International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Opensoar

Vipul Sharma[1], Aditya Shinde[2]

[1,2]Apex Institute of Technology, Chandigarh University Mohali, India

Abstract

SOAR solutions are designed to integrate multiple security components, often from different vendors. A stack of compatible security tools enables companies to collect data about attacks and respond to them without human intervention. SOAR tool's primary target is to increase the effectiveness of security operations. SOAR tools' main mechanisms are security orchestration, automation, and response. To build and automate numerous security tools to function as Security orchestration, automation, and response (SOAR) that will help small and medium-sized organizations automate security processes, particularly incident response, by collecting threat data from multiple sources. It can also respond to low-level incidents without human intervention. The user experience is paramount. Both end users and administrators are best served by SOAR that enables maximum productivity.

Keywords: OPEN SOAR, Threat Intelligence, SOC, SEIM, Cortex, Hive, MISP.

I. INTRODUCTION

Security automation is the machine-based implementation of security initiatives capable of programmatically detecting, analyzing, and remediating cyber-attacks by recognizing potential threats, triaging and classifying alerts as they arise, and then responding to them in a timely manner. Security automation works efficiently for the security team, so they no longer need to go through any alerts manually. Automated security detects threats in the workplace. It can also triage potential vulnerabilities and risks step-by-step according to the process, guidelines and decision-making defined by security professionals to evaluate an incident and determine whether it is a serious problem. All of this can happen in a matter of seconds without staff intervention. Repetitive and time-consuming tasks are reduced for security analysts when their systems are automated, allowing them to focus on more value-added work. Security automation can also easily identify threats. According to an ESG study, IT departments ignore 74% of security incidents or alerts – even when security solutions are in place due to their volume. Not only can safety automation detect and solve these common problems, but it can also eradicate human error, including inexperience, fatigue and carelessness.

SOAR solutions are designed to integrate multiple security components, often from different vendors. A stack of compatible security tools enables companies to collect and respond to attack data without human intervention. The main objective of the SOAR tool is to increase the efficiency of security operations. The main mechanisms of SOAR tools are security orchestration, automation and response. Build and automate multiple security tools that will act as Security Orchestration, Automation and Response (SOAR) to help SMBs automate security processes, especially incident response, by gathering threat data from multiple sources. It can also respond to low-level incidents without human intervention. User experience is paramount. Both end users and administrators are best served by SOAR, which enable maximum productivity.

SOAR products are purpose-built tools that connect activities and perform specific automated actions with other security tools in response to defined threats. RPA tools represent a wider range of automation tools for automating a wide range of processes. HR and finance have seen a significant increase in the use of RPA tools, but cybersecurity teams can also take advantage of them. Custom software and code can automate any form of analysis and are often used when faced with a shortage or specific problem in an enterprise without out-of-the-box resources. All of the above methods communicate with the organization's tools, collect data, interpret and act automatically or advise a team member to take next steps. In this essay, the concept of security automation and its relevance to information technology will be expected.

II. LITERATURE REVIEW

The purpose of this review was to examine the state of current security threat detection system using for security incidents. The corporate environment is becoming increasingly complex. Organizations now have a wide variety of systems spread across on-premises data centres and cloud deployments. The rise of telecommuting further complicates this issue as employees work from personal and mobile devices. The cost of the existing system is too high and it is not available online as open source. Securing the modern enterprise environment requires security solutions that can defend across multiple platforms against a wide variety of attack vectors. In most cases, organizations have chosen to deploy separate security solutions for specific use cases. The problem with this approach is that security teams are overwhelmed by a flood of security alerts and struggle to effectively manage and monitor their complex cybersecurity architecture. Security orchestration helps solve this problem by streamlining and automating threat detection and response. Four of the most current and relevant elements to consider when implementing security automation are:

1. Implementation of policies. Although networks have become much more complex, manually managing the associated security policies has become nearly impossible. Participate in automated policy enforcement that refers to automated processes for all IT security management activities. Our research shows that several vendors offer tools to automate the implementation of network security policies that make it easier to meet national or regulatory protection requirements. Most companies also offer automated systems for administrative tasks such as onboarding/departure and user lifecycle control. Automating application provisioning, delivery, and security gives IT and teams more control over data, costs, and time. Tools that enable business are often referred to as security automation.

2. Prioritizing and monitoring alerts. Our research shows that many people see the role of automation through a lens of control and priority alerts. Management and prioritization of alerts was usually manual and highly repetitive. A Security Centre analyst group needed to collect alerts and review monitors daily to identify key data points. Today there are many ways to automate monitoring and prioritize alerts. For example, rules and thresholds may be developed, threat intelligence may be used, and advanced behavioural analytics and machine learning may be deployed.

3. Plan for incident response. Contingency planning is also known as health automation. One way to think about these new technologies is as smart ticketing systems that enable businesses to track and orchestrate the steps needed to respond to evolving safety events. Providers in this space help companies build strategies against different types of threats. This allows you to automate parts of your response when every second counts.

4. Analysis, intervention and improvement. According to our research, automating the investigation, actions and remediation of cyber threats requires the use of technology to achieve the performance of a competent cyber analyst. In a way, the other components of security automation (policy, prioritization, scheduling) work to quickly identify and shut down threats before they impact operations. There are many aspects of analysis, action and recovery that businesses can automate. For example, some of these components can only address one thing, while others can focus on specific functions, such as automatically containing compromised devices. Some companies use automation and artificial intelligence as cyber analysts to run the entire process end-to-end. All of these security technologies free up a lot of security resources to support security teams, allowing them to focus only on mundane but critical tasks and primarily on enterprise strategies that make the business more secure. Based on research, the implementation of security automation in information technology focuses on the quality of information system security checks. Automated CM practices include knowledge of the procedures your company may use. It includes techniques and technologies used to obtain and review security information on a more regular basis. Therefore, companies should ensure that the CM plan includes the set of actions and mechanisms used to respond effectively to the collected data. Automation may change the nature of safety tasks, but they will not be eliminated immediately. For some tasks, it is better to leave other tasks to citizens as additional resources.

The concept of SOAR

SOAR systems (Security Orchestration, Automation and Response) are a toolkit that allows you to automate the process of information about security threat data for later analysis. They solve the following tasks:

- Intelligent collection mode real-time information security data from several sources with the necessary enrichment and aggregation information coming from heterogeneous means of information protection;
- automation of typical chains incident-related tasks Information security and detection of deviations from Established security policies and requirements
- Application of security policies in means of information protection in both proactive and reactive modes;
- Automation of the entire list of organizational and technical tasks and information security procedures as part of the information security incident response and detection of deviations from established security policies, including informing, appointing responsible persons and organizing their joint work;
- Retrospective analysis of conditions, conditions, actions taken and response results on information security incidents to increase effectiveness of practices, training and further investigations; SOAR is relatively recent. There are three SOAR Feature Groups: Integration (integration), automation and orchestration1 (orchestration).

How Security automation enhances increase safety of technological systems

Intrusions of company data continue to expand at an alarming pace. So many warnings, so many tools and not enough resources are available to organizations. Security teams are frustrated, and conventional safeguards have become apparent that data can no longer be secure. To tackle this issue, numerous organizations are improving their automation information security strategies. The following can be achieved by security automation in information technology:

Increase safety engineer productivity

Reduce resolution mean time

Incorporate products necessary to protect against agile threats. In the last 4-5 years, safety automation has become a niche area. It focuses on Safety Operations Centres (SOCs) and accelerates analysts' ability to alert on outages and initiate remediation. Therefore, it becomes a critical component in safety and incident response. Automation and orchestration technologies help us deal with mundane problems. Collect and enrich alerts. But it's starting to evolve to increase threat intelligence so we can better infer the right decisions and best actions in specific scenarios. Use artificial intelligence and computer training to help analysts make better decisions from better information. A common analogy for deciding what to wear is checking the weather and choosing clothes based on weather forecasts.

Automation is not a new topic, but its importance is increasing day by day due to the continuous and focused attacks on organizations in every industry. According to the Cyber Security Jobs Report, 10 million unfilled cybersecurity jobs will remain until 2023. Today's threats require more than a qualified security professional. Hackers have turned to automation to increase their capabilities. We have to do the same to keep up with them. By choosing the right automation and coordination method and use cases, organizations can make better decisions from the best data, improve efficiency and increase overall safety.

Existing System

SOAR leverages a combination of technical capabilities and embedded processes to automate previously time-consuming, manual security management tasks. A SOAR platform provides centralized security operations by coordinating incident response tasks through bidirectional integration with various third-party security tools. For example, with SOAR solutions, security administrators have a single console to monitor and interpret data generated by a wide variety of platforms including SIEM, IDS/IPS, FW, EDR, UEBA, malware, sandbox analysis, and more, and can to answer.

Others.

SOAR'S design allows it to be modified based on the needs of existing security systems. This means that it can be used in current settings without requiring a time-consuming or resource-intensive system redesign. SOAR can collect data from a variety of sources including manual entry, machines and email.

From the literature review, it is observed that studies highlight the need for an efficient and scalable approach for detecting code having software vulnerability. The existing techniques are not able to detect all types of vulnerable code and bugs. Different approaches suffer from a high false negative rate and are not scalable to large software systems due to high time complexity and high cost not everyone able to use the SOAR because company charges much high cost to set up a SOAR in the company or in your system.

Proposed System

We proposed a system which is more impactful than the existing system. We create a open-source project which is available to everyone free of cost and fully automated. We automate the SOAR using shuffle automation which helps to automate the tasks.

The images of SEIM, Hive, Cortex, Missp are containerized in docker and fully automated using the scripts. Policies, and people to create a better flow of processes. Most practically, SOAR creates automated and quicker manual actions to save overworked and understaffed security teams valuable time to focus on the more severe incidents. In more technical terms, this is accomplished through integration of tools via API’s. For instance, by connecting an API to a Security Information and Event Management platform (SIEM), responders would be able to automatically perform data calls upon the SIEM’s database to pull

the latest security logs and artifact information. Thus, saving the incident handlers valuable time in searching and creating automated remediation tactics based on the pulled information. These remediation tactics could be as simple as a button that automatically generates an email to an individual phished, informing the victim that they should remove the phishing email; or a tactic as detailed as integrations into their firewall to completely shut off communication going to or from specific IP addresses and ranges.

The SOAR Security Orchestration

The first component of SOAR, security orchestration, involves the integration of internal and external tools via the use of application programming interfaces (APIs). This integration is usually done via built-in or custom integrations. The internal and external tools that are integrated into the system mostly pertain to:

- Firewalls
- Vulnerability scanners
- Endpoint protection products
- End-user behaviour analysis programs
- Intrusion detection and prevention systems
- External threat intelligence feeds

Security orchestration ensures data is constantly collected, ensuring better threat detection. The trade-off, however, is that the system has to parse through a lot of data.

Once orchestration consolidates the data and threats, it is then handed over to automation to begin the response process.

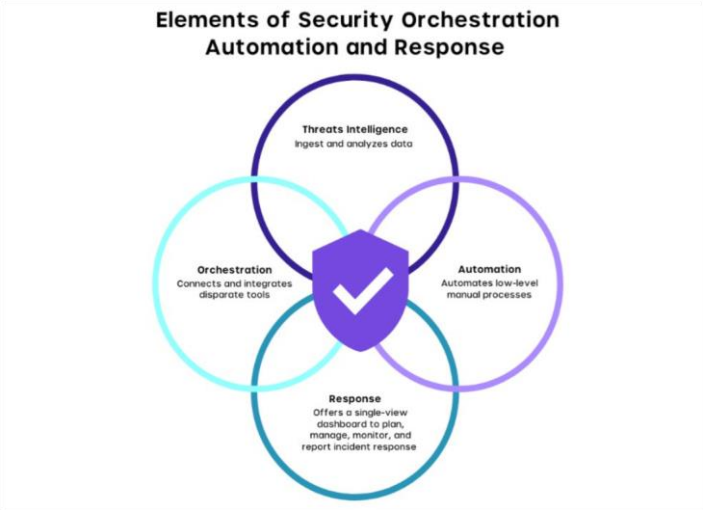
2. The SOAR Security Automation Based on data and alerts provided by orchestration, automation components initiate actions by analyzing data and creating automated processes to replace manual processes.

Manual processes replaced by security automation relate to vulnerability scanning, log analysis, ticket review, and auditing. These tasks were usually performed by analysts. All these tasks are standardized and automated by the SOAR system, reducing the manpower required. Automation can also leverage the power of artificial intelligence (AI) and machine learning to help decipher analyst insights, create unique recommendations, and automate future responses. As a useful alternative, automation can also increase threats in the presence of human intervention. Is necessary.

Playbooks are also used in SOAR security automation. Playbooks are essential to the success of any SOAR system.

Playbooks are pre-built or customized with predefined automated actions. Also, for greater productivity, multiple playbooks can be combined to complete more complex tasks and actions. If a suspicious or malicious URL is found in an employee's email, playbooks can be used to block the email and alert the involved employee to the possibility of phishing. For example, try to block an email sender's IP. SOAR tools can even go further and take advanced steps to mitigate risk.

You can scan all your employees' emails for similar malicious content and initiate investigative tasks such as blocking IP addresses of potential intruders.



3. The SOAR Security Response

The third component of SOAR, "Security Response," provides analysts with a unified view of monitoring, planning, managing, and reporting actions after a security threat is identified.

The Security Response component also provides post-incident activities such as case management, threat intelligence sharing, and reporting. A security threat has been detected.

The Security Response component also provides post-incident activities such as case management, threat intelligence sharing, and reporting.

III. DISCUSSION

Avoiding more and more sophisticated cyber-attacks is becoming increasingly difficult and decreasing. Thousands of alerts generated by various security tools are often inefficiently managed by security teams. Analysts must complete manual and repetitive work to analyse these potential risks. In addition to insufficient time and resources, many companies cannot keep up with secure workloads. The exponential increase in cyber-attacks has contributed to the emergence of security automation as an important issue for organizations and security teams. A technology that security analysts had to contend with, assess, and respond to every alert before automation finally became unattainable. A large number of threats required the identification of automated responses to respond more quickly in the event of a cyber-attack or security breach. Along with automated emergency management, a more proactive approach to solving safety concerns has become increasingly necessary. Safety automation was born from it, providing a systems-oriented approach to machines. In fact, it evolved into safety automation and orchestration, allowing security devices to be tied into workflows. Providers now sell SOAR solutions that automate responses and remediation. Security coordination solutions, automation and accountability. Providers use a variety of conflicting terms to describe their devices. Before you start looking for a vendor, figure out what features you want in your security automation platform.

A. Cybersecurity automation tools and platforms

Types of process automation and information security applications include:

1. Robotic Process Automation

1. Robotic process automation is usually defined as the process of automating routine tasks with the help of robots (physical or virtual application robots). In cybersecurity, this generally refers to the ability of automated systems to perform tasks such as testing, tracking, including low-level emergency response.

We simply collect and compile data, analysis and detection methods for simple violations and other limited cognitive tasks.

2. Response automation, security incident, event management, and security coordination - these apply to a variety of approaches that leverage the capabilities and productivity of the security operations center without tying human resources to low-level tasks. It enhances risk, vulnerability, and security incident management and simplifies three critical information security activities: protection structures, protection automation, and security response. SIEMs are mostly manual. This mobile solution system includes manual responses to alerts, regular updates and changes to systems, rule sets and signatures to automatically, efficiently and accurately identify them. However, the main purpose of this strategy is to identify known threats and identify new or unknown threats that are less successful. Using SOAR internally or externally is a little more complex, receiving specific SIEM alerts and automatically responding when triage and remediation are needed. It helps classify new threats using cognitive tools and methods used to learn from current threats through artificial intelligence (AI) and machine learning (ML). SOAR and SIEM are similar in some ways. However, both collect the same information from different sources and use it to search for anomalies.

3. Google's encryption command certificate management has created a number of dangerous vulnerabilities due to the widespread use of SSL certificates and keys. Lack of penetration into networks and public key infrastructures is one of the biggest challenges to security and business success. Certificate management systems and certificate discovery applications are useful for more than web certificates. Helps discover all X.509 digital certificates on your network regardless of brand, type, issue, date, or expiration date. This includes code signing certificates, client certificates, IoT, SSL/TLS, and device certificates. An obvious example is Sectigo Certificate Manager (SCM) or Comodo CA
Certificate Manager (CCM).

4. Development of custom automation solutions The idea of designing a custom automation system is another category that should not be neglected at least. We know that every business is different and organizations in different sectors have different needs. While some of the current techniques for cybersecurity automation are always effective, it can be beneficial for a particular company to develop solutions tailored to their business needs. It can be handled by an inhouse development team, but we recommend outsourcing it to a third-party provider.

B- The need for continuous security management

Security monitoring has historically been largely done according to strict procedures. The latest security patches should be installed on computers every three months, except in emergencies. In many organizations, computers are likely to be certified only every few years. However, this timeline is insufficient to meet today's security needs. New exploitable software vulnerabilities are discovered every day, thousands of which are publicly documented each year. every year. Given the number of fixes that must be implemented in a company, companies must also prioritize patching so that the most critical vulnerabilities are patched faster than others.

IV. CONCLUSION

How security automation is supported varies greatly by industry and company. Whether in retail, healthcare, manufacturing, financial services, the public sector or any other industry, resources and processes can be highly interdependent. For example, retailers deal with ransomware and phishing attacks in unpredictable ways. Automation is effective in clearing the deck of repeated attacks and false positives.

This allows security analysts to better investigate these issues and find long-term solutions. It's important to work with your IT team and other organizational leaders to identify issues that need to be addressed before considering a vendor. Automation is high on the list of priority areas because businesses know it removes risk, makes the network transparent, and increases the security stack. Reducing human error is one of the biggest threats. An engineer who is asked to do the same thing every day, finding a needle in a haystack, will eventually make a mistake. Many business security technologies and services are analyzed to understand automated controls, particularly those that enable the automation of central management operations. Managing information security is a very complex and ultimately costly problem. While small and medium-sized companies do not have the necessary financial resources to implement information management programs, large companies are facing increasing uncertainty in the IT industry. Security automation reduces the cost and complexity of secure operations without human intervention. Automation is not a joke or science joke. It is accepted for both small and medium businesses and large companies. Cyber security departments are focusing on more complex tasks by introducing automation within the enterprise framework. This means that machines can perform routine, repetitive tasks, allowing cybersecurity project managers to troubleshoot problems, improve organizational risk posture, and manually review systems and data to identify unwanted and repetitive tasks. Look for signs of compromise or failure.

V. REFERENCES

1. A.U. Haq and T. S. Khan, “Security in automation: Smartphone might be the greatest threat,” CFE Media, 2015.Retrieved from: https://www.controleng.com/articles/security-in-automationsmartphone might-be-the-greatest-threat/
2. E. Barak, “Explaining security automation and its evolving definitions, “New York, NY: IDG Communications, Inc,2016. Retrieved from: https://www.networkworld.com/article/3121275/explainingsecurity automation-and-its-evolving-definitions.html
3. K. Panos, “Security Automation and Threat Information Sharing Options,” IEEE Security & Privacy 12,2014,42-51. [4] M. Metheny, "Continuous monitoring through security automation, "ScienceDirect, 2017.Retrieved from: https://www.sciencedirect.com/topics/computerscience/security automation
4. P.Nguyen and A.Graham, “Enhancing Security with Automation and Orchestration, “Serious Edge,2015.Retrieved from: https://edge.siriuscom.com/security/enhancing-securitywith-automation and-orchestration R. Montesino and S. Fenz, "Automation Possibilities in Information Security Management," 2011 European Intelligence and Security Informatics Conference, Athens, 2011, pp. 259-262, DOI: 10.1109/EISIC.2011.39.
5. T. AlSadhan and J. S. Park, "Enhancing Risk-Based Decisions by Leveraging Cyber Security Automation," 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, 2016, pp. 164-167, DOI: 10.1109/EISIC.2016.042.
6. C. N. N. Hlyne, P. Zavarsky, and S. Butakov, "SCAP benchmark for Cisco router security configuration compliance," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 270-276, DOI:10.1109/ICITST.2015.7412104.
7. G. B. Peterside, P. Zavarsky, and S. Butakov, "Automated security configuration checklist for a cisco IPsec VPN router using SCAP 1.2," 2015 10th International Conference for Internet Technology and

Secured Transactions (ICITST), London,2015, pp.355-360, DOI:10.1109/ICITST.2015.7412120.

8. M. Brunner, C. Sillaber and R. Breu, "Towards Automation in Information Security Management Systems," 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS), Prague, 2017, pp. 160- 167, DOI: 10.1109/QRS.2017.26