response to Security Alerts

Sri kanth Mandru, Anvesh Gunuganti

*Mandrusrikanth9@gmail.com | Maverickanvesh@gmail.com

ABSTRACT

This research focuses on auto-solation, which is an advanced cybersecurity approach that autonomously isolates networks in response to security alerts. This is how a new approach helps to address the escalating threat of cyber-attacks with the use of artificial intelligence and software-defined networking (SDN); auto-isolation can rearrange networks on the fly to limit assaults. This answer consists of an innovative algorithm for producing decisions, operational scalability, robust security and safety measures, constant evolution, and enhanced interfacing. Auto-isolation is an effective way of solving the problems associated with compatibility, accuracy, and scalability, as well as taking a pro-active approach to the dynamic digital threat model.

Key words: Auto-isolation, Cybersecurity Resilience, Automated Network Segmentation, Security Alerts, Threat Mitigation.

INTRODUCTION

The contemporary business environment exposes organizations to a vast array of cyber threats; thus, the security policies developed must be creative and dynamic. Security threats affect cyberspace, and in particular, organizational systems are becoming more diverse and sophisticated, hence making standard approaches, which incorporate static protection measures and post-incident reactive countermeasures, inadequate. In this regard, the following innovation concerning cybersecurity resilience deserves specific attention: auto-isolation – the process of division of networks done automatically following the receipt of security alerts. To reduce and lessen the impact of such attacks, auto-isolation parturitions segments in real-time when noticing any malicious activity.

To establish a flexible security environment for an organization, this automated method leverages new-age technologies such as Software Defined Networking (SDN), Machine Learning (ML), and Artificial Intelligence (AI). Auto-isolation enhances the network's tenacity and the attackers' lateral movement ability since it rearranges or redesigns the network topology based on identified threats. However, there are several challenges that one is likely to encounter when implementing this multiple-layered system [1]. These are things like developing reliable and contextually conscious decision-making algorithms as well as ensuring that the auto-isolation mechanisms are sound and can be easily expanded. These issues have to be solved to make use of auto-isolation in protecting digital assets from the constant stream of cyber threats.

PROBLEM STATEMENT

Cyber-attacks are shifting escalation faster and are no longer stupid and destructive as they pose a big concern to modern organizations. Traditional security measures involving human participation cannot counter these threats because they are fluent and are derived from all aspects of life. One may be auto-isolation, a function that allows the network environment to self-segment based on the alarm signals raised for security concerns. Several intricate matters need to be answered to properly execute the incremental strategy of increasing cyber defense toughness [2].

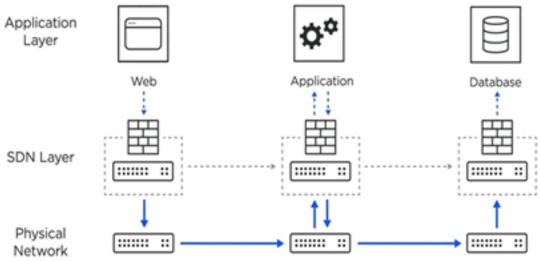

Figure 1: Automated Network Segmentation [2]

As for the compatibility and integration of the auto-isolation methods, there is a lot of expectation that these are appropriately placed in the network structures. Similar to the case with today's large corporations, many probably have components from both new and old technologies, and many modern corporate networks are also likely to be strongly heterogeneous. This can only occur if integration is well prepared and technical solutions are provided in advance to help avoid disrupting company activities through integration. Technical feasibility is another way of enhancing auto-isolation by improving reliability and accuracy. Non-essential networking segmentation might result from false positives, which will decrease the capability of working capacity and interfere with lawfulness in business dealings [3]. On the other hand, if false negatives are often present, the threats will spread through the network without an opportunity to be noticed. One significant difficulty is developing innovative, contextualized mechanisms that could distinguish between marginal peculiarities and tangible dangers.

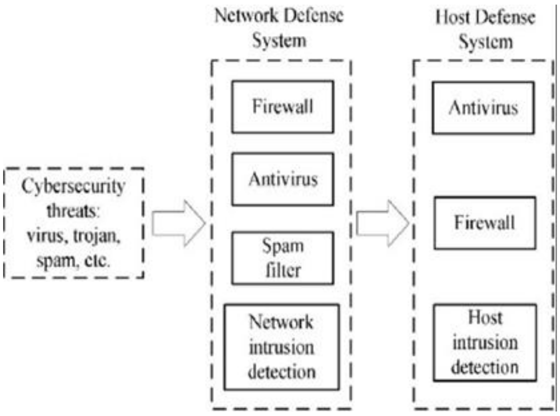

Figure 2: Traditional threat detection [3].

Also, auto-isolation solutions should be functional and scalable since risks are not static. This means that the auto-isolation techniques must be scalable, meaning they have to be capable of working in numerous and diverse scenarios as businesses evolve and broaden their reach. This scalability has to be achieved prudently, particularly given the constant volatility in the TTPs cyber attackers use in their operations. Auto-isolation systems must also be prepared to work under enhanced attack and failure conditions. These systems are open and can be threateningly attacked, resulting in dangerous compromise. To ensure that auto-isolation measures remain secure, it is essential to have appropriate security frameworks, backup measures, and fallback mechanisms.

SOLUTION

Discussing the difficulties of using auto-isolation to enhance resistance to cyber threats reveals that such an idea possesses certain conditions that a singular perspective cannot resolve. This system includes advanced integration processes, decision-making composite formulas, an adjustable system, and, above all, security [4].

Advanced Integration Strategies: Most of all, there has to be a possibility of integrating auto-isolation technologies to keep the networks invisible to the current topography. Due to the need to integrate older systems and new security measures, adaptive middleware technology is applied. This separation of the network may well be more accessible to manage dynamically using what was once called SDN or software-defined networking.

SDN makes it easier to control the network rules in reference to an optimal re-routing of the network paths when necessary while having minimal invasive impacts on the business processes that are disconnected for operational optimization. Nevertheless, API-based connectors may also assist in having a single posture of security because the integration of all the platforms is sure.

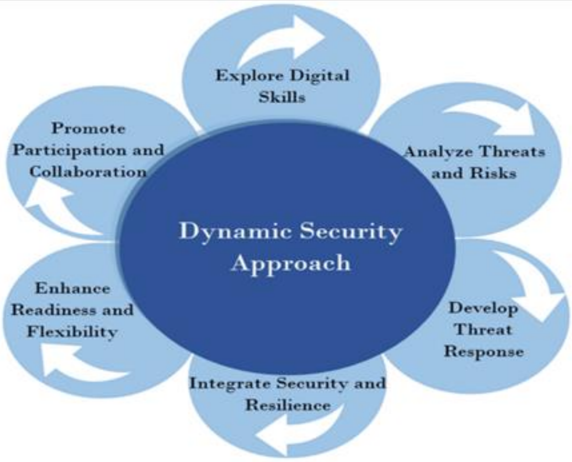
Explore Digital Skills
Promote Participation and Collaboration
Analyze Threats and Risks
Dynamic Security Approach
Enhance Readiness and Flexibility
Develop Threat Response
Integrate Security and Resilience

Figure 3: Rapid response to cybersecurity alerts [5].

Intelligent Decision-Making Algorithms: Auto-isolation requires the formation of intelligent and situational decision-making criteria. They must perform an excellent job of discerning between what is really a threat and what is just merely a distraction. Tools relevant to this area include Machine Learning (ML) and AI techniques. One is to teach it supervised and unsupervised learning models about petabytes worth of data to teach it what threats it should be looking out for. The integration of threat intelligence feeds enables the algorithms to collect new threats when they are occurring. Such approaches as ensemble learning methods can also be used to improve the detection rates and decrease the false alarm rates of the system while maintaining its efficiency. These methods involve the use of more than one ML model simultaneously.

Scalable Architecture: This means that one should have a solution that can be flexible enough to respond to changes in the business networks since the latter are dynamic. The use of microservices architecture enables the deployment of the auto-isolation components as individual units. The system can be made more scalable and updated to cater to the increasing network demands by addressing each microservice at a time [5]. As for other containerization solutions, such as Kubernetes and Docker, that could also be used to deploy and manage the mentioned microservices, more versatility and reliability could be obtained. It also integrates with CI/CD pipelines, which are helpful for the fast inclusion of security patches and other enhancements to the system.

Robust Security Measures: Self-protection and self-sustainability of the auto-isolation system have to be ensured. Incorporation of zero trust notion can be done in multi-layered security architectures. A series of penetration tests and security audits should be performed on all the parts of the systems.

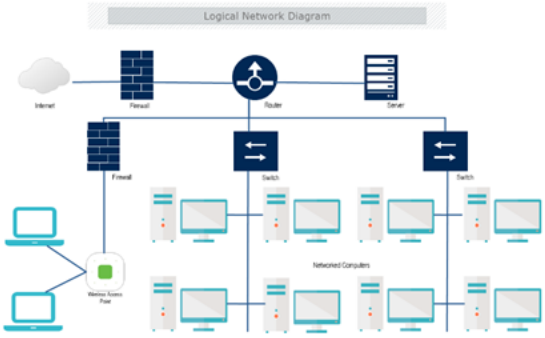

Figure 4: Network topology for automated network segmentation [5].

To ensure data assurance and privacy, robust access and permission checks should be implemented, and secure transmission between microservices should be employed. It is advisable to implement fail-over methods and redundant systems to ensure that activities will not be affected by system breakdowns or specific attacks.

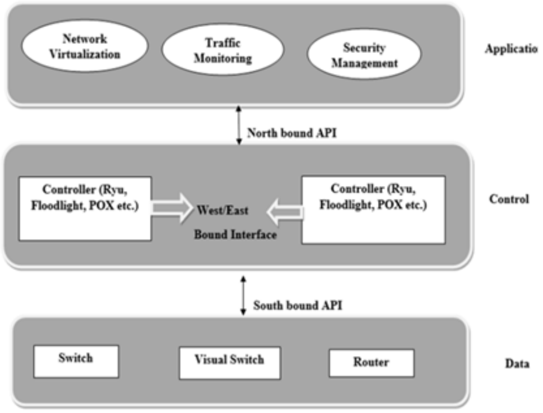

Figure 5:SDN-based Cyberthreat identification using Machine learning [5].

Continuous Monitoring and Adaptation: This means that for auto-isolation to be effective, one has to be very observant and learn with each new threat. The services are provided by a Security Operations Center (SOC) together with the help of advanced analytical and visualization tools, which enable real-time monitoring of network activities. Algorithms can continually be optimized, and as can be seen, it is possible to create automated feedback mechanisms such that the system is trained on an isolated incident basis [6]. While focusing on specific stand-alone instances as a way of enhancing the systems, the threat-hunting teams may employ advanced forensic solutions.

Compliance and Governance: Therefore, in adopting auto-isolation methods, it will be more appropriate if special care is taken to ensure they meet all the existing legal requirements and guidelines. A possible governance framework may include the establishment of audits, regulatory control, and policies that may need a continuous review to ensure that the best practices and other laws set the system. Therefore, the process of threat identification and the ability to recognize possible security threats that may occur in the future is improved by using machine learning and artificial intelligence, as shown in Figure 5. Businesses can also adopt the zero-trust security model.

USES

Given their topicality and applicability to a broad spectrum of cybersecurity challenges, it is possible to state that auto-isolation has been helpful in various organizational settings due to the possibility of providing individual reactions to general threats. However, to get a clearer picture of how auto-isolation can be used in practice and whether it is effective in cyber risk reduction, a case of auto-isolation can be somewhat helpful [6]. An essential element of the banking industry concerned with protecting data also utilizes auto-isolation to help respond swiftly to security issues. The auto-isolation mechanism of the bank's network shut down all the infected systems as soon as it felt the network was under threat, thus preventing unauthorized access to critical financial documents. This has helped protect the client data and the reputation of the bank at large by reducing the impact of this incident.

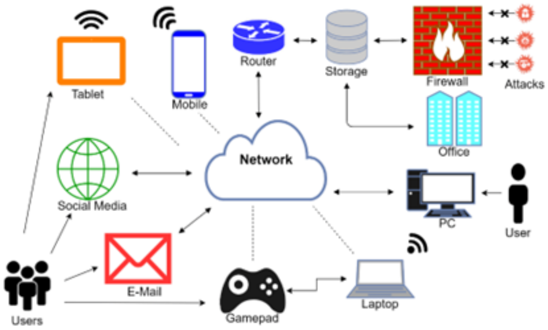

Figure 6: Applications of auto-isolation in detecting cyber attacks [7].

The healthcare sector also had an instance where auto-isolation occurred in mitigating patient data and healthcare apparatus on a hospital network from cyber threats. A good example is when the auto-isolation system detected a virus on a particular hospital's workstation; this acted fast to ensure that it did not spread to other critical healthcare systems [6]. As such, the hospital continues to maintain and enhance its patients' well-being by ensuring no hitches in patient care due to cyber threats. Moreover, self-containment has been very useful in combating ransomware, threatening many operations across industries.

Auto-isolation technology helps isolate infected endpoints in a manufacturing organization victim of a ransomware attack and prevent the virus from accessing production systems. With this containment method, ransomware spread in an organization was prevented from further spreading, and instances that caused downtime were eliminated.

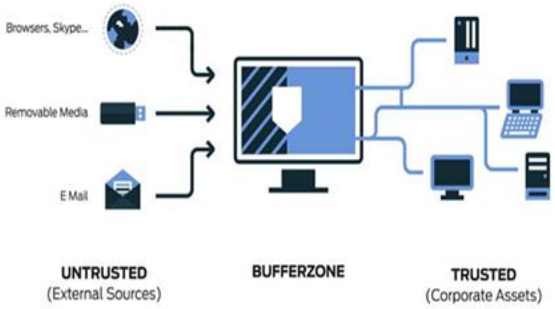

Figure 7: Auto-isolation of infected endpoints [7].

Based on these examples, one can realize how effectively auto-isolation limits the effects of cyber threats. Thus, decisions can be made to reduce the impact of security events on business processes and significantly reduce response times by automating actions based on threat information in near real-time [7]. Today, organizations must employ auto-isolation solutions to boost their capability of fending off cyber threats and safeguarding their assets.

IMPACT

Auto isolation mainly influences cybersecurity resilience in two ways: by reducing the time taken to respond to an incident and by reducing the number of threats that relate to cybersecurity. Auto-isolation is an example of technology that may contribute to increasing the speed of shutting down possible breaches. This feature quarantines the computers infected by malware from the network in case of security threats that might cause instability in the network. These cyber incidents affect business continuity and can significantly harm an organization's reputation; if countermeasures are taken quickly, the adverse outcomes and the virus spread can be considerably mitigated. Auto-isolation also provides substantially more operating ease and expense savings when positioned in synergy with human interaction arrangements [8]. This hampers the immediate identification and isolation of security threats resulting from the involvement of people in handling security incidents using traditional methods.

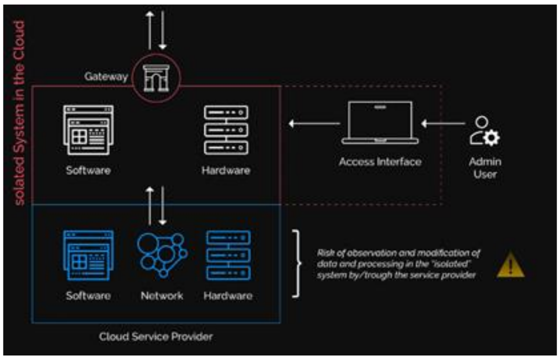
solated System in the Cloud
Gateway
Software
Hardware
Access Interface
Admin User
Software
Network
Hardware
Risk of observation and modification of data and processing in the "isolated" system by/trough the service provider
Cloud Service Provider

Figure 8: Benefits of auto-isolation [8].

These three come hand in hand with possible loss of business reputation, having to spend more money on recovering from the lost time, and even more time on downtime. In contrast, auto-isolation works the reaction steps based on predetermined security rules and threat information in advance, making an organization's incident response operations more effective. This minimizes the time occupancy of cybersecurity staff because the repetitive straightforward tasks that take much time have been automated; therefore, there is a low tendency of the staff to make mistakes when working on complex processes such as threat hunting and vulnerability analysis [8].

Besides, auto isolation excludes instances of data loss and system reimaging, which are avoidable, reactive, costly, and time-consuming. Auto-isolation may assist organizations suffering expensive disruptions and limit the impact category to the network level at which risks can be isolated from a business services perspective. Auto isolation could be helpful for organizations in terms of raising their 'collective immunity' against cyber threats, rapidly identifying novel threats and risks, and reducing tendencies towards vulnerability to cyber threats and cyber-attacks [8]. In connection with auto-isolation, the use of automation and relevant real-time data allows the protection of digital assets to be advanced to a new level and meet new generations of threats. Cybersecurity is a significant problem for most businesses worldwide, so auto-isolation tools have become critical in protecting against the latest threats while preserving the correct business operations.

SCOPE

Auto-isolation might be capable of addressing the need for different levels of cybersecurity Threats across the various entities at different scales, which may be configured in other ways. The solutions based on the concepts of automatic isolation can be easily adjusted to correspond to the requirements of every particular organizational structure and its characteristics, whether it is a home business, a vast global corporation, or a set of interconnected industrial networks [9]. For instance, SDN makes dynamic programming of the existing network about the various organizational structures or security statuses possible; this means that a network could be subdivided into as many parts as needed. However, some shortcomings and constraints have badly hampered the extent of auto-isolation, although this method has a lot of advantages [10]. The only disadvantage that can be pointed out is the potential requirement of being incorporated into modern cybersecurity's existing systems and technologies. Significant costs could be incurred for the advancement of technologies and the challenges associated with integrating auto-isolation systems into network interfaces with other old-fashioned systems.

Indeed, cultural factors and resistance to change within an organization may cause auto-isolation measures to fail to work as intended. Out of concerns about letting go of oversight or authority over company affairs, some organizations may not be willing to relinquish control over their networks' segmentation and handling of incidents when opting for SASE [11]. Furthermore, auto-isolation is effective only if combined with such threat detection methods that are accurate and, if possible, real-time. There is always the risk that the increase in productivity may be offset if false positives or notifications that come at the wrong time interrupt employees from their work. For auto-isolation measures to be effective, the operational threat detection systems must be trustworthy.

Looking at the future, there is potential to develop interesting new directions in auto-isolation research shortly. The enhancements of machine learning and the AI algorithm may help distinguish threats more effectively and react more predictively and effectively. The fine-tuning of existing auto-isolation techniques can be fine-tuned more effectively by studying new network segmentation and isolation methods like micro-segmentation and application-aware isolation. Further initiatives should also focus on developing reference models and good practice guidelines for auto-isolation solutions [12]. This would also assist with this issue and ease auto-isolation rollout for organizations of all sizes. By solving these problems and adapting to emerging technologies, organizations may improve their cybersecurity defenses and effectively mitigate progressing threats, thus expanding the width of auto-isolation.

CONCLUSION

Auto-isolation is one of the most vital processes of increasing organizational cybersecurity defense in anticipation of threats. It strengthens security by responding swiftly to security notices and automatically creating sub-networks to reduce the effects of such a breach. This report has revealed this by elaborating on such aspects as the shortcomings of auto-isolation conventional approaches and identifying potential directions for further research. Because threats in the cybersecurity realm are dynamic, organizations must always be ready to perform tasks like auto-isolating assets and solving new ones.

REFERENCES

[1]. K. Mishima, T. Sakurada, Y. Hagiwara, and T. Tsujisawa, “Secure Campus Network System with Automatic Isolation of High Security Risk Device,” Sep. 2018, doi: 10.1145/3235715.3235738. Available: https://doi.org/10.1145/3235715.3235738

[2]. Z. Hong, Q. Shao, X. Liao, and R. Beyah, “A secure routing protocol with regional partitioned clustering and Beta trust management in smart home,” *Wireless Networks*, vol. 25, no. 7, pp. 3805–3823, Dec. 2018, doi: 10.1007/s11276-018-01916-1. Available: https://doi.org/10.1007/s11276-018-01916-1

[3]. T. Kowalewski, “Value of work in relation to cyber threats in the development of new competencies of social workers in the local environment,” vol. 3, no. 3, pp. 91–96, Dec. 2017, Available: https://pjas.pwsip.edu.pl/index.php/pjas/article/download/81/66

[4]. G. Lykou, A. Anagnostopoulou, and D. Gritzalis, “Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls,” *Sensors*, vol. 19, no. 1, p. 19, Dec. 2018, doi: 10.3390/s19010019. Available: https://doi.org/10.3390/s19010019

[5]. F. Siddiqui, M. Hagan, and S. Sezer, “Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure,” Sep. 2019, doi: 10.1109/socc46988.2019.1570548325. Available: https://doi.org/10.1109/socc46988.2019.1570548325

[6]. C. Zhou, B. Hu, Y. Shi, Y.-C. Tian, X. Li, and Y. Zhao, “A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems,” *Proceedings of the IEEE*, vol. 109, no. 4, pp. 517–541, Apr. 2021, doi: 10.1109/jproc.2020.3034595. Available: https://doi.org/10.1109/jproc.2020.3034595

[7]. C. B. Jones, C. Carter, and Z. Thomas, “Intrusion Detection & Response using an Unsupervised Artificial Neural Network on a Single Board Computer for Building Control Resilience,” Aug. 2018, doi: 10.1109/rweek.2018.8473533. Available: https://doi.org/10.1109/rweek.2018.8473533

[8]. A. Boddy, W. Hurst, M. Mackay, and A. E. Rhalibi, “A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures,” Oct. 2017, doi: 10.1145/3109761.3109793. Available: https://doi.org/10.1145/3109761.3109793

[9]. I. Linkov and A. Kott, “Fundamental Concepts of Cyber Resilience: Introduction and Overview,” in Springer eBooks, 2018, pp. 1–25. doi: 10.1007/978-3-319-77492-3_1. Available: https://doi.org/10.1007/978-3-319-77492-3_1

[10]. S. Nazir, S. Patel, and D. Patel, “Assessing and augmenting SCADA cyber security: A survey of techniques,” Computers & Security, vol. 70, pp. 436–454, 2017, doi: 10.1016/j.cose.2017.06.010. Available: https://doi.org/10.1016/j.cose.2017.06.010

[11]. N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, 2017, doi: 10.1016/j.telpol.2017.09.003. Available: https://doi.org/10.1016/j.telpol.2017.09.003

[12]. M. M. Hassan, S. Huda, S. Sharmeen, J. Abawajy, and G. Fortino, “An Adaptive Trust Boundary Protection for IIoT Networks Using Deep-Learning Feature-Extraction-Based Semisupervised Model,” IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2860–2870, Apr. 2021, doi: 10.1109/tii.2020.3015026. Available: https://doi.org/10.1109/tii.2020.3015026