*Intelligent Automation & Soft Computing*
DOI:10.32604/iasc.2021.016240
***Article***

Tech Science Press

# AI/ML in Security Orchestration, Automation and Response: Future Research Directions

**Johnson Kinyua[1] and Lawrence Awuah[2,*]**

[1]College of Information Sciences and Technology, Pennsylvania State University, State College, PA 16801, USA
[2]Department of Cybersecurity, University of Maryland Global Campus, Adelphi, MD 20783, USA
[*]Corresponding Author: Lawrence Awuah. Email: lawrence.awuah@umgc.edu
Received: 28 December 2020; Accepted: 28 January 2021

**Abstract:** Today's cyber defense capabilities in many organizations consist of a diversity of tools, products, and solutions, which are very challenging for Security Operations Centre (SOC) teams to manage in current advanced and dynamic cyber threat environments. Security researchers and industry practitioners have proposed security orchestration, automation, and response (SOAR) solutions designed to integrate and automate the disparate security tasks, processes, and applications in response to security incidents to empower SOC teams. The next big step for cyber threat detection, mitigation, and prevention efforts is to leverage AI/ML in SOAR solutions. AI/ML will act as a force multiplier empowering SOC analysts even further. We conducted a detailed survey by studying work by both security researchers and industry practitioners on SOAR, including its interpretations, from an AI/ML perspective by reviewing works published in academic journals, conferences, websites, blogs, white papers, etc. (a multi-vocal view). We report on our findings and future research directions in this area.

**Keywords:** Security management; security orchestration and automation; machine learning; SOAR; security orchestration; security automation; deep learning; deep reinforcement learning; incident response

## 1 Introduction

Today's SOC analysts are finding it increasingly difficult to effectively monitor and manage current levels of data volume, velocity, and variety across firewalls, IDS, and SIEM devices. This is exacerbated by the fact that most medium to large organizations use a multitude of security tools/products to secure their data, network, endpoint devices and other critical infrastructure. In addition, organizations lack a single security tool that can meet all their security operations needs and end up installing several types of products and tools from different vendors that provide different dimensions of security services and solutions. It is not unusual for an organization to have more than two dozen security tools running simultaneously to identify and prevent cyber-attacks. This results in complex security stacks with increased overhead in terms of cost and time for SOC establishments. Current cyber defense products and tools work independently, have their own data representations and interpretation mechanisms with no

standardization for data exchange between different tools, have inconsistent workflows, and have a non-integrated architecture [1]. Consequently, SOC analyst may find it difficult to have a holistic picture of their organizational security posture through individual security tools working separately, and to appropriately configure and integrate the activities of multi-vendor security products and tools. This challenge usually calls for continuous involvement of humans (HITL) in the entire process of security incident response that places a heavy burden on human experts, which leads to complex, inefficient and suboptimal incident response processes and security management in general. Moreover, threats continue to escalate at a breakneck rate and make the situation worse due to the complexity of security stacks and the diversity of security tools. The disappointing shortage of security experts is also a contributing factor in this strenuous task [2–4].

A Security Information and Events Management (SIEM) system was designed to collect, correlate, and store security events and generate appropriate security alerts for the Security Operations Center (SOC) operational needs. Since their inception, SIEM systems functionality have evolved to include various levels of threat intelligence (TI), which allow the more accurate generation of security alerts as well as basic enrichment of previously generated alerts. Following alert generation and perhaps basic enrichment, incident response has remained a largely manual process in SIEM-only environments. Using the SANS PICERL (Planning, Identification, Containment, Eradication, Recovery and Lessons Learned) incident response framework, a SIEM falls in the Identification phase [5]. Popular threat detection technologies such as SIEMs, IDS/IPSs, UTMs, and next-gen firewalls lack awareness of an organization's entire IT ecosystem.

Therefore, there is a need to automate and orchestrate processes by plugging in various tools using vendor-specific APIs to empower analysts to investigate and make decisions that increase the effectiveness of incidence response processes. An incident response playbook is a linear-style checklist of steps and actions (workflows) needed to respond successfully to specific incident types and threats. A playbook has a defined set of rules and actions that are executed and triggered by one or more events. Security Orchestration, Automation, and Response (SOAR) systems are designed to pick up the incident response process where SIEM functionality ends, providing an automated and orchestrated response throughout the Identification Phase, as well as the Containment, Eradication and Recovery Phases. SOAR is a critical component of cybersecurity threat mitigation when the disparate tools are integrated within a common platform. Traditionally, security logs are displayed by different consoles by different appliances such as SIEM, UTM, Threat Intelligence (TI), Endpoint Detection and Response (EDR) solutions, and sandbox solutions making it tedious and challenging for SOC analysts and cybersecurity experts to track emerging cyber threats and attacks. Some SOAR solutions, such as IncMan by DFLabs [6], also enable the Planning and Recovery Phases through features such as knowledge bases, key performance indicators, and advanced reporting. SOAR and SIEM are complementary solutions with which each provide a unique set of values to the organization which are extremely powerful when combined as part of a holistic security program. A SOAR solution is not the same as a SIEM solution and does not need a SIEM to function properly. SIEM solutions which have been key cyber defense platforms in industry for over a decade have been subsumed by SOAR solutions which are discussed in more detail in the other sections of this paper.

A SOAR system is not intended to be a replacement for skilled SOC analysts. Deploying a SOAR solution with the intended goal of replacing analysts will inevitably create more risk than it mitigates. The traditional human-in-the-loop (HITL) model of man-machine integration struggles to adapt nimbly in dynamic cyber defense environments because the machine or some autonomous agent carries part of the task and must halt to wait for the SOC analyst's response before completing the task. What is required is a human-on-the-loop (HOTL) model of man-machine integration that allows the machine to autonomously perform a task whilst the SOC analyst monitors and intervenes the operations only when necessary. Hence, a SOAR solution should be viewed as an enabler for the security program and the

security analysts alike. SOAR solution should be viewed as a force multiplier for security analysts, allowing them to work smarter and provide increased value to the organization. According to Gartner, "by year-end 2022, 30% of organizations with a security team larger than five people will leverage SOAR tools in their security operations, up from less than 5% today" [7]. According to the Enterprise Strategy Group (ESG), "19% of enterprise organizations have already deployed technologies for security automation and orchestration extensively, 39% have done so on a limited basis, and 26% are engaged in a project to automate/orchestrate security operations" [8].

The need to prop up defensive cyber operations with advances in automation and autonomy has also gained tractions in today's search for efficient technology solutions. This is a critical aspect of cyber threat detection, mitigation, and prevention efforts. However, in automating threat detection, mitigation, and prevention, collecting actionable cyber threat intelligence (CTI) remains a huge challenge. In other words, the development, implementation, and maintenance of technologies to enable automation and autonomous/semi-autonomous systems as part of defensive capabilities are key to defensive cyber operations. In these efforts, machine intelligence has become ubiquitous and indispensable tool in defensive and offensive cybersecurity operations.

AI/ML-powered cyber defense systems will be instrumental in responding to the continuing growth in the number and complexity of threats, the evolving nature of threats, and the need for rapid and substantially automated responses to threats. For example, AI/ML-powered defense systems have the ability to analyze large data sets and identify anomalies and suspicious patterns instantaneously. Automatic updates to existing software based on sophisticated real-time analysis by AI/ML can prevent cybersecurity attacks on a large scale. Large-scale email providers are using AI techniques to prevent undesirable images, detect phishing, malware and fraudulent payments [9,10]. Other providers are using artificial neural network (ANN)-based models for detection and classification of phishing and malware emails [11]. Additionally, AI/ML is ideal for malware detection and anti-virus defense and does not rely on static signatures used in conventional anti-virus systems [12,13]. The primary targets for AI/ML applications at present are known to be intrusion detection (network-based attacks), phishing and spam (emails), threat detection and characterization, and user behavioral analytics.

A recent study revealed that organizations are increasing the pace of adoption of AI/ML in cybersecurity and overall, close to three-quarters of firms surveyed admitted that they were testing use cases for AI/ML for cybersecurity [9]. In the development of SOAR systems, the role of machine intelligence and cybersecurity analytics in automating threat detection and prevention, threat intelligence are critical part of SOC strategic and tactical functions. Hence, the development, implementation, and maintenance of intelligent and adaptive cyber analytics capabilities to enable orchestrations and automations as part of SOC capabilities are key to defensive and offensive cyber operations [14]. The desire to use AI/ML to learn, adapt and potentially act autonomously to enhance decision making, reinvent business strategies is expected to be the forefront for cybersecurity professionals and technology vendors for digital initiatives through 2025 [15].

The main contributions of this survey paper are as follows:

- Provided a synthesis of security orchestration, automation and response endeavors by security researchers and practitioners from an AI/ML perspective.
- Reviewed various interpretations of security orchestration and automation and created a unified definition of security orchestration and automation that integrates important themes and concepts associated with SOAR.
- Reviewed the capabilities of SOAR solutions provided by several top vendors from an AI/ML perspective
- Identified key areas for security researchers to investigate for AI/ML powered security orchestration, automation and response systems.

The rest of this paper is organized as follows. In Section 2 we explore SOAR and SOAPA concepts based on our review of the literature. In Section 3, we discussion security orchestration and automation efforts. Section 4 explores on AI/ML integration in well-known current SOAR solutions. In Section 5, we review AI/ML research in SOAR. In Section 6, we explore future research directions for AI/ML powered SOAR systems. The conclusion is provided in Section 7.

## 2 SOAR and SOAPA

In this section, we discuss SOAR and the Security Operations and Automation Platform Architecture (SOAPA) and explore the differences between them. We first discuss SOAPA and then SOAR detailing the internal architectures of both platforms, and illustrating them using schematic diagrams that we developed. SOAPA is an architecture made up of many product categories, which is designed to ensure efficient and effective data collection, processing, sharing, and analysis [16]. SOAR is a product line category of SOAPA. A SOAPA platform integrates technologies across data collection, processing, analytics, and security operations as depicted in Fig. 1.

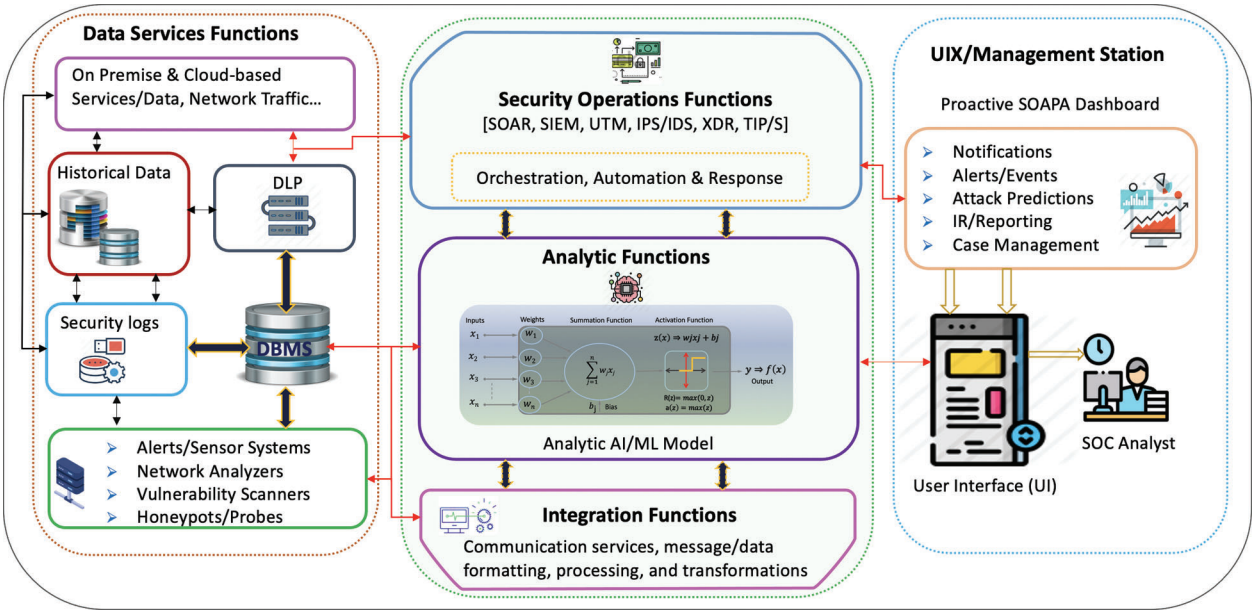


**Figure 1:** A High-Level Multi-Functional SOAPA System

With SOAR as a product line category and SOAPA as an architecture consisting of several product categories, platforms, and functions, we reviewed both systems in our study from the perspectives of the existing literature, the manufacturers of these platforms, and the professionals in the field. From the standpoint of how the SOAPA platform integrates several technologies, our SOAPA architecture has four key functions along with a user interface/management station. The back-end functions include security operations, analytics, integration, data services functions, as well as the front-end user interface and experience (UIX)/Management station as shown in Fig. 1.

In addition, the security operations functions of Fig. 1 carry out the orchestration, automation and response tasks and focus on incident response operations to detect, classify, and address threats detected by SOAPA systems to create actionable alerts or intelligence. Some security devices relevant to facilitate these functions include SOAR, SIEM, UTM, TIP and others. Additionally, this system functions to

minimize such metrics as mean time to detect (MTTD), mean time to respond (MTTR), and time to investigate (TTI), which drive effective incident response investigations. From the perspective of the analytic functions, the embedded AI/ML model with encapsulated algorithms promotes the intelligence-based classifications and predictions and analysis of security logs and other network traffic. These intelligent models help monitor endpoint devices, attack behaviors, and threat intelligence, which are required to accelerate threat detection and prioritization of security incidents.

Furthermore, the integration functions (Fig. 1) serve as an interconnected and integral hub between data services functions, analytic functions, security operations functions, and the front-end UIX/management station. Key roles include delivering communication services, message formatting, processing, and transformations functions. As the name suggest, the data services functions are responsible for data generation, data aggregation, data protection, and data storage capabilities. As the SOAPA deals with huge number of security logs, effective management, processing, and protection of data is essential to the overall functioning of the entire SOAPA system. Finally, the front-end UIX/management station of Fig. 1 tie it all together to the SOAPA dashboard with telemetric and case management system information, which produces appropriate metrics including notifications, alerts, events, predictions, and reporting. In this case, SOC team and analysts can analyze this critical information via appropriate user interfaces with the capability to mitigate all forms of cyberthreats.

According to Oltsik, a SOAPA architecture is composed of a common distributed data service, software services and integration layer, analytics layer, and security operations platform layer [17]. A combination of these functions allows for efficient and effective SOC to facilitate collaboration between various security operations teams with integration of appropriate tools, technologies, and processes to ensure system and data protection. According to Laliberte, implementing a common distributed data services layer as part of a comprehensive SOAPA along with security operations, orchestrations, and automation can reduce costs, mitigate risks, and improve operational efficiency for the SOC team [18]. Working in tandem with the other SOAPA's bottom-up architecture capabilities such as the analytics layer, the common distributed data service can help the SOC team collect, process, and distribute the right data to the right tools at the right time. From the perspectives of the analytics layer, the cybersecurity analytics functions can be employed to data that can be analyzed, managed, and reported by a host of technologies working in tandem [17]. This aligns with the analytics function of SOAR platform that deploys statistical models for analytics to score indicators, provide insights across datasets, and improve the ability to recommend actions [17,19,20]. Additionally, AI/ML along with process automation and orchestration can be effectively used to improve threat prevention, detection, and response [16,18,21].

Within the SOC environment, a SOAR solution, part of the security operations platform layer within SOAPA, triggers actionable security operations playbooks to facilitate investigations, delegate tasks, orchestrate disparate tools to create workflows or playbooks, and automate remediation actions, among many other diverse capabilities. For example, with the complimenting capabilities of both SOAR and SIEM, a SOC analyst can use the derived aggregated log files and playbooks to derive a system profile, which can be used as a baseline to identify and detect network anomalies. SOAR and SIEM tools represent a component of SOAPA, which combine a set of technologies that unify them into one huge integrated platform. SIEM solutions which have been key cyber defense platforms in industry for over a decade have been subsumed by SOAR solutions which are discussed further below.

Additionally, the SOAPA is a bottom-up architecture with a programmable top layer or stack, which can be instrumented to take automated actions, such as gathering data for an investigation, blocking a network connection, or opening a trouble ticket in a case management system, among others [21]. The SOAPA technologies can further integrate advanced analytics with security operations process management designed to help organizations improve security lifecycles from data collection to threat detection through

incident response [16]. Furthermore, the tightly coupled architecture adds advanced analytics using AI/ML-based process automation and orchestration to improve threat prevention, detection, and response [16,21].

After SOAPA analytics engines identify problems, the automation and orchestration layer of SOAPA, the SOAR portions, can help the SOC team coordinate incident response and remediation processes [18]. The SOAR's automation and orchestration processes can actively support tasks like case management, collaborative workflows, and process automation as indicated in Fig. 1 [16,21,22]. Developing tools to automate some key security activities such as alert triage, case management, indicator enrichment, threat intelligence collection, response, and reporting cannot be overemphasized. Organizations need relevant security tools to automate manual repetitive tasks. Fujitsu has emphasized that an efficient SOC requires automation of the processes of the threat defense life cycle to free up SOC analysts' time and keep the system up to date [23]. Industry practitioners and researchers have for some years recognized the importance of coordinating and automating key security activities offered by SOAR. However, the definition of the terms orchestration and automation vary slightly across practitioners and researchers.

Microsoft defines security automation and security orchestration as follows: "Security Automation is the use of information technology in place of manual processes for cyber incident response and security event management" while "security orchestration is the integration of security and information technology tools designed to streamline process and drive security automation." [24]. ThreatConnect has provided the following definitions for security automation and security Orchestration [25]: "Security automation is the automatic handling of a task in a machine-based security application that would otherwise be done manually by a cybersecurity professional" and "security orchestration is the connecting and integration of various security application and process together". According to Forrester, security automation and orchestration should be described together as technology products, and they have defined security automation and orchestration as follows [26]: "Technology products that provide automated, coordinated, and policy-based action of security processes across multiple technologies, making security operations faster, less error-prone, and more efficient". Islam et al. have defined security orchestration as follows [1]: "Security Orchestration is the planning, integration, cooperation, and coordination of the activities of security tools and experts to produce and automate required actions in response to any security incident across multiple technology paradigms".

*We define SOAR as the end-to-end planning, coordination, cooperation, and integration of the activities of disparate security services, processes, applications, and tools, along with the SOC team, to automate required actions in response to security incidents across enterprise security processes and technologies*.

Fig. 2 depicts a SOAR system and the SANS PICERL incident response framework mentioned in section 1. It integrates security automation, orchestration, and incident response; and critical to a SOAR system is actionable threat intelligence (TI). Actionable TI is a critical component of an effective and efficient incident response program. According to Solomon, actionable TI means that it is accurate, relevant and timely in order to enable an organization to take a proactive approach to cybersecurity with connectivity to the entire security footprint [27,28]. A proactive security program requires actionable threat intelligence be properly correlated to discover attack patterns, potential vulnerabilities, and other ongoing risks to the organization. Generally, this correlation should be automated and be able to provide information on whether an ongoing incident shares common factors with any previous incidents. The other important component of modern and future SOAR solutions is leveraging AI/ML in its automation, orchestration, incident response and threat intelligence capabilities as depicted in Fig. 2. Further aspects of SOAR solutions are discussed in Sections 3 and 4.

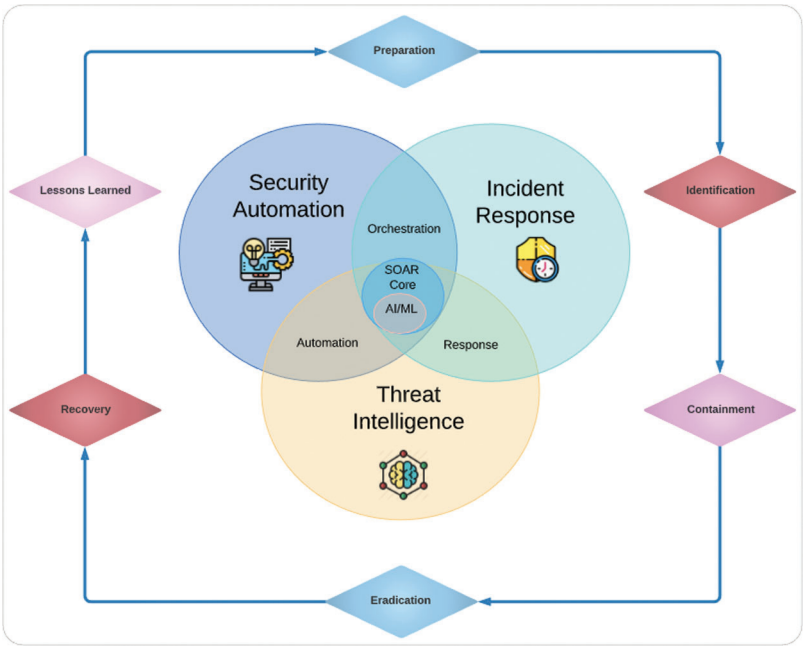


**Figure 2:** A SOAR System and SANS PICERL Phases

## 3 Security Orchestration and Automation Efforts

Automation of security controls for network access and device compliance initiatives for a SOC team is a necessity. In one research study, Montesino et al. [29] noted that a security control can be automated provided that the operation of the control can be performed without the intervention of humans in the playbook process. The authors indicated that about 30% of the security controls can be automated. In a situation like this, SOAR can play a key role by providing a unified operational environment, which allows security teams to be more efficient in addressing security incidence response concerns. Fortunately, such controls can present pragmatic approaches offering prioritized guidance on critical steps for implementing SOAR-specific orchestration and automation in incidence response requirements, a blueprint for reducing risk and managing compliance.

By automating security controls, SOCs can enable security teams to do much more with less, essentially operationalizing cyber response best practices. In order to identify automatable controls, Montesino et al. [29] surveyed several enterprise level security software and hardware solutions with emphasis on those that allow the automation of operations of controls in a centralized fashion. The authors were of the view that a Security Content Automation Protocol (SCAP) can be used to validate information security management processes in order to provide an automated way of making some functionalities feasible. This assessment or observation implies that performing continuous monitoring of system security configuration settings, examining systems for potential threats or compromise, or having situational awareness can lead to an improved security posture of the organization [29].

A research study conducted by Saraiva de Sousa et al. [30] on network service orchestration indicates that coordinating specific network services and actions can respond proactively to changes in network conditions to achieve resilience and fault tolerance capabilities without human intervention similar to that in a SOAR system. Another study also provided a taxonomy of security orchestration based on the execution environment, automation strategy, deployment type, mode of task and resource type comparable to network service orchestration [3]. Obviously, one of the goals of the security orchestration is to bridge the gap between detection and remediation of security incidents [3] making orchestration at

the task level for applications more flexible, robust, and more dynamic and smarter. Additionally, Ahmad and Kim proposed orchestration at the task level that is scalable and flexible due to the automation at a more granular level [31]. Wang et al. proposed a Security Device Orchestration Framework (SDOF) with the aim of realizing real-time dynamic orchestration by putting forward uniform interfaces and designing a data-driven orchestration engine [32]. The authors perceive orchestration as one of the key features of Software-Defined Security (SDS), which not only facilitates open services, but also allows devices from multi-vendor provided services in the same application layer of SDS.

AlSadham and Park proposed a framework to enhance Information Security Continuous Monitoring (ISCM) capabilities by leveraging security automation to achieve real-time threat detection, incident response, and risk-based decision-making capabilities [33]. With rapid pace of development and desire for more effective cyber defense strategies, AI/ML comes as a solution to the problem of coping with incidence response initiatives to mitigate the ever-growing number of cybersecurity attacks [11]. One power of SOAR lies in the use of trackable metrics, which helps cybersecurity analysts better understand the effectiveness of workflows by swiftly identifying and addressing potential areas for improvement [34]. The key SOAR metrics, according to the researcher, include mean time to detect (MTTD), mean time to respond (MTTR), time to qualify (TTQ), and time to investigate (TTI), which empower the SOC leadership to audit the overall business value driven by the team. These metrics are key ingredients to mitigate security incidents because many security breaches go undiscovered for longer than expected, giving attackers more time to pivot different network segments and hence the likelihood to access sensitive information. The faster detection and response time amount to less damage to organizational asserts.

According to Shoard [35], consolidation of security operations capability, such as integration of user and entity behavior analytics (UEBA) capability in many security information and event management (SIEM) platforms, is an important element in all forms of threat mitigations. Network detection and response (NDR) vendors continue to implement state-of-the-art automated and manual response features in their solutions by applying ML models and other analytical techniques to network traffic [36]. This approach helps enterprises detect suspicious traffic far better than other security tools. In addition, NDR can monitor network traffic that crosses the enterprise perimeter as well as analyze raw traffic and/or flow records from strategically placed network sensors to build models that reflect normal network behavior.

SOAR have become closely aligned with security incident response and general operations processes to the extent that SIEM vendors have incorporated automated response capabilities to various levels of their products [37]. Neiva et al. noted that lack of centralized capabilities in the SOC solutions leaves security teams with a responsibility to manually collect and stitch all triaging components together in manual playbooks for tasks related to the severity of incidents. The role of machine intelligence cannot be overemphasized. By 2022, at least 40% of new application development projects will have AI co-developers on the team [38]. Despite all the benefits derived, AI models and Algorithms have the flip side, which can catastrophic. According to Gartner analyst Cearley et al, by 2022 30% of all AI cyberattacks will leverage training-data poisoning, AI model theft or adversarial samples to attack AI-powered systems, while 30% of organizations using AI for decision making will contend with shadow AI as the biggest risk to effective and ethical decision-making.

## 4 AI/ML Integration in SOAR Solutions

Several SOAR systems are available such as FireEye, IBM Resilient, Splunk, Demisto, DF Labs, etc. These tools use a platform-based approach for provisioning security orchestration, automation, and response activities of the threat defense lifecycle. The tools available differ in platform capabilities in terms of automation strategy, execution environments, how they are deployed (i.e., distributed, centralized, or hybrid), level of automation, and resource type [1]. HEXADITE has identified five

approaches to security automation adopted by current vendors based on the tools/techniques used: workflow tools, orchestration tools, scripting tools, prioritization tools, and intelligence security automation [39]. Our focus is on intelligent security automation strategies leveraging AI/ML techniques. We consider intelligence security automation as a security orchestration platform that includes some of the available automation tools as well as AI/ML capabilities to orchestrate and automate incident response processes. According to Demisto, automation and human tasks need to be interweaved and work together in a seamless fashion to achieve the desirable goal [40]. A recent study by Capgemini [9] revealed that organizations are increasing the pace of adoption of AI/ML in cybersecurity and overall, close to three-quarters of firms (73%) surveyed said they were testing use cases for AI/ML for cybersecurity. The survey also revealed that 28% are using security products with AI/ML embedded, with 30% using proprietary AI/ML algorithms. The remainder, 42%, currently either use (or plan to use in the next year) both proprietary solutions and embedded products.

We reviewed several top SOAR solutions according to Gartner and other sources [41–45]. Our objective was to compare these platforms based on the following SOAR capabilities: automation, orchestration, response, and how these platforms leverage AI/ML in the incident response processes. There are two incident response frameworks that are mainly used in industry, the NIST [46] framework and the SANS framework [47]. A comparison of these frameworks is provided in [5], and we opted to compare the levels of automation using the SANS PICERL (Planning, Identification, Containment, Eradication, Recovery and Lessons Learned) incident response framework. In particular, we focused on the Identification, Containment, Eradication, and Recovery (ICER) phases, because available sources did not discuss how these platforms support the planning and lessons learned phases.

All SOAR security solutions incorporate internal and external TI in the incident response processes. The automation capability is a core feature of any SOAR security platform, and automation is implemented using playbooks and runbooks [27,48]. A playbook is a linear-style checklist of steps and actions (workflows) needed to respond successfully to specific incident types and threats. Incidence response playbooks provide a simple step-by-step, top-down approach to orchestration. Because workflows are the core of the automation and orchestration processes within a SOAR solution, both flexibility and ease of use are equally important. In contrast, a runbook consists of a series of conditional steps to perform actions, such as indicator enrichment, threat containment and sending notifications, automatically as part of the incident response or security operations process. Runbooks are flow-controlled workflows and they should be able to support different types of flow control mechanisms, including those that allow SOC analysts to make decisions manually before the workflow continues. The implementation of these workflows (playbook or runbook) should be flexible enough to support nearly any process, which might need to be codified within a SOAR solution.

We reviewed the levels of orchestration by considering which phases of ICER framework were supported by the orchestration capability. The final important consideration is where and how AI/ML was leveraged by these platforms in the ICER phases of the SANS framework. Tab. 1 shows the results of our survey. All SOAR platforms support automation and orchestration in all four phases of the SANS ICER framework. The main difference that we found is where and how AI/ML is leveraged in the SOAR platforms as discussed below.

AI/ML is leveraged in different ways in the various SOAR platforms reviewed. FireEye has implemented a ML PowerShell detection engine for detecting PowerShell attacks, and it is able to successfully detect commodity malware such as Kovter and red team penetration test activities [49–52]. In addition, they have developed a production end-to-end ML pipeline that constantly evolves with adversaries through re-labeling and re-training. Another notable use of AI/ML is FireEye's MalwareGuard that uses a ML model to detect and prevent Malware [53]. Siemplify's SOAR platform

leverages Machine Learning to better prioritize and investigate alerts and assign the best analyst to a case. Secondly, ML continuously analyzes and prioritizes an analyst's case queue to ensure analysts address critical cases first. It assigns higher priority to cases that resemble ones historically deemed malicious and assigns a lower priority to cases resembling ones that were previously flagged as false positives. In assigning the best analyst to a case, the ML algorithms use the previous analyst's performance to make instant case assignment recommendations to maximize an analyst's productivity and effectiveness. Finally, Siemplify's SOAR platform has an ML capability that also provides a list of similar cases that analysts can use to aid their current investigation based on historical contexts to inform the response actions they may take for their active investigations.

**Table 1:** Automation, Orchestration Levels (OL) and AI/ML in SOAR Platforms

| | AUTOMATION | | | | | OL | AI/ML |
|---|---|---|---|---|---|---|---|
| **VENDORS** | **CTI** | **Identification** | **Containment** | **Eradication** | **Recovery** | **ICER** | **ICER** |
| **FireEye** | * | * | * | * | * | ICER | ICE |
| **IBM Resilient** | * | * | * | * | * | ICER | ICER |
| **Splunk** | * | * | * | * | * | ICER | ICER |
| **Siemplify** | * | * | * | * | * | ICER | ICER |
| **D3 Security** | * | * | * | * | * | ICER | ICER |
| **DFLabs** | * | * | * | * | * | ICER | ICER |
| **Rapid7** | * | * | * | * | * | ICER | ICER |
| **ThreatConnect** | * | * | * | * | * | ICER | ICER$^{-}$ |
| **Demisto** | * | * | * | * | * | ICER | ICER |
| **ATAR Labs** | * | * | * | * | * | ICER | ICER$^{+}$ |
| **ServiceNow** | * | * | * | * | * | ICER | ICER |

Legend:
* = Yes; - = No
$^{+}$ Via external integrations with Micro Focus ArcSight and Interset.
$^{-}$ Via integration with Exabeam's Security Intelligence Platform.

Splunk has implemented a Machine Learning Toolkit (MLTK) that uses the features of Python's Scikit-learn ML package in the back end [54,55]. The MLTK can be applied to security problems such as anomaly detection, user behavior analytics, events classification and clustering, and forecasting and prediction [56,57]. DFLabs IncMan leverages ML algorithms in the form of supervised active intelligence (SAI) and automated responder knowledge (ARK) to support dynamic interaction capabilities for the SOC analysts during all phases of the incident response workflow to quickly deal with existing and emerging threats [58,59]. The ML models are used to maximize the effectiveness and efficiency of security operations teams, or augment human analysts, and reduce the time from the onset of breach discovery to resolution and hence increase the return on investment for existing security technologies [60].

IBM Resilient is used for incident categorization, prioritization, and analyst assignment [16,61]. The ML models are trained with historical data, can predict the severity of new incidents, estimate time to resolve, and even find similar incidents that were closed previously. It accelerates incident response by dynamically classifying incident attributes' as attacks are unfolding. Demisto implements an AI-based cybersecurity

strategy, to deliver automated threat prevention and response for security teams [27,62]. The solution makes use of AI algorithms to support intelligent functions such as incident triage and to offer SOC analysts some suggestions for next steps. The solution helps analysts to collaborate on automated IR investigations, with action being auto documented for post-incident reporting. Additionally. ThreatConnect leverages AI/ML via integration with Exabeam's Security Intelligence Platform that uses behavioral modeling and machine learning for advanced analytics and automated incident response [63]. It supports intelligence-led patch management, phishing email triage, infected host containment, detection and alert enrichment in the SIEM, and intelligence report creation and sharing, etc [19,20,64]. The platform has a Collective Analytics Layer (CAL) that deploys statistical models for analytics to score indicators, provide insights across datasets, and improve the ability to recommend actions.

Rapid7 SOAR platform is called InsightConnect and complements their SIEM platform called InsightIDR [65,66]. InsightConnect's security orchestration and automation help SOC analysts optimize operations through a library of about 300 plug-ins and a visual workflow builder. InsightIDR provides centralized log management, threat detection rules and correlations, user behavior analytics, machine learning, compliance dashboards, attacker behavior analytics, and integrates easily into existing workflows. Specifically, the platform combines machine learning and ongoing human input to detect attacks as early as possible and provide critical context about both the user and adversary in order to accelerate incident response [66]. The ServiceNow platform ingests events, logs and metrics to deliver a comprehensive solution with AI/ML-based correlation, anomaly detection and predictive intelligence [67,68]. This SOAR platform applies machine learning and advanced analytics to correlate events, adapting automatically to rapidly evolving virtualized and cloud environments. It uses AI/ML to automatically model normal behavior for performance metrics and detect anomalies for new metrics that fall outside predicted thresholds, and this helps detect, diagnose, and mitigate anomalous events quickly and accurately, significantly reducing MTTD, and MTTR.

ATAR platform provides comprehensive automation and tight SIEM integrations with the capabilities to monitor KPIs via customizable dashboards [15,41]. ATAR has been integrated with Micro Focus ArcSight and Interset User and Entity Behavioral Analytics (UEBA) to create a fast-acting environment against threats with top-of-the-line capabilities distributed across an enterprise at your fingertips [69]. Using machine learning, the Interset platform detects unusual behaviors that signal an attempt at data exfiltration, and then informs the ATAR platform, which then connects suspicious endpoints to collect evidence, lock the user accounts, and isolate them from the network automatically [69,70]. D3 Security's SOAR platform is designed to respond to adversarial intent with automated kill chain playbooks based on the MITRE ATT&CK framework involving other tactics, techniques, and procedures (TTP) [15,41]. The D3 solution integrates with other tools, which are critical to the SOAR platform to centralize security operations, ensure efficient and repeatable workflows, and leverage the power of automation and orchestration in a SOC environment. SOC team puts security alerts via D3's MITRE ATT&CK correlations, which identify related events to predict adversaries' next steps [71].

## 5 AI/ML Research in SOAR

Research efforts on SOAR in the past few years have established the most important AI intelligence capabilities in the design and implementation of SOAR, and SOAPA. Specifically, AI/ML plays a unique role in cybersecurity analytics, threat intelligence, and automated detection and incident response processes. We reviewed research efforts on SOAR undertaken by some security researchers, and in this section, we discuss our findings. Our review was conducted by reviewing research papers that we could find after searching most common publication venues for security researchers in journal and conferences under ACM Digital Library, IEEE, Xplore, Scopus, Journal of Computer Security, ACM SIGSAC,

Conference on Computer and Communications Security, USENIX Security Symposium, and research from a leading research and advisory organizations such as Gartner. We found research efforts that focused on different aspects of security orchestration and automation such as SOC analysis processes, events classification and prioritization, ontologies, etc.

Gupta et al. [72] discuss a deep learning approach for the automation for incidents classification and prioritization to assist SOC security analysts manage the huge volume and velocity of security events. Oprea et al. [73] developed a system called Malicious Activity Detection in Enterprises (MADE) that uses supervised ML to prioritize enterprise malicious communications to empower SOC analysts. The system uses supervised ML learning based on a large set of features extracted from web proxy logs to proactively detect network connections resulting from malware communications [73]. MADE has been used in operational settings in a large enterprise achieving 97% precision in the set of 100 detected domains of highest risk, with low false positive rates. Specifically, MADE was able to detect well-known malicious domains and entirely new malicious domains, significantly empowering SOC analysts.

Amthor et al. [74] describe techniques for automating cyber threat detection and response by integrating threat intelligence sharing platforms (TISP) and security-policy-controlled system (SPCS). A SPCS is a security system that uses security policies to automatically enforce a set of rules that control and restrict access to resources. They argue that fast and fully automated responses to cyber threats can be achieved by integrating threat intelligence sharing platforms for sensing and disseminating threat intelligence, as well as employing SPCS policy enforcement. In another research study, Teeraratchakarn et al. [75] discuss a honeypot-based system for collecting, analyzing, and classifying cyberattack patterns that can be deployed to improve organization's security policies and proactive security operations. Their system performs log management and analytics using Elastic Stack.

Liao et al. [76] have developed a tool for automatic extraction and retrieval of CTI from blogs, forums, tweets, and other online sources using Natural Language Processing (NLP) techniques. Their system generates an IOC file based on OpenIOC's schema for Indicators of Compromise (IOC). The IOC file mainly contains intelligence on forensic artifacts such as virus signatures, IPs/domains of botnets, MD5 hashes of attack files, etc. The work of Ghazi et al. [77] takes this effort step further by using NLP and supervised ML approach for automatically extracting high-level threat information such as attack patterns and techniques from unstructured texts from reputable security blogs. According to Ghazi et al. [77], the annotation tool can be used as an open portal for users to load threat intelligence documents. The system would the do a real-time document scan and then return "appropriate tagged information in a structured format, reducing manual labor and allowing cyber security professionals to optimally configure security tools and ultimately provide optimal defense". Alauthman et al. [78] used machine learning and reinforcement techniques and traffic reduction methods to address botnet detection problems. In the same vein, Lopez-Martin et al. [79] have presented an application of several deep reinforcement learning (DRL) algorithms to intrusion detection using a labeled dataset.

Adoption of cybersecurity ontologies can be useful in specific cybersecurity areas by categorizing identified causes and effects relationships among various entities. The concepts of cybersecurity ontology have been proposed mostly to formalize several concepts in the cybersecurity domain in areas such as malware analysis [80,81], intrusion detection systems [82,83], threat intelligence [84–88], vulnerabilities [89], and security incident classification [90]. Chauhan et al. [91] have developed a set of ontologies to enable tool-as-service (TSPACE) for a cloud-based platform. In TSPACE, ontologies are used to select, and provision a tool based on stakeholder requirements, and then semantically integrate the artifacts of the tools. Islam et al. [92] have developed an ontology-driven approach for security orchestration platform to automate the process of integration of security systems, and they have demonstrated the feasibility of their approach by using it to automate the execution of an incident response process for a

DDoS attack with three different security systems: Splunk, Snort and Limacharlie. Onwubiko has developed an ontology for SOC analysis process called CoCoa [93]. According to Onwubiko, CoCoa captures a SOC analysis process and provides a repeatable and consistent framework that can be reused to rollout a SOC function in an organization. The work of Syed et al. [94] is an effort to create a unified cybersecurity ontology termed Unified Cybersecurity Ontology (UCO). A cybersecurity ontology can enable interpretability and interoperability among security tools developed by different vendors and can ease automation as well as incident response processes. In the context of SOAR, such an ontology can create a standardized approach for SOC process workflows that are codified through a Playbook or a Runbook.

As noted by Gupta et al. [72], research work on security orchestration, automation and response is still at a nascent stage. While we have noted some efforts on security automation, it appears that there is still a lot of work to be done in the area of orchestration and incident response and management automation including reporting. There are a limited number of papers published on improving SOC effectiveness and efficiency via workflow orchestration and automation using AI/ML.

## 6 Future Research Directions in AI/ML Powered SOAR

Some researchers have focused on leveraging deep learning to automate security incidents classification and prioritization to ease the burden on SOC security analysts who have to manage huge volumes and velocity of security events. Other researchers have developed AI/ML approaches for automating cyber threat detection and response by integrating CTI gathered from different sources such as from blogs, forums, tweets, and other online sources. Some researchers provided atomic CTI [76] (virus signatures, IPs/domains of botnets, MD5 hashes of attack files, etc.), while some harnessed high-level CTI such as attack patterns and techniques [77] for integration into threat detection and response processes. Although these are significant endeavors for empowering SOAR with AI/ML, work on security orchestration, automation and response is still at a nascent stage because end-to-end applications of AI/ML to security orchestration, automation, and response are yet to be developed.

Artificial neural networks (ANN) can be trained to ANN discover hidden CTI patterns in data without the involvement of specific human knowledge to make predictions. However, the rules to detect, prevent, remediate, recover, or respond to security incidents is still, to a large extent, manually determined by SOC analysts and may involve unrealistic settings in modeling the dynamic cybersecurity environments; and in most cases it relies heavily on the logic imposed by the SOC analysts. To achieve full AI/ML empowerment of SOAR, reinforcement learning (RL) models can be leveraged for security orchestration, automation and response. RL can model autonomous software agents that make observations and take sequential actions optimally without or with limited prior knowledge of the operational environments and are therefore particularly adaptable for deployment in real-time and dynamic cybersecurity environments [95]. These RL agents receive rewards for their actions, and their objective is to learn to act in ways that maximize their expected rewards over time. In particular, deep reinforcement learning (DRL) is widely acknowledged due to its superior performance and has been applied to solve complex and challenging problems in different domains [95–99]. There are a number of state-of-the-art DRL algorithms that should be explored for SOAR such as policy gradients (PG), deep Q-networks (DQNs), Double DQN, Dueling DQN, Actor-Critic, Asynchronous Advantage Actor-Critic (A3C), Advantage Actor-Critic (A2C), Soft Actor-Critic (SAC), deep deterministic policy gradient (DDPG), and proximal policy optimization (PPO) [100].

Nguyen and Reddi have provided an excellent survey of DRL in Cybersecurity grouped into three major categories: DRL-based security solutions for cyber-physical systems, autonomous intrusion detection systems, and multi-agent DRL-based game theory for cyber security [97]. The survey found two emerging areas in the applications of DRL in Cybersecurity; security solutions for cyber-physical

systems, and the use of game theory models involving multiple DRL agents to deal with attacks in adversarial environments. They have identified a number of areas for the potential applications of DRL in Cybersecurity, for example, exploiting the capabilities of DRL to solve complex and sophisticated intrusion detection problems, and the investigation of model based DRL for cybersecurity. They have stated that "current literature on applications of DRL to cybersecurity often limits at discretizing the action space, which restricts the full capability of the DRL solutions to real-world problems." [97]. As they also have noted, there is a need to investigate methods that can deal with the continuous action space in dynamic cybersecurity environments, which speaks to the need for security orchestration, automation and response. We think that DRL systems using multiple agents that communicate, cooperate and coordinate should be investigated as an approach for AI/ML enabled SOAR systems for an effective and efficient large-scale defense solution in dynamic cybersecurity environments.

We have noted some significant efforts to develop cybersecurity ontologies to enable interpretability and interoperability among security tools developed by different vendors such as CoCoa by Onwubiko [93], onSOAP by Islam et al. [92], and Unified Cybersecurity Ontology (UCO) by Syed at al. [94]. More research work is needed to investigate the integration of ontologies into security orchestration, automation, and response processes in AI/ML powered systems.

## 7 Conclusion

There is an urgent need to prop up cyber defense operations with advanced orchestration and automation capabilities for effective and efficient cyber defense operations in today's advanced and dynamic cyber threat landscape. SIEM platforms, and other security appliances such as unified threat management (UTM), intrusion detection and preventing system (IPS/IDS), and data loss prevention (DLP); have played a key role in cyber defense operations for several years but they have a number of limitations despite the fact that they have matured over the last decade or so. However, with ever evolving and complex cyber threats, SIEM only environments which operate on the HITL model, place heavy workloads and fatigue on SOC analysts and hence the need to empower them with intelligent and automated systems that operate on the HOTL model. SOAR systems are designed to empower SOC analysts in order to reduce the MTTD, MTTR, TTQ, and TTI that are critical metrics for cyber threat detection, mitigation, and prevention efforts. This should also increase the ROI for SOAR systems. The next big step for cyber threat detection, mitigation, and prevention efforts is to leverage AI/ML in SOAR platforms. AI/ML will act as a force multiplier empowering SOC analysts even further. As borne out by the survey, some SOAR vendors have started to leverage AI/ML in their SOAR platforms but there is still a lot more work to be done.

As Gupta et al. [72] noted, research work on security orchestration, automation and response systems that leverage AI/ML is still at a nascent stage, and we found no evidence of security orchestration, automation and response support all stages of the SANS PICERL incident response framework [5]. The efforts by Gupta et al. [72], Oprea et al. [73], Amthor et al. [74], Teeraratchakarn et al. [75], Liao et al. [76], Ghazi et al. [77], Alauthman et al. [78], and Lopez-Martin and Sanchez-Esguevillas [79]; endeavor to leverage AI/ML in different phases of security orchestration, automation and response processes. End-to-end implementations of AI/ML to security orchestration, automation, and response are yet to be developed.

Furthermore, deep reinforcement learning (DRL) has some state-of-the-art DRL algorithms that should be explored for SOAR empowerment. Nguyen et al. [97] have identified a number of areas for the potential applications of DRL in Cybersecurity such as exploiting the capabilities of DRL to solve complex and sophisticated intrusion detection problems, and the investigation of model based DRL for cybersecurity. DRL systems using multiple intelligent agents that communicate, cooperate, and coordinate should be investigated as an approach for AI/ML powered SOAR systems for an effective and efficient large-scale defense solutions in dynamic cybersecurity environments. In addition, research work is required to

develop ontologies such as the ones by Islam et al. [92], Onwubiko [93], and Syed et al. [94] for integration into AI/ML powered SOAR systems to enable interpretability and interoperability among security tools developed by different solution providers.

**Acknowledgement:** The authors declare that there are no other contributors to the present study and therefore no acknowledgements to be made.

**Funding Statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] C. Islam, M. A. Babar and S. Nepal, "A multi-vocal review of security orchestration," *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–45, 2019.

[2] S. Morgan, "Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021," 2019. [Online]. Available: https://cybersecurityventures.com/jobs/.

[3] Cyberseek, "Hack the gap: Close the cybersecurity talent gap with interactive tools and data," 2020. [Online]. Available: https://www.cyberseek.org/index.html.

[4] NIST, "Cybersecurity workforce demand," 2020. [Online]. Available: https://www.nist.gov/system/files/documents/2017/10/26/nice_workforce_demand_pdf.pdf.

[5] SANS, "Incident response steps and frameworks for SANS and NIST," 2020. [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide.

[6] J. Moran, "DFLabs: Security orchestration, automation and response (SOAR) technology," 2018. [Online]. Available: https://www.dflabs.com/.

[7] Gartner, "Market guide for security orchestration, automation and response solutions," 2019. [Online]. Available: https://www.gartner.com/en/documents/3942064/market-guide-for-security-orchestration-automation-and-r.

[8] J. Oltsik, "Enterprise plans for security automation and orchestration," 2018. [Online]. Available: https://www.esg-global.com/blog/enterprise-plans-for-security-automation-and-orchestration.

[9] Capegemini Research Institute, "Reinventing cybersecurity with artificial intelligence, the new frontier in digital security," 2019. [Online]. Available: https://www.capgemini.com/.

[10] V. Hedge, "Obfuscated command line detection using machine learning," 2018. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/11/obfuscated-command-line-detection-using-machine-learning.html.

[11] R. Trifonov, O. Nakov and V. Mladenov, "Artificial intelligence in cyber threats intelligence," in *Proc. ICONIC: 6th & 7th Dec 2018*, Holiday Inn, Plaine Magnien, Mauritius, 2018.

[12] M. Berninger and A. Sopan, "Reverse engineering the analyst: building machine learning models for the soc," 2018. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/06/build-machine-learning-models-for-the-soc.html.

[13] D. Krisiloff, "Churning out machine learning models: Handling changes in model predictions," 2019. [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/04/churning-out-machine-learning-models-handling-changes-in-model-predictions.html.

[14] P. A. Rao, B. Navaneesh Kumar, S. Cadabam and T. Praveena, "Distributed deep reinforcement learning using tensorflow," in *2017 Int. Conf. on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC): IEEE*. Mysore, India, 171–174, 2018.

[15] Gartner, "Cybersecurity scenario 2025: Outrageous intelligence," 2017. [Online]. Available: https://www.gartner.com.

[16] B. J. Oltsik, "SOAPA: Unifying SIEM and SOAR with IBM security QRadar and IBM security resilient," 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/resilient/unifying-siem-and-soar-with-soapa/.

[17] J. Oltsik, "SOAPA vs. SOAR: How these security terms differ," 2019. [Online]. Available: https://www.csoonline.com.

[18] B. Laliberte, "The importance of a common distributed data services layer," 2019. [Online]. Available: https://www.esg-global.com/research/esg-brief-the-importance-of-a-common-distributed-data-services-layer.

[19] T. Palmer, A. Arcilla and D. Amato, "ESG validation - threatconnect security operations and analytics platform," 2019. [Online]. Available: https://threatconnect.com/wp-content/uploads/ESG-Lab-Validation-ThreatConnect-Platform-Jan-2019.pdf.

[20] ThreatConnect, "Increase the accuracy and efficiency of your security team with an intel-driven SOAR platform," 2019. [Online]. Available: https://threatconnect.com/solution/soar-platform/.

[21] J. Oltsik, "Goodbye SIEM, hello SOAPA," 2019. [Online]. Available: https://www.csoonline.com/article/3145408/goodbye-siem-hello-soapa.html.

[22] J. Oltsik, "Devo: A modern security operations and analytics platform," 2019. [Online]. Available: https://www.devo.com/soapa/.

[23] T. Sadamatsu, Y. Yoneyama and K. Yajima, "Practice within fujitsu of security operations center: Operation and security dashboard," *Fujitsu Science Technical Journal*, vol. 52, no. 3, pp. 52–58, 2016.

[24] J. Trull, "Top 5 best practices to automate security operations," 2017. [Online]. Available: https://cloudblogs.microsoft.com/microsoftsecure/2017/08/03/top-5-best-practices-to-automate-security-operations/.

[25] ThreatConnect, "Security automation and orchestration," 2020. [Online]. Available: https://www.threatconnect.com/security-automation-orchestration/.

[26] J. Blankership, S. Balaouras, B. Barringham and R. Birrell, "Breakout vendors: Security automation and orchestration (SAO)," 2017. [Online]. Available: https://www.forrester.com/report/Breakout+Vendors+Security+Automation+And+Orchestration+SAO/-/E-RES136903.

[27] A. Iyer, "*Security orchestration for dummies*," Demisto Special Edition. Hoboken, NJ, USA: John Wiley & Sons, Inc, 2019.

[28] M. Solomon, "The art of making threat intelligence actionable," 2017. [Online]. Available: https://www.securityweek.com/art-making-threat-intelligence-actionable.

[29] R. Montesino and S. Fenz, "Automation possibilities in information security management," in *Proc. of the European Intelligence and Security Informatics Conf. (EISIC)*, Athens, Greece, pp. 259–262, 2011.

[30] N. F. Saraiva de Sousa, D. A. L. Perez, R. V. Rosa, M. A. S. Santos and C. E. Rothenberg, "Network service orchestration: A survey," *Computer Communications*, vol. 142-143, no. 1, pp. 69–94, 2019.

[31] S. Ahmad and D. H. Kim, "A multi-device multi-tasks management and orchestration architecture for the design of enterprise IoT applications," *Future Generation Computer Systems*, vol. 106, pp. 482–500, 2020.

[32] W. Wang, X. Qiu, L. Sun and R. Zhao, "A data driven orchestration framework in software defined security," in *Proc. of 2016 5th International Conf. on Network Infrastructure and Digital Content, IEEE IC-NIDC*, Beijing, China, pp. 34–39, 2017.

[33] T. AlSadhan and J. S. Park, "Security automation for information security continuous monitoring: Research framework," in *Proc. IEEE World Congress on Services, SERVICES*, pp. 130–131, 2016.

[34] R. Brewer, "Could SOAR save skills-short SOCs?," *Computer Fraud & Security*, vol. 2019, no. 10, pp. 8–11, 2019.

[35] P. Shoard, "Hype cycle for security operations," 2020. [Online]. Available: https://www.gartner.com.

[36] L. Orans, J. D'Hoinne and J. Chessman, "Market guide for network detection and response," 2020. [Online]. Available: https://www.gartner.com.

[37] C. Neiva, C. Lawson, T. Bussa and G. Sadowski, "Innovation insight for security orchestration, automation and response," 2017. [Online]. Available: https://www.gartner.com/en/documents/3834578/innovation-insight-for-security-orchestration-automation.

[38] D. Cearley, N. Jones, D. Smith, B. Burke, A. Chandrasekaran *et al.,* "Top 10 strategic technology trends for 2020," *AI Security, Gartner Research*, ID G00432920, pp. 1–54, 2020.

[39] HEXADITE, "What is security automation? A guide for an evolving landscape," 2020. [Online]. Available: http://Hexadite.com.

[40] Demisto, "Security automation and orchestration - the human perspective," 2019. [Online]. Available: https://www.paloaltonetworks.com/resources/whitepapers/security-automation-and-orchestration.

[41] C. Neiva, C. Lawson, T. Bussa and G. Sadowski, "Market guide for security orchestration, automation and response solutions," Gartner Inc. (ID G00389446), 2019. [Online]. Available: https://www.gartner.com.

[42] EM360 Tech., "Top 10 SOAR solutions for 2019," 2019. [Online]. Available: https://www.em360tech.com/continuity/tech-features-featuredtech-news/top-10-soar-platforms.

[43] Cortex XSOAR, "Top security orchestration use cases, palo alto networks," 2020. [Online]. Available: https://start.paloaltonetworks.com.

[44] Solutions Review, "The five SOAR vendors to watch in 2020," 2020. [Online]. Available: https://solutionsreview.com/security-information-event-management/top-5-soar-vendors-to-watch-in-2020-by-solutions-review/.

[45] Cortex XSOAR, "Your-guide-to-security-orchestration, Palo Alto Networks," 2020. [Online]. Available: https://start.paloaltonetworks.com.

[46] NIST, "NIST SP 800-61, revision 2, Computer security incident handling guide," 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[47] SANS, "SANS incident handler's handbook," 2011. [Online]. Available: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

[48] DFLabs, "The difference between playbooks and runbooks in incident response," 2019. [Online]. Available: https://www.dflabs.com/resources/blog/the-difference-between-playbooks-and-runbooks-in-incident-response/.

[49] FireEye, "Helix security platform," 2020. [Online]. Available: https://www.fireeye.com/solutions/helix.html.

[50] FireEye, "Security orchestrator: simplify threat response through integration and automation," 2020. [Online]. Available: https://www.fireeye.com/solutions/security-orchestrator.html.

[51] V. Fang, "Malicious powershell detection via machine learning," 2018. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/07/malicious-powershell-detection-via-machine-learning.html.

[52] FireEye, "Security orchestration: best practices for any organization," 2017. [Online]. Available: https://www.fireeye.com/solutions/security-orchestrator/wp-best-practices-in-orchestration.html.

[53] J. John, "MalwareGuard: Fireeye's machine learning model to detect and prevent malware," 2018. [Online]. Available: https://www.fireeye.com/blog/products-and-services/2018/07/malwareguard-fireeye-machine-learning-model-to-detect-and-prevent-malware.html.

[54] Splunk, "Splunk enterprise security," 2020. [Online]. Available: https://docs.splunk.com/Documentation/ES.

[55] Scikit-learn, "Scikit-learn machine learning in python," 2020. [Online]. Available: https://scikit-learn.org/stable.

[56] Splunk, "User guide," 2020. [Online]. Available: https://docs.splunk.com/Documentation/MLApp/5.1.0/User/Algorithms.

[57] Splunk, "Splunk enterprise security," 2020. [Online]. Available: https://www.splunk.com/en_us/software/enterprise-security.html.

[58] J. Morgan, "DFLabs IncMan SOAR: For incident and forensics management," 2018. [Online]. Available: https://www.dflabs.com/wp-content/uploads/2018/08/DFLabs_White_Paper_IncMan_SOAR_For_Incident_and_Forensics_Management.pdf.

[59] DFLabs, "How to use IncMan SOAR to manage the OT-IT convergence and improve cyber security operations," 2020. [Online]. Available: https://www.dflabs.com/resources/white-papers.

[60] DFLabs, "Gartner market guide for SOAR solutions: Techno-Darwinism and the next evolution of SOAR," 2019. [Online]. Available: https://www.dflabs.com/download/2151.

[61] D. Monahan, "How using security orchestration, automation, and response tools makes life easier… and more difficult," 2019. [Online]. Available: https://www.ibm.com https://www.enterprisemanagement.com/research/asset.php/3823/How-Using-Security-Orchestration,-Automation,-and-Response-Tools-Makes-Life-Easier.and-More-Difficult.

[62] Palo Alto Networks, "Completes acquisition of Demisto, Palo Alto Networks," 2019. [Online]. Available: https://www.paloaltonetworks.com.

[63] Exabeam, "Combating cyber attacks with SOAR," 2020. [Online]. Available: https://www.exabeam.com.

[64] ThreatConnect, "SOAR: An incident responder's best friend," 2020. [Online]. Available: https://threatconnect.com.

[65] Rapid7, "Rapid7 attacker behavior analytics brings together machine learning and human security expertise," 2018. [Online]. Available: https://www.rapid7.com/about/press-releases/attacker-behavior-analytics-brings-together-machine-learning-and-human-security-expertise.

[66] Rapid 7, "Catching modern threats: InsightIDR detection methodologies," 2020. [Online]. Available: https://www.rapid7.com/resources.

[67] ServiceNow, "ServiceNow security operations," 2018. [Online]. Available: https://www.servicenow.com/products/predictive-intelligence.html.

[68] ServiceNow, "A new finish line for ai in organizations," 2020. [Online]. Available: https://workflow.servicenow.com/it-transformation/a-new-finish-line-for-ai-in-organizations.

[69] ATARLabs, "Integrated defense with ATAR, ArcSight and Interset," 2020. [Online]. Available: https://www.atarlabs.io.

[70] ATARLabs, "The business case for ATAR," 2018. [Online]. Available: https://www.atarlabs.io.

[71] Security, "Does D3 Integrate with my security tools? (Fortinet, McAfee, Symantec, CrowdStrike, Splunk, and more)," 2020. [Online]. Available: https://d3security.com/blog/does-d3-integrate-with-my-security-tools.

[72] N. Gupta, I. Traore and P. M. Quinan, "Automated event prioritization for security operation center using deep learning," in *2019 IEEE Int. Conf. on Big Data, 2019*, Los Angeles, CA, USA, 2019.

[73] A. Oprea and Z. Li, "MADE: Security analytics for enterprise threat detection," in *2018 Annual Computer Security Applications Conf. (ACSAC '18)*, New York, NY, USA, pp. 1–13, 2018.

[74] P. Amthor, D. Fischer, W. E. Kühnhauser and D. Stelzer, "Automated cyber threat sensing and responding: Integrating threat intelligence into security-policy-controlled systems," in *Proc. of the 14th Int. Conf. on Availability, Reliability and Security (ARES 2019) (ARES '19)*, Canterbury, United Kingdom, 2019.

[75] V. Teeraratchakarn and Y. Limpiyakorn, "Automated monitoring and behavior analysis for proactive security operations," in *Proc. of the 2020 2nd Int. Conf. on Management Science and Industrial Engineering (MSIE 2020)*, Osaka, Japan, pp. 105–109, 2020.

[76] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing *et al.,* "Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence," in *Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security*, New York, NY, USA, pp. 755–766, 2016.

[77] Y. Ghazi, Z. Anwar, R. Mumtaz, S. Saleem and A. Tahir, "A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources," in *Proc. 2018 Int. Conf. on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan, pp. 129–134, 2018.

[78] M. Alauthman, N. Aslam, M. Al-kasassbeh, S. Khan, A. Al-Qerem *et al.,* "An efficient reinforcement learning-based botnet detection approach," *Journal of Network and Computer Applications*, vol. 150, no. 11, pp. 102–479, 2020.

[79] M. Lopez-Martin, B. Carro and A. Sanchez-Esguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," *Expert Systems with Applications*, vol. 141, no. 6, pp. 112963, 2020.

[80] D. A. Mundie and D. M. Mclntire, "The MAL: A malware analysis lexicon," *Technical Note: CMU/SEI-2013-TN-010, CERT Program, SEI*, 2013 [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_40250.pdf.

[81] I. Kirillov, D. Beck, P. Chase and R. Martin, "MAEC – malware attribute enumeration and characterization," 2020. [Online]. Available: https://maecproject.github.io.

[82] F. Abdoli and M. Kahani, "Ontology-based distributed intrusion detection system," in *Proc. 14th IEEE Int. CSI Computer Conf.*, Tehran, Iran, pp. 65–70, 2009.

[83] T. Kenaza and M. Aiash, "Toward an efficient ontology-based event correlation in SIEM," in *The 7th Int. Conf. on Ambient Systems, Networks and Technologies*, Madrid, Spain, 2016.

[84] MITRE, "Standardizing cyber threat intelligence information with the structured threat information eXpression (STIX)," 2013. [Online]. Available: https://oasis-open.github.io/cti-documentation.

[85] MITRE, "Trusted automated eXchange of indicator information," 2013. [Online]. Available: https://taxiiproject.github.io.

[86] CybOX, "Cyber observable eXpression," 2014. [Online]. Available: https://cyboxproject.github.io.

[87] A. Evesti and E. Ovaska, "Ontology-based security adaptation at runtime," in *Self-Adaptive and Self-Organizing Systems (SASO), 2010 4th IEEE Int. Conf. on*, Budapest, Hungary, pp. 204–212, 2010.

[88] A. Kim, J. Luo and M. Kang, "Security ontology for annotating resources," in *OTM Confederated Int. Conf. on the Move to Meaningful Internet Systems, Center for High Assurance Computer Systems*, Washington, DC, USA: Naval Research Laboratory, pp. 1483–1499, 2005.

[89] H. Booth and C. Turner, "Vulnerability description ontology (VDO), draft NISTIR 8138," 2016. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/nistir/8138/draft/documents/nistir_8138_draft.pdf.

[90] S. A. Elnagdy, M. Qiu and K. Gai, "Cyber incident classifications using ontology-based knowledge representation for cybersecurity insurance in financial industry," in *2016 IEEE 3rd Int. Conf. on Cyber Security and Cloud Computing*, Beijing, China, 2016.

[91] M. A. Chauhan, M. A. Babar and Q. Z. Sheng, "A reference architecture for provisioning of tools as a service: Meta-model, ontologies and design elements," *Future Generation Computer Systems*, vol. 69, pp. 41–65, 2017.

[92] C. Islam, M. A. Babar and S. Nepal, "An ontology-driven approach to automating the process of integrating security software systems," in *2019 IEEE/ACM Int. Conf. on Software and System Processes (ICSSP)*, Montreal, Canada, 2019.

[93] C. Onwubiko, "CoCoa: An ontology for cybersecurity operations centre analysis process," in *2018 Int. Conf. on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Glasgow, UK, pp. 11–12, 2018.

[94] Z. Syed, A. Padia, T. Finin, L. Mathews and A. Joshi, "UCO: A unified cybersecurity ontology," in *Proc. AAAI Workshop on Artificial Intelligence for Cyber Security*, Phoenix, Arizona, USA, pp. 1–8, 2016.

[95] M. H. Ling, K. L. A. Yau, J. Qadir, G. S. Poh and Q. Ni, "Application of reinforcement learning for security enhancement in cognitive radio networks," *Applied Soft Computing*, vol. 37, no. 4, pp. 809–829, 2015.

[96] V. Mnih, A. Badia, M. M. A. Graves, T. Lillicrap, T. Harley *et al.,* "Asynchronous methods for deep reinforcement learning," in *Proc. Int. conf. on machine learning*, New York, NY, USA, pp. 1928–1937, 2016.

[97] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," 2019. [Online]. Available: https://arxiv.org/pdf/1906.05799.pdf.

[98] T. Chen, J. Liu, Y. Xiang, W. Niu, E. Tong *et al.,* "Adversarial attack and defense in reinforcement learning-from AI security view," *Springer Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.

[99] Z. Liang, H. Chen, J. Zhu, K. Jiang and Y. Li, "Adversarial deep reinforcement learning in portfolio management," 2018. [Online]. Available: https://arxiv.org/pdf/1808.09940.pdf.

[100] P. Henderson, R. Islam, P. Bachman, J. Pineau, D. Precup *et al.,* "Deep reinforcement learning that matters," 2019. [Online]. Available: https://arxiv.org/pdf/1709.06560.pdf.