Toward Intelligent Cyber Defense: A Comprehensive Study of SOAR Technologies for AI-Based DDoS Detection

Article · August 2025

CITATIONS
0

READS
46

2 authors, including:

Rahma Alliouche
Université Constantine 2
6 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Toward Intelligent Cyber Defense: A Comprehensive Study of SOAR Technologies for AI-Based DDoS Detection

Rahma Alliouche[1,†], Hind Chenni[1]
[1]Abdelhamid mehri constantine2 university , Faculty of New Technologies,

---

Abstract

This research paper explores Security Orchestration, Automation, and Response (SOAR) technologies, examining their architecture, core components, and growing relevance in modern cybersecurity ecosystems. Particular emphasis is placed on the integration of artificial intelligence (AI) and machine learning techniques for Distributed Denial of Service (DDoS) detection and mitigation, highlighting how intelligent models can enhance SOAR workflows by enabling faster, more accurate threat identification. The study discusses the critical challenges of implementing AI-driven SOAR solutions, including the management of false positives, data imbalance and quality issues, interoperability with existing security tools, and regulatory compliance requirements. Existing SOAR platforms, such as Fortinet FortiSOAR, IBM QRadar SOAR, and Palo Alto Cortex XSOAR, are analyzed to illustrate current capabilities and limitations. Furthermore, the paper investigates the role of explainable AI (XAI) in improving analyst trust and decision-making within automated response systems. The findings underscore the importance of a balanced approach that combines automation, AI-based decision support, and human expertise, ensuring resilient, scalable, and adaptive cybersecurity operations capable of defending against evolving DDoS threats.

1 Introduction

The growing threat of cyberattacks, particularly *Distributed Denial-of-Service (DDoS) attacks*, poses a significant risk to organizations worldwide. These attacks overwhelm

targeted systems and services, leading to *service disruption, financial losses, and reputational damage* [15]. The challenge is especially critical in *sensitive and high-value sectors such as healthcare, finance, and critical infrastructure*, where system downtime can have life-threatening or highly disruptive consequences [16]. The increasing scale, sophistication, and automation of DDoS campaigns—often leveraging *botnets, IoT devices, and multi-vector attack strategies*—make traditional defense mechanisms inadequate [22, 4].

To address these challenges, *Security Orchestration, Automation, and Response (SOAR) technologies* have emerged as a vital component of modern cybersecurity operations [8]. SOAR platforms enable organizations to *detect, analyze, and respond to threats more efficiently* by integrating multiple security tools into a centralized system. Through *workflow automation, playbook-driven incident response, and orchestration of security processes*, SOAR reduces response time, minimizes reliance on manual intervention, and enhances consistency in security operations [10].

A key advancement in this field is the *integration of artificial intelligence (AI) and machine learning (ML)* into SOAR platforms [2]. AI-enhanced SOAR enables intelligent detection of anomalies and automated correlation of alerts, improving accuracy and reducing *false positives* [20]. Moreover, the use of *explainable AI (XAI)* offers transparency in decision-making, helping analysts understand the rationale behind automated responses and fostering trust in AI-driven security systems [12].

This study focuses on understanding the *core components of SOAR*, evaluating existing platforms such as *Fortinet FortiSOAR, IBM QRadar SOAR, and Palo Alto Cortex XSOAR* [6, 9, 18], and examining how AI integration strengthens DDoS detection and response. By addressing challenges related to *data quality, interoperability, compliance, and automation risks*, the paper highlights the need for a *balanced approach* that combines automation with human expertise. Ultimately, this research provides insights into how SOAR technologies, empowered by AI, can build more *resilient, adaptive, and proactive defenses* against evolving cyberthreats [13].

Understanding SOAR: What is it and how it works

SOAR, which stands for Security orchestration, automation and response, is a technology that combines incident response, orchestration, automation and threat intelligence management capabilities. Beyond the obvious uses of the technology as the term itself suggests SOAR provides services across operational manuals, workflows and processes, machine based assistance and human security in general. SOAR solutions are designed to manage workflows, store incident data, better utilize intelligence and more.

The term "SOAR" appeared the year of 2015 at the hands of Gartner, and its

solutions were divided according to its basic advantages: coordination of security, automation of security and response to accidents. Solutions work by integrating SOAR platforms with other tools, and through these integrations they can perform functions.

In other words, they are technologies that enable organizations to collect inputs monitored by the security team (e.g. SIEM alerts) for the purpose of analyzing and responding to attacks, where these responses are generated by both human and automated forces, Additionally, playbooks help standardize and streamline responses to various security incidents, ensuring consistency and reducing response time.

- **What is SIEM ?**

  Security Information and Event Management (SIEM) is a security solution that helps organizations detect threats, automate incident response, and ensure compliance by collecting and analyzing security data in real-time.

  Originally, SIEM combined only Security Information Management (SIM) and Security Event Management (SEM) without the intervention of artificial intelligence (AI). It has since evolved to incorporate AI, machine learning, and User and Entity Behavior Analytics (UEBA) for advanced threat detection.

  The key functions of SIEM include log management, event correlation, incident monitoring, and compliance reporting. This occurs after SIEM collects data from various infrastructures. Finally, it helps comply with standards such as PCI-DSS and GDPR through automated reporting.

- **SOAR vs SIEM**

  A quick comparison between SIEM and SOAR systems reveals the most significant differences in their approach.

  SIEM systems focus on comprehensive data collection, analysis, and alert generation (collecting and correlating logs from various sources, real-time monitoring, and generating alerts based on predefined rules and templates), threat detection, and compliance reporting. This requires greater manual intervention for investigation and response.

  SOAR solutions, on the other hand, focus on automating and streamlining security operations. SOAR reduces manual workload through automation. This distinct functionality makes SOAR a tool for improving operational efficiency and accelerating security incident management, rather than focusing primarily on detection and compliance, as is the case with SIEM.

- **What are Playbooks ?**

Feature	SOAR	SIEM
Purpose	Automates security tasks	Collects and analyzes security events
Automation	High level of automation using playbooks	Limited automation, requires manual analysis
Integration	Integrates with various security tools	Centralizes log data from different sources
Intelligence	AI and ML for intelligent response	Basic analytics and reporting

Table 1: SOAR vs SIEM

A SOAR playbook is an organized set of tools and processes used to respond to security incidents. By orchestrating security tools, it integrates orchestration, automation, and response.

Playbooks use conditions to trigger activities such as running scripts, adding tasks, updating data, or initiating external actions.

Using the playbook designer, workflows can be created through a visual interface, while rules and workflows provide flexibility to handle complex scenarios.

A vignette -in a SOAR platform is a brief scenario that outlines a specific type of security incident.A playbooks is an automated workflow to respond to these incidents. The mapping between them ensures that when a vignette is detected, the corresponding playbook is triggered, automating tasks like alert triage, containment, and remediation, reducing manual effort and response time.

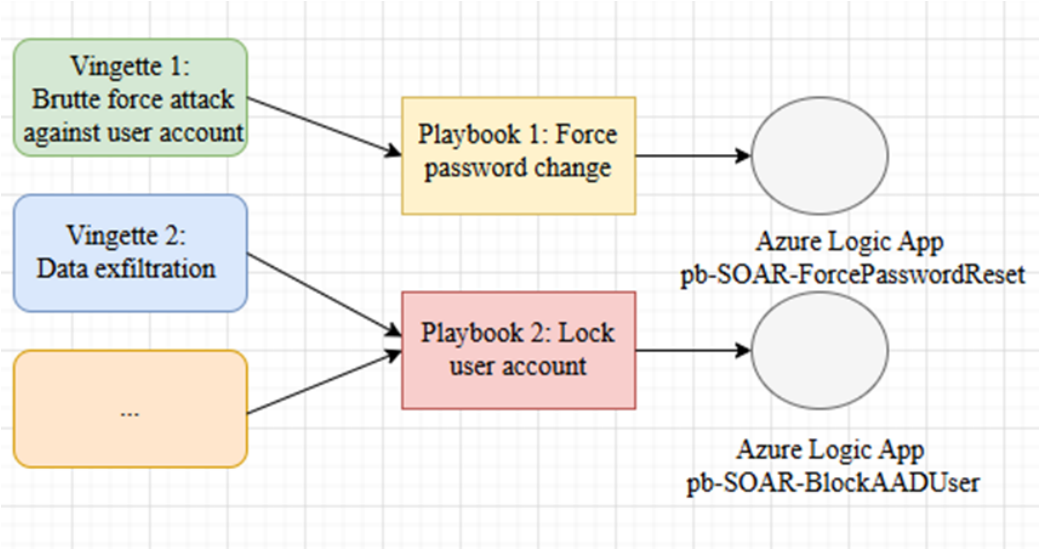

Figure 1: Mapping between vingettes & playbooks

- **Social Engineering Response in SOAR**

  It is a manipulation technique that awaits human error, centered on how people think and act. It is exploited to obtain private or valuable information, and also exploits users' lack of knowledge. In cybercrimes, unwary users are lured into revealing sensitive data, deploying malware, or allowing access to systems that are not intended to be accessed. Attacks can occur online, in person, or through other interactions.

  These are social engineering attacks (phishing, impersonation, phishing, and human psychology to breach security). Integrating these responses into a SOAR system improves threat detection and incident response.

  Social engineering techniques include:

Technique	Description	Vulnerability Exploited
Phishing	Sending deceptive emails	Trust in email communications
Pretexting	Creating a fake scenario to gain access to data	Authority and urgency
Baiting	Offering tempting rewards to lure users into clicking malicious links	Curiosity and desire for freebies

Table 2: Social engineering techniques

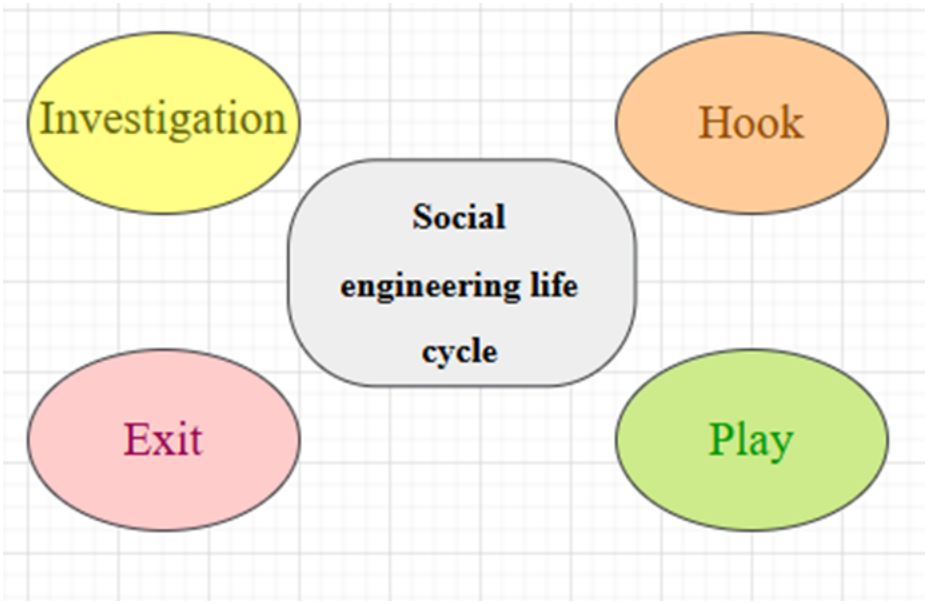

Figure 2: Social engineering life cycle

Generally, we see that SOAR solutions (Security Orchestration, Se-

curity Automation, and Incident Response) are based on three elements:

1.1 Security Orchestration

By integrating security tools (firewalls, antivirus, and threat intelligence platforms), the integration and integration of tools provides a security service without moving between tools.

Security Orchestration includes :

- Combining multiple security systems and applications.
- Integrating diverse security technologies.
- Synchronizing the functionality of security tools, thereby simplifying security procedures.
- Adapting to new threats and tools (due to an infrastructure-centric approach).
- Improving the integration of machine learning with threat detection and response.
- Enhancing response effectiveness.

Security Automation

That is, there are tasks that will occur automatically and they are tasks related to achieving security, for sure, such as creating tickets, analyzing alerts, enriching data, and others.

Security Automation ensures the following:

- Automation of security tasks (alert triage, vulnerability scanning, and log analysis).
- Reduction of human effort and response time.

- Improvement of effectiveness and efficiency.
- Enhancement of artificial intelligence/machine learning.

Incident Response

Several sources feed their events and alerts into a central unit, which is SOAR (SOAR collects these alerts), so that incidents are investigated and analyzed and thus work on a better response.

Some SOAR solutions provide artificial intelligence and machine learning technologies to provide proactive recommendations on how to deal with future threats.

SOAR mitigates many important obstacles faced by security teams, such as ensuring that all systems operate simultaneously and efficiently, gathering and compiling the necessary information to distinguish between real threats and false positives, and developing appropriate corrective actions to address risks.

Through its basic stages: detection, analysis, containment, eradication, recovery, and lessons learned, we summarize the importance of Incident Response in the following points :

- Responding to incidents by implementing necessary measures based on the analysis of security incidents.
- Providing tools for incident tracking, workflow management, and reporting.
- Improving response times and thereby reducing potential damage.
- Enhancing the integration of artificial intelligence and machine learning in determining the best course of action during incidents.
- Improving the effectiveness and efficiency of security systems.

With the integration of artificial intelligence and blockchain technology, SOAR platforms can further enhance their capabilities.

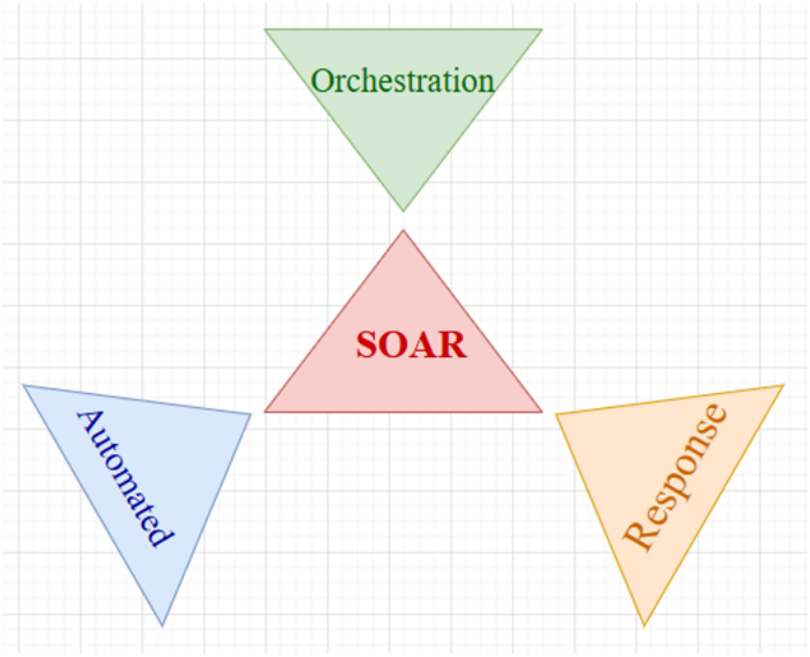

Figure 3: The three elements of SOAR

In general, the SOAR workflow includes five main steps:

- **Ingestion (or Collection):** Gathering data from various security tools (SIEMs, IDS/IPS, firewalls, etc.)

    1. **Analysis:** The SOAR system analyzes the received alerts to determine their nature, severity, and the severity of potential threats.
    2. **Decision:** Based on the analysis, SOAR systems and human analysts decide on the appropriate response to the situation. This is often done after assessing the severity of the threat and determining the type of intervention, whether automated or human-only.
    3. **Response (or Containment):** This is the process of implementing a previously planned response. The system implements pre-defined operational guidelines to mitigate the threat

(isolating affected devices, blocking malicious IP addresses, etc.)

4. **Feedback:** After the threat is addressed (response), feedback is collected on the actions taken by the system. Analysts will review incidents to improve processes and implement possible updates to operating manuals, ensuring a smarter and more efficient system over time.

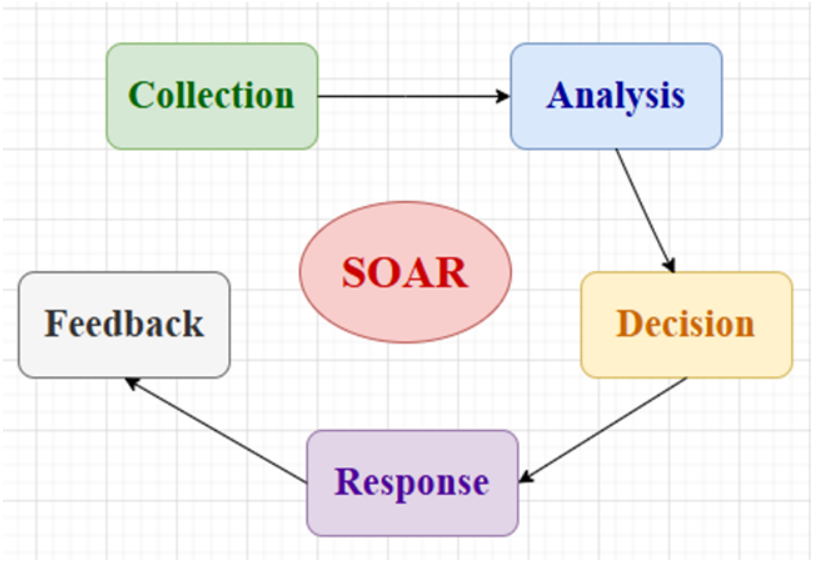

Figure 4: SOAR five essential steps

- **The Role of Blockchain in Strengthening SOAR Frameworks :** Blockchain security is a comprehensive risk management system for blockchain networks. It provides best practices to mitigate the risk of attacks and fraud.

  Blockchain technology plays a significant role in enhancing security (particularly in business operations). It is a powerful tool for enhancing cybersecurity, providing a decentralized system that protects data from fraud and manipulation and ensures trust based on consensus mechanisms and encryption. This technology enables several functions, including secure data sharing, automation

of business processes with minimal manual human intervention, supply chain management (transparently tracking products from source to destination), and improved transparency in government services.

Blockchain security uses a combination of cybersecurity best practices, proven frameworks, and technical safeguards to protect against fraud and cyberattacks.

Today, there are many different blockchain networks used in various fields around the world, including banking, healthcare, and more, so blockchain plays a fundamental role in our daily life.

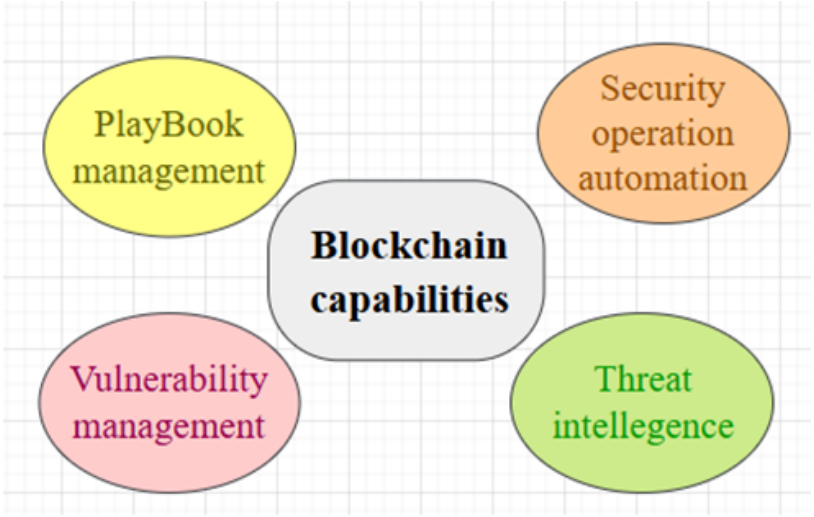

Figure 5: Blockchain capabilities

Existing Technologies for Incident Management

As we discussed earlier, SOR solutions are supervised by incident management technologies in order to detect threats and deal with them quickly. Here we list the most famous effective platforms for this:

Fortinet FortiSOAR

FortiSOAR is a SOAR platform used with SIEM, UEBA, or EDR that helps SOC teams thwart attacks by unifying incident management and automating the analysis that leads to investigation and effective response.

FortiSOAR is a leading SOAR platform that is used in conjunction with SIEM, UEBA, EDR, or other threat detection platforms... FortiSOAR helps IT/OT security teams thwart attacks by centralizing incident management and automating the myriad of analyst activities required for effective threat investigation and response.[7]

Figure 6: FortiSOAR UI

IBM Security QRadar SOAR

Microsoft describes Microsoft Sentinel as an update to the Security Operations Center, detecting and responding to the most complex threats,

and providing a robust security information and event management solution, all proactively while reducing costs by up to 48% compared to current SIEM solutions.

The platform offers several services:

- Accelerating the response process by using dynamic playbooks and AI-driven response recommendations.
- Simplifying, by time-stamping critical actions and integrating real-time threat intelligence.
- Compliance with over 200 global privacy and data breach regulations.

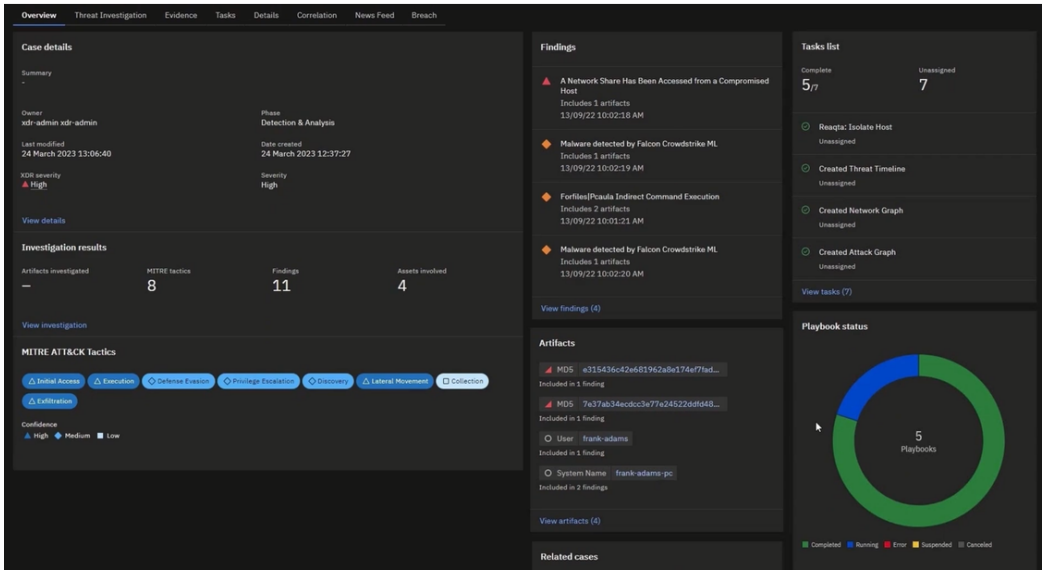

Figure 7: IBM Security QRadar SOAR UI

Best SOAR Platforms for Enhancing Security with Existing AI Systems

There are many security coordination, automation and response platforms, if enhanced with the power of artificial intelligence, this will

create a greater enhancement to the cybersecurity position of any organization. Here we list the most prominent platforms that provide this integration that combines the functions of artificial intelligence and solutions of security coordination, automation and response (SOAR) platforms.

Palo Alto Networks Cortex XSOAR

Through a single platform, Cortex XSOAR provides unified automation, case management, real-time collaboration, and threat intelligence, simplifying security operations. Simplifying everything helps speed up the response time, so it improves **incident response**, reduces the burden on analysts, and reduces manual tasks (NDIT in North Dakota used Cortex XSOAR to automate processes, which saved them about 8-10 additional analysts), and helps prevent attacks (via advanced tools like Mimikatz) such as data theft, which it automatically responds to.

Microsoft Sentinel

Microsoft describes Microsoft Sentinel as an update to the Security Operations Center, detecting and responding to the most complex threats, and providing a robust security information and event management solution, all proactively while reducing costs by up to 48% compared to current SIEM solutions.

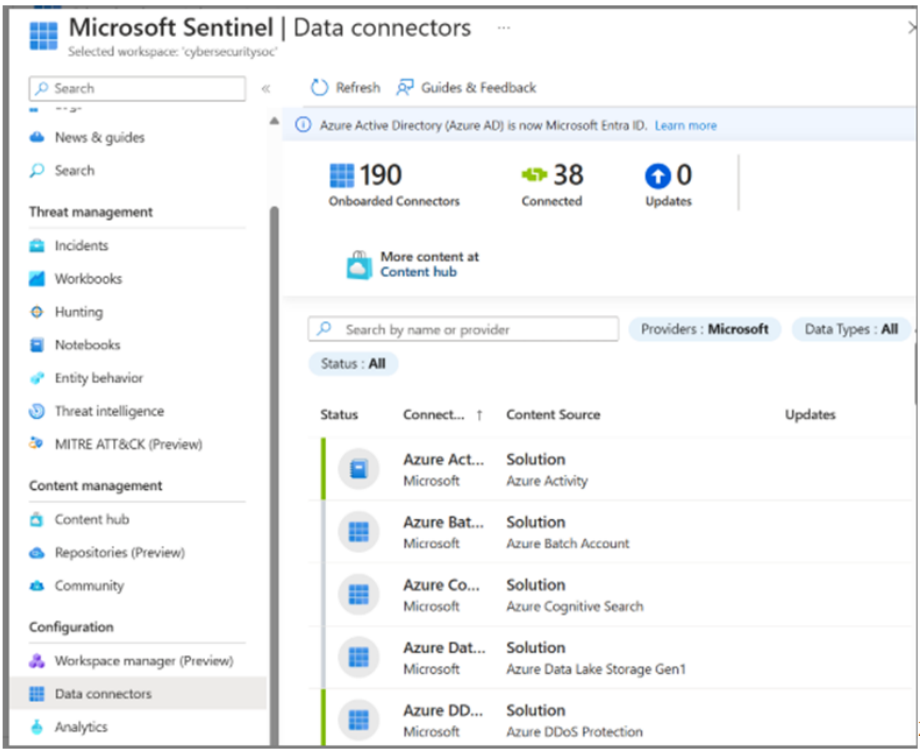

Figure 8: Microsoft Sentinel UI

Vectra AI

Vectra and Splunk integration enables discovery, triage, investigation, and response to security incidents from a central dashboard (i.e. one) based on artificial intelligence. The integration is deployed directly from Splunkbase.

The role of this platform is highlighted in removing the ambiguity created by attackers due to the large number of alerts they send, which conceal the real danger behind them. Security Operations Centers (SOC) can detect hidden threats, analyze data effectively, and anticipate attackers' attacks, which enhances their ability to defend and control.

[Cortex XSOAR helps simplify security operations by unifying automation, case management, real-time collaboration and threat intel

management. This datasheet gives you an overview of key Cortex XSOAR features, support programs and deployment options]

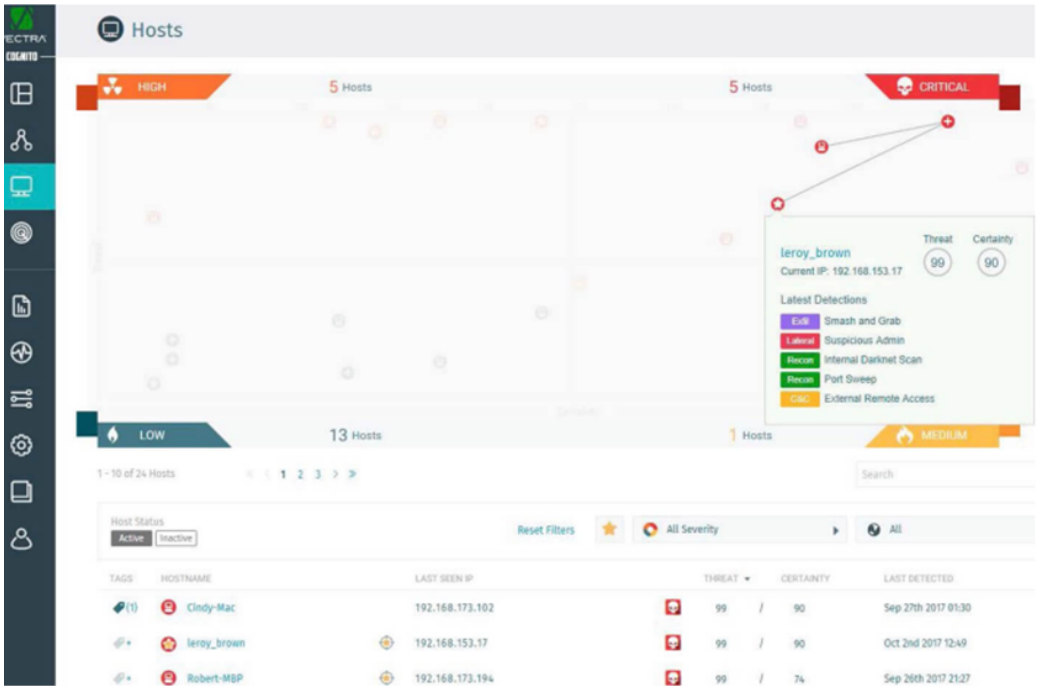

Figure 9: Vectra AI UI

Splunk

Splunk is a popular security information and event management (SIEM) platform. It collects security logs from various sources, detects any anomalies, and raises alerts.

Splunk is based on a philosophy of responsible AI use, while maintaining human participation in resolving processes. AI is designed to complement, not replace, humans.

Splunk offers customers and partners the ability to extend Splunk models or apply their own models to data across Splunk and other data stores.

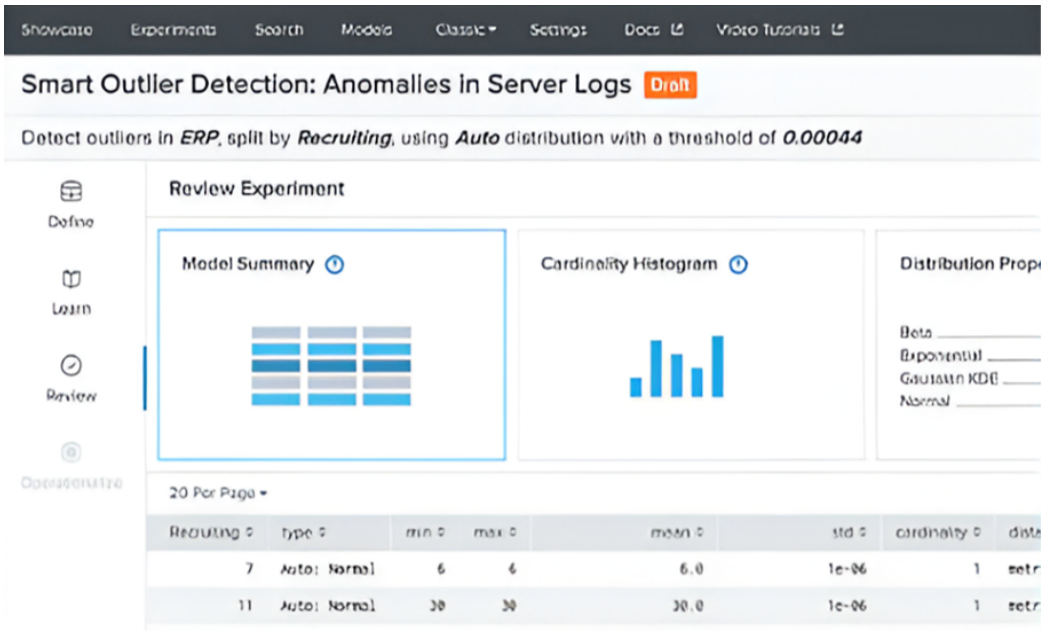

Figure 10: Splunk UI

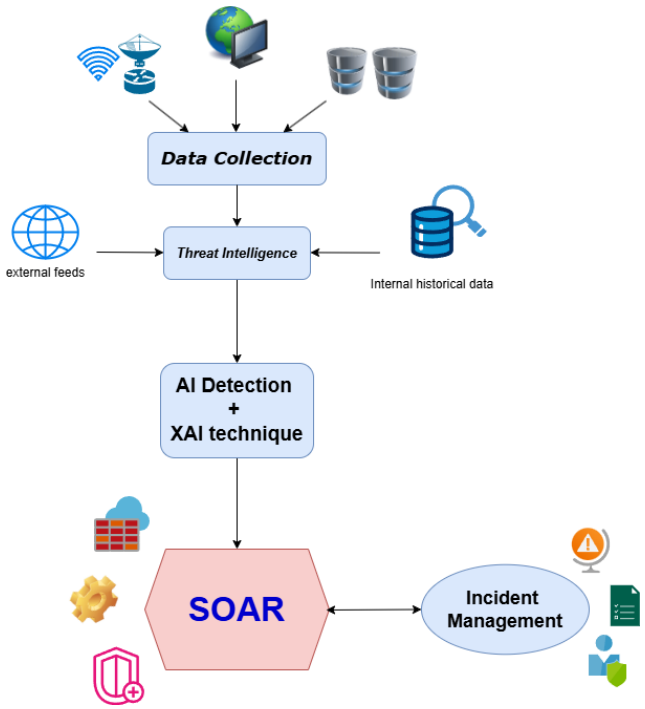

Figure 11: AI-Driven Threat Detection and Automated Incident Response Workflow

- **Phishing Emails Response Use Case with Splunk SOAR**

  This scenario was chosen because it is a common scenario where automation reduces response time. We assume the process will be processed by Splunk SOAR.

  A report reaches the Security Operations Center (SOC), say from an employee, about a suspicious email. Now it's the SOC's turn to automate the investigation and rapid response.

  1. **Trigger and Ingestion:**

     The platform receives the reported email (integration with email systems like Gmail allows this) or via a SIEM alert. Splunk SOAR then extracts key elements from the message, such as the sender's address, subject line, message content, and any attachments or URLs.

  2. **Automated Analysis:**

     Processing the message text, i.e. analyzing it and extracting information from it using natural language processing (NLP) and applying its algorithms, is useful in searching for phishing indicators.

     Checking attachments and URLs if any to see if they are malicious or benign, perhaps using threat intelligence sources (VirusTotal and URLhaus).

     Another essential element of the investigation is checking whether the sender's domain is registered and has not previously interacted with the organization (newly registered).

  3. **Decision and Response**

     In order for the system to decide to respond to an alert, it must classify its type:

     If the message is clearly and directly malicious, the sender's email domain is blocked, the message is deleted from all recip-

ients' inboxes to prevent similar scams, and links are disabled if there is any. Other measures are also taken.

If there is no clear malicious intent, the system takes certain actions based on unsubstantiated suspicion, such as isolating the message, escalating the alert to a human analyst, etc.

If the message is legitimate, no action is required.

4. **Post-Incident Actions**

   This is where machine learning and artificial intelligence can come into play, with the results fed into a machine learning model to improve phishing detection in the future.

   Supervised learning can be applied to train the model on classified phishing versus legitimate emails, use anomaly detection algorithms (such as quarantine forest, autoencoders), and improve the playbook by updating decision trees and automation workflows to handle emergencies identified during the incident.

5. **Feedback and Continuous Improvement** Review the actions taken and identify any shortcomings or errors, update operational manuals and machine learning models to improve detection accuracy, and share the results with the threat intelligence team to enhance future human responses. This can leverage past experiences and gain expertise, whether for machines or humans.

Limitations of Existing SOAR-AI Technologies

Although SOAR platforms integrated with AI are pioneering, effective, and indispensable for organizations, they face several challenges, including:

- ***False Positives***

Due to AI results that can sometimes be erroneous, and because the platforms are coupled with these models, benign activities may be classified as threats that must be stopped, which certainly increases the burden on analysts.

- ***Data Quality and Bias Issues***

This is related to the data that AI models rely on for training, which may be outdated, incomplete, or even biased, resulting in biased or incomplete results.

- ***Limited Contextual Awareness***

Context-based decisions are a challenge for AI in SOAR systems. Therefore, the lack of a deep understanding of processes, attack patterns, or other factors can lead to ineffective, if not harmful, responses.

- ***Over-reliance on Automation***

Total reliance on automation is harmful and can lead to disastrous consequences due to the potential for errors (blocking legitimate traffic or escalating non-critical incidents) resulting from other reasons already mentioned. Therefore, despite its power and effectiveness, the human element in processing operations must not be neglected.

- ***Compliance and Legal Challenges***

Complying with various privacy laws and security regulations for AI-powered incident response systems is a significant security challenge.

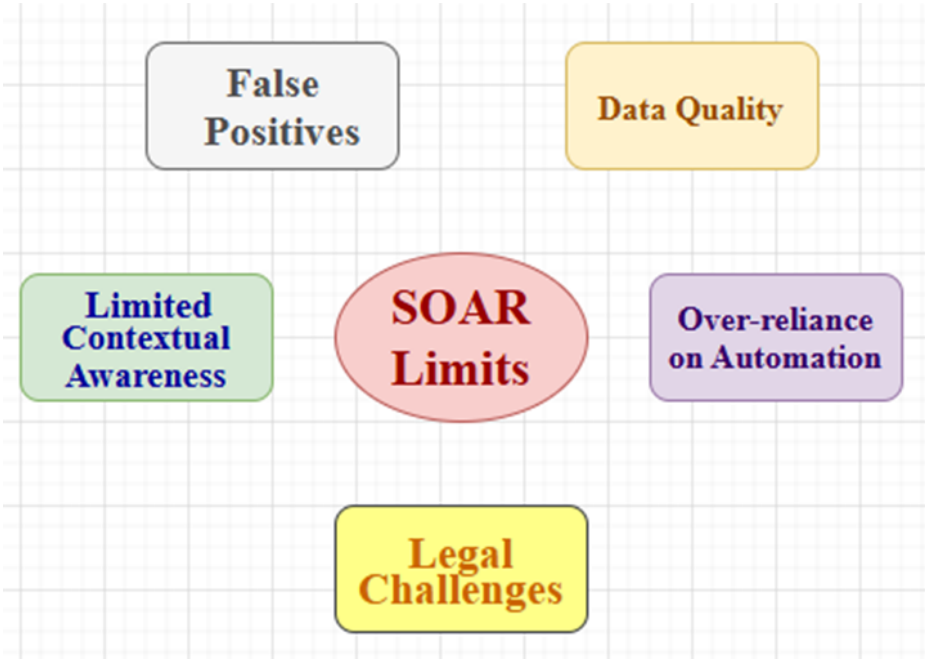

Figure 12: SOAR limitations

Conclusion

With the passage of time and the advancement and acceleration of modern technologies, threats are constantly increasing and may even become more complex than before. Therefore, SOAR technologies are a boon in the world of cybersecurity and protection for various types of systems institutions, networks, and even individuals as they provide protection against various types of malicious attacks, such as distributed denial of service (DDoS) attacks. This is achieved through their ability to automate process processing and rapid response to incidents, thereby reducing manual labor.

Artificial intelligence enhances these capabilities, making alert detection faster and smarter, and the system gains experience that provides it with stronger future performance based on continuous learning.

Although the integration of this duo suggests tremendous power in

cybersecurity, like any scientific approach, the combination faces challenges that we hope our defenses will evolve to confront in the future.

Bibliography

[1] Vectra AI. *Vectra AI and Splunk Integration Overview*. n.d. URL: https://www.vectra.ai/partners/splunk.

[2] Clarence Chio and David Freeman. *Machine Learning and Security: Protecting Systems with Data and Algorithms*. O'Reilly Media, 2018.

[3] Splunk SOAR Documentation. *Splunk SOAR Documentation: docs.splunk.com, Palo Alto Cortex XSOAR: paloaltonetworks.com, Wikipedia on Security Orchestration, Automation, and Response: en.wikipedia.org*. n.d.

[4] Christos Douligeris and Aikaterini Mitrokotsa. "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art". In: *Computer Networks* (2004).

[5] Fortinet. *Fortinet FortiSOAR Documentation*. n.d. URL: https://www.fortinet.com/products/fortisoar.

[6] Fortinet. *FortiSOAR Product Datasheet*. 2023.

[7] Fortinet Inc. *FortiSOAR Product Overview: Security Orchestration, Automation, and Response*. Available at: https://www.fortinet.com/products/fortisoar [Accessed: 26-Aug-2025]. 2023.

[8] Gartner. *Market Guide for Security Orchestration, Automation and Response Solutions*. 2019.

[9] IBM. *IBM QRadar SOAR Documentation*. 2023.

[10] IBM. *IBM QRadar SOAR Product Overview*. 2023.

[11] IBM. *IBM Security QRadar SOAR Documentation*. n.d. URL: https://www.ibm.com/security/security-intelligence/qradar.

[12] Scott Lundberg and Su-In Lee. "A Unified Approach to Interpreting Model Predictions". In: *Advances in Neural Information Processing Systems (NeurIPS)*. 2017.

[13] Vasileios Mavroeidis and Siri Bromander. "SOAR in Cybersecurity: Security Orchestration, Automation, and Response". In: *IEEE Security & Privacy* (2019).

[14] Microsoft. *Microsoft Sentinel Overview*. n.d. URL: https://learn.microsoft.com/en-us/azure/sentinel/.

[15] Jelena Mirkovic and Peter Reiher. "Internet Denial of Service: Attack and Defense Mechanisms". In: *ACM SIGCOMM* (2004).

[16] Yisroel Mirsky et al. "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection". In: *NDSS*. 2018.

[17] Palo Alto Networks. *Cortex XSOAR Datasheet*. n.d. URL: https://www.paloaltonetworks.com/cortex/xsoar.

[18] Palo Alto Networks. *Palo Alto Cortex XSOAR Product Overview*. 2023.

[19] OpenAI. *ChatGPT (March 22 version)*. Retrieved from https://chat.openai.com. 2025.

[20] Nathan Shone et al. "A Deep Learning Approach to Network Intrusion Detection". In: *IEEE Transactions on Emerging Topics in Computational Intelligence* (2018).

[21] S. Waelchli and Y. Walter. *Reducing the risk of social engineering attacks using SOAR measures in a real-world environment: A case study*. Demonstration of vignette 4, page 6, Fig. 2. Mapping between the vignettes and the playbooks. n.d.

[22] Wang Zhou et al. "A Survey of DDoS Attacks and Defenses in Cloud Computing". In: *IEEE Communications Surveys & Tutorials* (2021).

Acronyms

- **AI**: Artificial Intelligence
- **API**: Application Programming Interface
- **APT**: Advanced Persistent Threat
- **C2**: Command and Control
- **CERT**: Computer Emergency Response Team
- **DDoS**: Distributed Denial of Service
- **DNS**: Domain Name System
- **EDR**: Endpoint Detection and Response
- **HTTP**: HyperText Transfer Protocol
- **HTTPS**: HyperText Transfer Protocol Secure
- **IBM**: International Business Machines
- **IDS**: Intrusion Detection System
- **IPS**: Intrusion Prevention System
- **IoT**: Internet of Things
- **MITRE ATT&CK**: MITRE Adversarial Tactics, Techniques, and Common Knowledge framework
- **NOC**: Network Operations Center
- **OT**: Operational Technology
- **QRadar**: IBM's Security Information and Event Management (SIEM) platform
- **SIEM**: Security Information and Event Management

- **SOC**: Security Operations Center
- **SOAR**: Security Orchestration, Automation, and Response
- **TCP**: Transmission Control Protocol
- **UDP**: User Datagram Protocol
- **UEBA**: User and Entity Behavior Analytics
- **VM**: Virtual Machine
- **XAI**: Explainable Artificial Intelligence