Intrusion Detection and SoC applied to IoT

Mohammed Islem NADJI
LIFO
INSA CVL
Bourges, France
mohammed_islem.nadji@insa-cvl.fr

Soumaya BEL HADJ YOUSSEF
LIFO
INSA CVL
Bourges, France
youssef.soumaya@gmail.com

Pascal BERTHOME
LIFO
INSA CVL
Bourges, France
pascal.berthome@insa-cvl.fr

Jeremy BRIFFAUT
LIFO
INSA CVL
Bourges, France
jeremy.briffaut@insa-cvl.fr

***Abstract*—The rapid expansion of the Internet of Things (IoT) has introduced significant security challenges that traditional Security Operations Centers (SOCs) are not fully equipped to handle. This research aims to develop a comprehensive architecture that addresses currently identified but untreated specificities in IoT environments. The primary focus is on defining a generic and scalable model for retrieving and processing data, considering the heterogeneous nature and constraints of IoT systems, as this is foundational for building a SOC capable of managing the complexities of a heterogenous IoT environment. This model will take into account for protocol diversity, data variety and representations, low energy requirements, connected/ disconnected modes, the potential for physical reactions, and the need for both active and passive monitoring. Subsequently, the research will explore storage and visualization models tailored to these heterogeneous environments. One innovative approach involves coupling Blockchain technology, which offers decentralization and data integrity and non-repudiation, with a time-series database for efficient querying and ease of visualization. Additionally, the research will focus on implementing automatic and generic penetration tests specifically designed for heterogeneous IoT systems. These tests will identify potential vulnerabilities, enable preventive security measures, and test the robustness of the proposed architecture. In summary, this research will address critical security aspects in IoT environments by enhancing monitoring, data analysis, and threat responsiveness, and by incorporating penetration tests to bolster system resilience.**

***Index Terms*—Internet of Things , Intrusion Detection , Data Analysis , System and Network Security ,Security Testing**

I. Introduction

The internet of things has become an emerging technology in various sectors: healthcare, smart cities, agriculture, and industry 4.0 by connecting numerous devices, enabling data collection and automation. Statistics show that by 2030, the IoT devices will reach 40 billion which means that we have a real challenge to ensure security . However, this widespread connectivity has introduced a multitude of challenges and security risks due to inherent vulnerabilities and security issues of IoT devices that can be exploited by attackers, which leads to several consequences: loss of confidentiality, protocols and application integrity attacks, DDOS attacks and much more.Also , the constructors don't make security updates to fix the issues. The need for a comprehensive security monitoring tool is critical to address the gaps in IoT security . A Security Operation Center (SOC) play a pivotal role in safeguarding the security by threat detection, and swift incident response capabilities.However, the integration of SOC into a heterogeneous IoT environment brings a lot of challenges.Like the complexity of handling diverse communication protocols in different layers especially the network layer.And the huge amount of data generated by devices .

II. Literature Review

.

According to Bennouri et al [1], the importance of Security Operations Centers (SOC) in IoT environments cannot be overstated.Because they play a pivotal role in monitoring, detecting, and responding to security threats.As IoT devices proliferate, they bring unique security challenges that traditional SOCs are not fully equipped to handle. Then, they discuss the challenges include the diverse protocols used by different devices, their limited computational resources, and their widespread and often unsecured deployment across various networks. Current SOC practices, while effective in traditional IT environments, often fall short in the IoT context due to these complexities. Existing SOC practices struggle with the heterogeneity and volume of IoT data. Making it difficult to maintain robust security measures. To address these shortcomings, there is a pressing need for tailored SOC solutions that can adapt to the specific demands of IoT ecosystems. Recommendations for improving SOC capabilities in IoT environments include the development of enhanced real-time monitoring systems that can handle the high variability of IoT devices, advanced anomaly detection algorithms to identify unusual behavior across diverse devices, and automated response mechanisms to swiftly mitigate threats. By adopting these enhancements, SOCs can significantly improve their ability to safeguard

IoT networks against an evolving landscape of security threats.

In [2] Ashok Chopra discuss: the technological evolution driven by the Internet of Things (IoT) has significantly transformed various industries, marking a shift from traditional Information Technology (IT) environments to IoT-driven ecosystems. This transformation brings a host of security challenges, primarily due to the lack of standardized security practices and the vastly increased attack surface introduced by the myriad of connected devices. IoT's integration into industrial operations also underscores the stark differences between IT and Operational Technology (OT) security. While IT security focuses on data protection and network security, OT security involves securing physical processes and legacy systems that were not originally designed for internet connectivity. This integration poses complexities, as legacy OT systems must be retrofitted with modern IoT devices, creating potential vulnerabilities. From the IT domain, several lessons learned can be applied to bolster IoT security. These include the implementation of comprehensive security frameworks that encompass all layers of IoT architecture, as well as proactive threat management strategies to anticipate and mitigate potential risks. By leveraging these insights, industries can better navigate the security landscape of IoT, ensuring a more robust and resilient infrastructure against emerging threats.

David and Anura [3] show that Security Operations Centers (SOCs) play a critical role in modern network infrastructures, especially with the integration of IoT devices, by providing timely security alerts and taking necessary defensive actions. For SOCs to effectively manage the security landscape of IoT environments, enhanced visibility and monitoring are paramount. This includes having real-time monitoring capabilities and maintaining accurate asset inventories to ensure comprehensive awareness of all IoT devices within the network. However, SOCs face significant challenges due to the protocol diversity inherent in IoT ecosystems. IoT devices communicate using a wide array of protocols, many of which are unfamiliar or incompatible with traditional SOC tools. This diversity requires that SOCs develop the ability to interpret and respond effectively to various communication protocols, ensuring seamless security management across all devices. To address these challenges, a proposed framework for improving SOC capabilities in IoT environments emphasizes the importance of security orchestration and automation. This framework advocates for robust monitoring solutions that can dynamically adapt to the heterogeneous and scalable nature of IoT networks, ensuring that SOCs can provide effective, real-time security responses and maintain the integrity of evolving digital infrastructures.

A. Summary

In summary, according to the papers reviewed in this literature review, several significant drawbacks and gaps have been identified in the current approaches to IoT security and the role of Security Operations Centers (SOCs). Common drawbacks include:

- The lack of standardized protocols for managing heterogeneous IoT environments due to wide variety of IoT protocols (e.g., RF, Z-Wave, Zigbee, Matter, Thread) .
- The difficulty in achieving real-time monitoring and maintaining accurate asset inventories, and scalability issues in processing diverse data formats .
- The vast number of IoT devices and the extensive data they generate .
- The integration of IT and OT security,ighlighting the need for a unified approach that combines the best practices from both domains .

III. Attack Example

The Mirai botnet is one of the most notorious examples of how unsecured Internet of Things (IoT) devices can be exploited on a massive scale. In 2016, Mirai infected thousands of IoT devices—such as IP cameras, DVRs, and home routers—by scanning the internet for devices using default or weak login credentials (like "admin/admin" or "root/1234"). Once a device was compromised, it became part of a larger "botnet" army, silently controlled by the attacker. These enslaved devices were then directed to flood targeted servers with overwhelming amounts of traffic, a tactic known as a Distributed Denial of Service (DDoS) attack. Major platforms like GitHub, Twitter, Netflix, and Reddit were temporarily taken offline due to Mirai's power.

What made Mirai so dangerous wasn't just the scale, but the stealthy and automated nature of its infection. Users were unaware their devices were weaponized. This highlights a crucial need: real-time supervision tools like a SOC for IoT environments. These tools can monitor traffic, detect abnormal behavior, identify unauthorized access, and alert administrators before a device is weaponized. In an era where billions of devices are connected, vigilance is not optional—it's essential.

IV. Required Solutions

Research gaps identified in the literature include the necessity for a generic and scalable model for data retrieval and processing, enhanced frameworks for integrating various IoT protocols into SOC operations, and improved methods for real-time monitoring and threat response. Addressing these gaps is essential for developing robust and effective SOC capabilities tailored to the unique demands of IoT environments.

The research objectives are : definining a generic and scalable model for retrieving and processing, storage and visualization models for retreived data , and implementating of automatic and generic penetration tests.

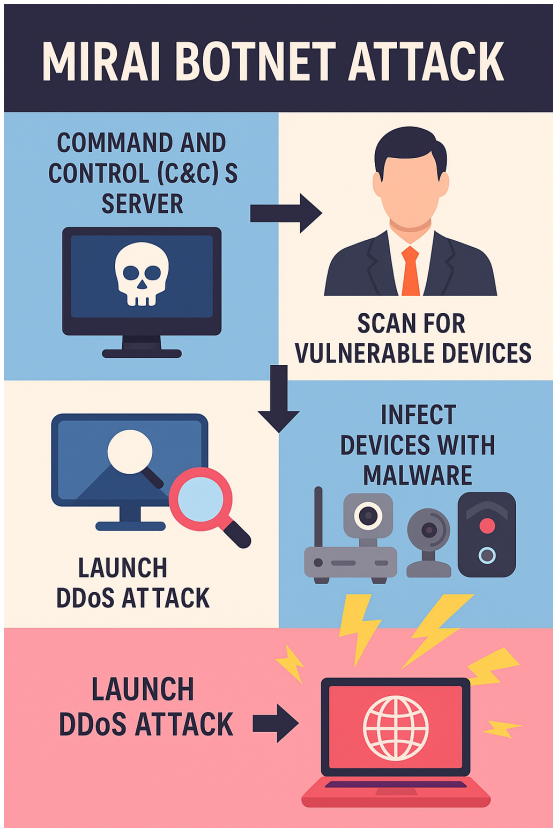

Fig. 1. Mirai botnet attack

A. Developing a Generic and Scalable Model

The primary focus is to create a generic and scalable model that can efficiently handle diverse data types and protocols, incorporate real-time data processing and analysis capabilities to enhance threat detection and response, and provide an adaptable system that can interpret and standardize data from multiple sources. This involves several key components and steps. To achieve this, the process begins with understanding data sources and protocols by identifying and categorizing all potential data sources and communication protocols used in the IoT environment. This involves creating a comprehensive inventory of IoT devices, detailing their types, manufacturers, and communication protocols (e.g., RF, Z-Wave, Zigbee, Matter, Thread), and analyzing each protocol's specifics, such as data formats, communication patterns, and security features.
The next step is data standardization, which aims to develop a method to standardize data from diverse IoT protocols into a common format. This involves designing a flexible data schema that accommodates various data types and structures from different IoT protocols and ensures the schema supports necessary metadata (e.g., device ID, timestamp, data type). The normalization process includes creating procedures to transform raw data from different protocols into the standardized schema and implementing protocol-specific parsers and converters to handle the normalization.
To handle data collection efficiently, a robust and scalable framework must be implemented. This involves deploying lightweight data collectors on edge devices or gateways to gather data from nearby IoT devices, ensuring these collectors can manage intermittent connectivity and cache data when the central system is unavailable. Additionally, central data aggregation points should be established to receive data from edge collectors, using message brokers like MQTT or Apache Kafka to manage data streams and ensure reliable data transmission. Finally, developing capabilities for real-time data processing and analysis is crucial for immediate threat detection and response. This involves implementing stream processing platforms (e.g., Apache Flink, Apache Storm) to analyze incoming data streams in real time and designing processing pipelines for filtering, aggregating, and enriching data. Event detection mechanisms, such as rules and algorithms for identifying security events and anomalies within the data streams, should be defined, and machine learning models can be employed to enhance detection accuracy. This comprehensive approach ensures the model is robust, scalable, and effective in managing the complexities of a heterogeneous IoT environment.

B. Storage and Visualization

Developing effective storage and visualization models for data retrieved and processed in a heterogeneous IoT environment is crucial for managing and analyzing the vast amounts of data generated by these devices. One promising approach involves coupling blockchain technology with a time-series database. Blockchain provides decentralization and data integrity, ensuring secure and tamper-proof storage, while time-series databases (e.g., InfluxDB, TimescaleDB) facilitate efficient querying and ease of defining visualization models.
To establish scalable storage solutions, a hybrid storage architecture can be implemented. This architecture combines the strengths of time-series databases for quick data retrieval and blockchain for immutable, secure storage. Additionally, relational or NoSQL databases can be used to store and query metadata, further enhancing the system's flexibility and robustness.
Data retention and archiving are also critical components. Defining clear data retention policies will help manage the life cycle of stored data, ensuring that data is archived appropriately for long-term storage and historical analysis.
For data visualization and analysis, developing interactive dashboards using tools like Grafana or Kibana is essential. These dashboards should be customizable, allowing different stakeholders to view real-time and historical data relevant to their needs. Furthermore, reporting and analytics tools should be developed to generate periodic security reports and summaries, as well as support advanced analytics for deep dives into data for forensic analysis and insights. This comprehensive approach ensures that IoT data is not only securely stored but also readily accessible and analyzable, providing valuable insights for enhancing IoT security and performance.

C. Scalability , Flexibility

To ensure the scalability and flexibility of the model, it is essential to design a system that can adapt to the increasing number of IoT devices and evolving protocols. This begins with a modular architecture, allowing for the seamless addition of new data collectors, processing modules, and storage components. Each module should operate independently while communicating through well-defined interfaces, enabling easy upgrades and integrations without disrupting the entire system

Integrating cloud and edge computing solutions is another critical step. Cloud platforms provide scalable data processing and storage capabilities, accommodating the vast amounts of data generated by IoT devices. Meanwhile, edge computing solutions can handle data processing closer to the source, reducing latency and bandwidth usage by performing preliminary data filtering and analysis locally.

D. Security and Privacy Considerations

Security and privacy considerations are paramount to protect the integrity, confidentiality, and availability of data throughout the system. Implementing robust data encryption for both data in transit and at rest is crucial to safeguard against unauthorized access. Secure protocols, such as TLS, should be used for data transmission between devices, collectors, and central systems.

Access control policies must be defined and enforced to restrict data access based on user roles and responsibilities. This involves implementing robust authentication and authorization mechanisms for all system components, ensuring that only authorized personnel can access sensitive data.

Additionally, maintaining comprehensive logs of all data collection, processing, and access activities is essential. These logs are invaluable for auditing, troubleshooting, and forensic analysis, providing a detailed record of system operations and aiding in the detection and investigation of security incidents. By addressing these scalability, flexibility, and security considerations, the model can effectively support a growing and evolving IoT environment while ensuring data integrity and privacy.

V. Implementation of Automatic and Generic Penetration Tests

Implementing automatic and generic penetration tests for heterogeneous IoT environments requires a systematic approach encompassing various crucial steps. The process begins with device identification and categorization, where a comprehensive inventory of all IoT devices is developed, capturing essential metadata such as device type, manufacturer, firmware version, communication protocol, and network topology. Devices are then categorized based on their function, communication protocol, and criticality to the overall system. Following this, tailored test scripts are developed, covering both protocol-specific and device-specific tests to identify common vulnerabilities such as weak authentication, unencrypted communication, and default credentials. Automation plays a pivotal role, with the selection or development of tools supporting scripting and capable of handling diverse IoT protocols. Integration into the continuous integration (CI) pipeline ensures regular and automated testing, facilitating early vulnerability identification and continuous security monitoring. Centralized logging and alerting mechanisms enable efficient analysis and immediate response to critical vulnerabilities detected during tests. Moreover, dashboards and reporting tools provide visual insights into test results and aid in tracking remediation efforts and compliance. Subsequently, mitigation and response strategies are devised based on test findings, including the development and implementation of remediation plans, retesting to validate effectiveness, and continuous improvement to enhance the overall security posture. This systematic approach ensures robust security measures in heterogeneous IoT environments, safeguarding against potential threats and vulnerabilities.

VI. Conclusion

This research aims to address the critical security challenges posed by the rapid expansion of IoT by enhancing SOC functionality through defining one architecture that contains : developing a generic and scalable data retrieval and processing model , exploring innovative storage and visualization solutions, this research will contribute to more robust and effective security monitoring in heterogeneous IoT environments.Furthermore, implementing automatic and generic penetration tests specifically tailored to the unique characteristics of heterogeneous IoT environments is essential. These tests play a vital role in identifying potential vulnerabilities within the IoT system, enabling proactive measures to enhance security. Additionally, they serve as a means to test and challenge the defined architecture, ensuring its resilience and effectiveness in safeguarding IoT environments against emerging threats. Through these combined efforts, organizations can strengthen their security posture and optimize data management practices in the dynamic landscape of IoT technologies.

Acknowledgment

We would like to take a moment to sincerely thank INSA CVL and the Centre-Val de Loire region for their generous financial support for my thesis journey. Their funding is absolutely essential in helping me carry out my research and push the boundaries of knowledge in my field.

References

[1] Hajar Bennouri, Abdiaziz Abdi, Iqbal Hossain, Alexandre Pujo, “The Role of SOC in Ensuring the Security of IoT Devices: A Review of Current Challenges and Future Directions.” MECO 2023: 1-8.

[2] Ashok Chopra, Paradigm Shift and Challenges in IoT Security,Journal of Physics: Conference Series, Volume 1432, First International Conference on Emerging Electrical Energy, Electronics and Computing Technologies 2019 30–31 October 2019, Melaka, Malaysia.

[3] David Weissman, Anura Jayasumana, “Integrating IoT Monitoring for Security Operation Center,” 2020 Global Internet of Things Summit (GioTS), IEEE, 17 June 2020, Dublin, Ireland .