International Journal of Computer Engineering and Technology (IJCET)
Volume 15, Issue 1, Jan-Feb 2024, pp. 1-6, Article ID: IJCET_15_01_001
Available online at https://iaeme.com/Home/issue/IJCET?Volume=15&Issue=1
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

CYBERSECURITY EVOLUTION MODEL: AI/ML IN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE

Vinay Dutt Jangampet
Staff App Ops Engineer, Intuit, United States

ABSTRACT

The development of Security Orchestration, Automation, and Response (SOAR) systems is the main topic of this paper's investigation into the history of cybersecurity. In contemporary cybersecurity, SOAR—which consists of orchestration, automation, and response capabilities—is essential. The shift from conventional network operations centers to advanced security operations centers is depicted in the cybersecurity evolution model.

The SOAR platform's architecture-centric design emphasizes the value of integration and adaptability. Organizations use functional requirements as a reference when evaluating their security needs. These requirements include integration capabilities, automation, orchestration, incident response, threat intelligence, scalability, and usability.

Artificial Intelligence (AI) and Machine Learning (ML) combined with SOAR improves response efficacy, streamlines processes, and improves detection. Organizations must manage issues such data quality, algorithm selection, system complexity, and privacy concerns while benefiting from enhanced efficiency and scalability.

Keywords: SOAR, AI, ML

Cite this Article: Vinay Dutt Jangampet, Cybersecurity Evolution Model: AI/ML in Security Orchestration, Automation, and Response, International Journal of Computer Engineering and Technology (IJCET), 15(1), 2024, 1-6.
https://iaeme.com/Home/issue/IJCET?Volume=15&Issue=1

I. INTRODUCTION

The emergence of the digital age has presented numerous opportunities as well as a number of difficulties. One such difficulty is safeguarding information systems from possible attacks, a worry that gave rise to the cybersecurity industry. Cybersecurity has changed dramatically over the years, moving from simple antivirus programs to complex systems that can defend against a wide variety of attacks [5]

The rise of Security Orchestration, Automation, and Response (SOAR) solutions is a noteworthy milestone in this process. Organizations can improve their security operations with the help of the SOAR suite of capabilities. It gives organizations the ability to compile threat information from several sources, evaluate that information to identify dangers, and then effectively and efficiently address those threats.

In today's cybersecurity environment, SOAR plays a critical role. It makes it easier to respond to threats quickly, which reduces the possible damage that security breaches can inflict. The notion of SOAR, its different forms, and the incorporation of AI and ML in SOAR solutions will all be thoroughly examined in this paper.

A. Model of Cybersecurity Evolution

The evolution of cybersecurity measures over time is described by the cybersecurity evolution model [1]. Since physical presence was necessary for computer contact, cybersecurity was once not a big worry. But as network connectivity and the internet increased, cybersecurity became its own discipline. The paradigm emphasizes the transition from the conventional network operations center (NOC) to the security operations center (SOC), as well as the advent of intrusion prevention systems, firewalls with dynamic packet filtering, antispam software, vulnerability management, and vulnerability management [1]

B. SOAR and Its Types

Three essential components of contemporary cybersecurity systems are encapsulated in the term Security Orchestration, Automation, and Response, or SOAR.

- Security orchestration is the process of combining several security apps and systems to optimize security procedures.
- Automation is the process of doing security tasks that would normally need human intervention using automated tools and methodologies. Response times can be greatly accelerated by doing this, freeing up resources for other projects.
- In order to lessen possible dangers, response entails implementing the necessary measures based on the analysis of security occurrences.

There are various kinds of SOAR systems on the market, and each has a unique set of features and functionalities. Certain solutions concentrate more on orchestration and offer strong capabilities for combining different security systems. Others might place more of an emphasis on automation and provide cutting-edge tools to automate routine security activities. Comprehensive SOAR solutions are also available, offering a well-balanced combination of response, automation, and orchestration capabilities.

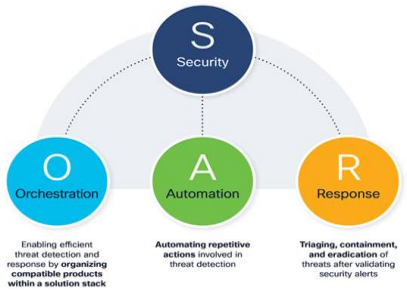

Figure 1. Figure 1. SOAR [7]

All SOAR solutions aim to increase the efficacy and efficiency of security operations, regardless of their specific design. These solutions can further improve their capabilities by integrating AI/ML technology, which will be covered in the sections that follow in this paper.

II. ARCHITECTURE CENTRIC APPROACH TO SOAR

When creating and deploying a Security Orchestration, Automation, and Response (SOAR) platform, an architecture-centric approach is essential. This strategy focuses on the SOAR platform's architectural architecture to make sure it can successfully integrate different security technologies.

The foundation of the architecture-centric approach is the idea that a system's usefulness and performance are greatly influenced by its architecture. By concentrating on the architecture, a SOAR platform may be created that can easily interface with a variety of security solutions, increasing the platform's functionality and efficacy.

This method makes it possible to develop a scalable and adaptable SOAR platform. It makes it possible for the platform to adjust to modifications in the security environment, including the arrival of fresh threats or the creation of new security instruments. Additionally, by using an architecture-centric approach, the SOAR platform's capabilities can be improved through the easier integration of AI/ML technologies.

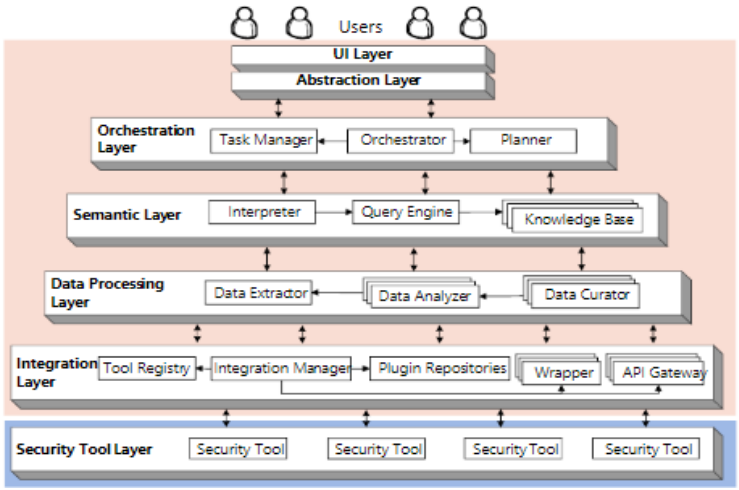

Figure 2. Architecture for SOAR platform

In conclusion, designing and implementing a SOAR platform requires an architecture-centric approach. It makes it possible for the platform to successfully integrate different security solutions, adjust to changes in the security environment, and improve its capabilities by integrating AI/ML technologies.

III. FUNCTIONAL REQUIREMENTS OF SOAR

Depending on the unique demands of a company, a Security Orchestration, Automation, and Response (SOAR) platform may have different functional requirements. But there are a few essential specifications that apply to all SOAR systems in general:

1. **Integration Capabilities:** An extensive array of security technologies should be able to be integrated with a SOAR platform. This covers, among other things, endpoint protection systems, firewalls, intrusion detection systems, and threat intelligence platforms**.**
2. **Automation:** Regular security tasks should be able to be automated by the platform. By doing this, security teams' workloads may be lighter and they will have more time to concentrate on more difficult jobs

3. **Orchestration:** The platform ought to have the capacity to synchronize the functions of several security instruments. This can enhance the security operations center's overall effectiveness and streamline security procedures**.**
4. **Incident Response:** Features for incident response ought to be included in the platform. This offers reporting, workflow management, and incident tracking capabilities.
5. **Threat Intelligence:** A variety of sources of threat intelligence should be gathered and analyzed by the platform. This may enhance the ability to identify and address security threats.
6. **Scalability:** As the business expands, the platform should be able to accommodate its security requirements.
7. **Usability:** The platform must to be simple to use and straightforward to navigate. Security teams may find that this shortens their learning curve and boosts productivity.

These are but a handful of a SOAR platform's functional specifications. Depending on the organization's size, type of company, and particular dangers it confronts, different standards may apply. Thus, before selecting a SOAR platform, it's critical for enterprises to perform a complete assessment of their security needs.

IV. AI/ML INTEGRATION IN SOAR SOLUTIONS

Security Orchestration, Automation, and Response (SOAR) systems are seeing a transformation in cybersecurity due to the introduction of Artificial Intelligence (AI) and Machine Learning (ML) [4,6]

There are various ways that AI/ML can be included into SOAR solutions. To find patterns and abnormalities that can point to a security concern, for example, ML algorithms can be used to examine massive volumes of security data. This can greatly enhance a SOAR platform's detection capabilities.

Conversely, complicated security procedures that would normally require human interaction can be automated with AI. AI, for instance, may automate the security alert triage process, identifying which alarms need to be addressed right once and which can be safely disregarded [3]. Security teams' workload may be lessened as a result, freeing them up to concentrate on more important duties.

Moreover, a SOAR platform's response capabilities can be improved by AI/ML. AI algorithms can be used to assess the best course of action in response to a particular security threat, taking into consideration variables including the threat's nature, the assets it poses a risk to, and its possible effects [6]

V. BENEFITS AND LIMITATIONS

The benefits of using AI/ML into SOAR solutions are numerous:

1. **Increased Efficiency:** Security teams can concentrate on more difficult problems by using AI and ML to automate repetitive operations. This has the potential to greatly increase security operations' efficiency **[8]**
2. **Improved Detection Capabilities:** Machine learning algorithms have the capacity to examine vast amounts of data in order to spot trends and abnormalities that could point to a security risk. This can improve a SOAR platform's detection capabilities.
3. **Better Decision Making:** AI can enhance decision-making processes by assisting in the identification of the best course of action in response to a particular security issue.
4. **Scalability:** AI/ML can assist SOAR solutions in scaling alongside an organization's security requirements.

But there are also possible limitations and difficulties:

1. **Data Quality:** The caliber of the training data that AI/ML uses in a SOAR platform determines how effective the technology is. Inaccurate outcomes can arise from data of poor quality [8]
2. **Algorithm Selection:** The AI/ML performance of a SOAR platform can be greatly impacted by the algorithm selected. The intended outcomes might not be obtained by an improper algorithm [9]
3. **Complexity:** Adding AI/ML to SOAR solutions might make them more complicated, which could be problematic for some businesses.
4. **Privacy Issues:** Using AI/ML requires processing a lot of data, which could lead to privacy issues.

VI. CONCLUSION

In summary, a major development in the field of cybersecurity is the incorporation of Artificial Intelligence (AI) and Machine Learning (ML) into Security Orchestration, Automation, and Response (SOAR) systems. The field of cybersecurity has advanced from simple antivirus protection to the advanced capabilities of SOAR, providing an all-inclusive suite of tools for enterprises to strengthen their security operations, thanks to the ongoing advancements in technology.

The consolidation of AI and ML further upgrades the capabilities of SOAR systems, offering benefits including scalability, improved discovery capabilities, better dynamic cycles, and expanded productivity. Notwithstanding, it is urgent to know about potential weaknesses such the reliance on excellent information, the meaning of picking a fitting calculation, the general intricacy of the system, and protection concerns.

To guarantee that incorporating AI/ML into SOAR systems meets their particular security objectives and concerns, associations should gauge the benefits and drawbacks of exploring the cybersecurity landscape. By carrying out a strategic plan and monitoring possible dangers, associations may effectively stand up to the consistently impacting universe of computerized threats and lift their cybersecurity tasks by utilizing the progressive force of AI and ML.

REFERENCES

[1] Codecademy. (2017). The Evolution of Cybersecurity. Codecademy; Codecademy. https://www.codecademy.com/article/evolution-of-cybersecurity

[2] Islam, C., Muhammad Ali Babar, & Surya Nepal. (2020, September 16). Architecture-centric Support for Integrating Security Tools in a Security Orchestration Platform. ResearchGate; unknown. https://www.researchgate.net/publication/344260727_Architecture-centric_Support_for_Integrating_Security_Tools_in_a_Security_Orchestration_Platform

[3] Jangampet, Vinay Dutt. “Automation Response to Cyber Threat.” https://ijrdst.org/, 2023. https://ijrdst.org/public/uploads/paper/856821701755768.pdf.

[4] Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. Intelligent Automation and Soft Computing, 28(2), 527–545. https://doi.org/10.32604/iasc.2021.016240

[5] The Evolution of Security Operations and Strategies for Building an Effective SOC. (2019). ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

[6] What is SOAR (security orchestration, automation and response)? | IBM. (2023). Ibm.com. https://www.ibm.com/topics/security-orchestration-automation-response

[7] Matzek, S., & Matzek, S. (2020, September 22). Why SOAR Is a Compelling Proposition for Your IT Security. Cisco Blogs. https://blogs.cisco.com/services/why-soar-is-the-future-of-your-it-security.

[8] Vinay Dutt Jangampet, Srinivas Reddy Pulyala and Avinash Gupta Desetty, Optimized Alternating Graph-Regularized Neural Network for Cyber Security Threats Detection in Internet of Things, International Journal of Information Security (IJIS), 2(1), 2023, pp. 1-12 doi: https://doi.org/10.17605/OSF.IO/45A32

[9] Reddy Pulyala, S., Gupta Desetty, A.., & Dutt Jangampet, V. (2019). The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 10(3), 1545–1549. Retrieved from https://www.turcomat.org/index.php/turkbilmat/article/view/14323

Citation: Vinay Dutt Jangampet, Cybersecurity Evolution Model: AI/ML in Security Orchestration, Automation, and Response, International Journal of Computer Engineering and Technology (IJCET), 15(1), 2024, 1-6.

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_1/IJCET_15_01_001.pdf

Abstract Link:
https://iaeme.com/Home/article_id/IJCET_15_01_001

✉ **editor@iaeme.com**