International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Case Study for Cyber Security Automation

Shruti Anandrao Hanbar , Prof. Shambhu Rai

Bharati Vidyapeeth' Institute of Management & Information Technology, University of Mumbai, India

Abstract

Cyber Security automation has evolved as a hot topic for organisations and IT and security teams. It offers a way to drive efficiencies within security operations and help to free up analyst time that would otherwise be spent conducting repetitive tasks and to allocate it to higher value technical activities. The purpose of this research is to provide an overview of automation methods used in cyber security, and evaluate how automation can improve security. Deploying automation is challenging because of the lack of qualified professionals and the incompatibility of multi-vendor software and hardware.

Cybersecurity automation is one of the major developments in information technology. Automating
repeatable processes will increase focus on the more productive problem and solving tasks within organizations and individuals. Focusing on these issues will advance innovation and contribute to a powerful organization from a cyber-security point of view. As long as the information will be available, the
confidentiality, integrity, and availability of the cybersecurity programs will be protected.

Keywords

Security orchestration, automation and response (SOAR), security operations centre (SOC), Cyber security, Automation, Information technology.

Introduction

Cyber security threats have become advanced and the traditional predefine based security solutions have become quite ineffective. Advanced security solutions that take advantage of artificial intelligence (AI) and machine learning (ML) are required to automate information security management. A security breach can thus have destructive effects on a company's operations. To enhance the security of their information will benefit, organizations can get advantage of AI and ML technologies to automate their security management tasks and increase understanding into security threats. AI is concerned with information systems that automate complex and complicated tasks that are necessary for threat detection and mitigation. The systems is capable of analysing huge volumes of data and identifying patterns that they use to make decisions. Machine learning (ML) is a core component of AI that provides computer systems with a means to learn and adapt through its experience. The purpose is to examine and get benefited of AI-based information security solutions in reducing security risks and improving efficiency and addressing common cyber security threats.

Security automation consists of the machine-based implementation of security Solutions capable of programmatically detecting, analysing, and rectifying cyber-attacks by identifying potential threats, triaging, and classifying alerts as they occur and then acting on them on timely based. Security automation works incredible for the security team and so they don't have to go through any warning

anymore manually. Automated security detects threats in the workplace environments. It also can classify potential vulnerabilities and risks by step-by-step process, guidelines, and decision making defined by security professionals to evaluate the incident and find out if it is a serious problem. All this can be done in seconds without any staff action. Repetitive and time-consuming tasks is reduced for the security analysts when their systems are automated so that they can focus on greater value-adding work.

Literature Review

Humans are subjected to making errors and whereas machines are reliable and accurate as long as the logic inserted into them is working as accordingly. Human errors can lead to configuration errors and information leakage, failure to update patches for system on time, or overlooking an important alert in a security system. Cyber Security automation has evolved as an important topic for organisations as well as for IT and security teams, in large part to the continuously increase in the volume and velocity of cyber-attacks over recent years. Previously the automation capabilities, analysts were required to combination through and investigate and act on every alert.

Security automation has also evolved from automated incident response. Most relevant it also helps with security issues a more proactive approach was Finally needed. And from there came security process automation which provide a systematic, machine-based approach. This in turn has grown into security automation and orchestration and which enables connectivity between disparate security tools and workflows.

1. Asymmetry in attack and defence.

A malicious attacker only needs to find one weak point so that it can utilize to gain access to a system and whereas a defender needs to make sure all points are secure and no vulnerabilities exist from any side. Needless to say, it is an impossible task for defender. New vulnerabilities are found all the time, and once they are detected need to act rapidly to patch the vulnerability and release an update to a secure version, and users need to install the updates to avoid becoming a victim of attackers and misuse the vulnerability in their systems. Attackers can identify how security tools work and adapt their attacks to take advantage of that knowledge.

Cyber security has to gain a knowledge of changing threat landscape continuously. Adoption of new technologies like as 5G, IoT, and cloud systems also introduce new attack surfaces which generates new threats continuously. Advances in technology also required more advanced and Advanced tactics, techniques, and procedures used in attacks.

Due to these facts, SOCs (Security Operations centre) and security tools have to evolve to keep up with the threats organizations are facing, and automating security is a high priority operation to keep up with the increasing requirements in security system. The goal of cyber security automation is not to replace human analysts but to increase entitle of SOCs with better capabilities to monitor, identify, and respond to threats immediately.

2. Staff shortage

The important factor for expanding cyber security automation actually facing shortage of skilled security professionals. The definition of workforce shortage is the number of qualified workers needed to fulfil the needs of the industry, which is not directly means the number of open job positions.

Now a days there is a high demand for cyber security professionals but the required skillset for security positions is increasing continuously. Security analysts can able to work in high-pressure situations to quickly analyse the threats and respond to security incidents. Stressful working conditions can increase the burnout and employee churning. Automation can increase to higher productivity and it can reduce the stress

experienced at work which will lead to less burnout for employee.

Methodology

The case study methodology it allows for comparison of different aspects of AI based security systems and signature-based system(traditional). Security automation and its tools does excellent work for security bench and for security incident response.
Security automation is all about of simplifying and driving productivity within your security operations. Security orchestration connects all your different and varying security tools so that they feed into one another and also share information and respond to alerts, even when the data is spread across a large digital resource. The terms are often used correspondently but the two types of platforms actually serve different purposes and tasks. Security automation reduces the time taken to detect and respond to repetitive incidents and security alerts don't stay unaddressed. This frees the analysts from mundane tasks and allows them to allocate their time towards higher value technical activities.
Security orchestration, automation and response (SOAR) can face even the most repetitive of tasks. Any process that involves detection, investigation, containment that can be orchestrated across the many IT and security tools and automated without any human interaction.

Automation Platform and Tools

1. Robotic Process Automation (RPA)

Robot process automation defined as a process of automating routine tasks utilizing robots virtual like application bots. In cybersecurity it refers generally to the automated systems' ability like to conduct tasks like testing, tracking including low-level emergency response. It simply collecting and compile data, analysis, and detection methods for simple breaches and other cognitive tasks.

RPA tools are a larger set of automation tools that allow for the automation of a wide range of business processes like everything from HR to cyber security. This type of automation is based on symbolic software robots or bots. For Each and every robotic instance has its own virtual workstation.

2. SOAR platforms

Security Orchestration Automation and Response platforms (SOAR) take orchestration and automation one step ahead. It defined as technologies that allow an organization to collect inputs from different sources, and it include capabilities of vulnerability management and security operations automation and incident response. SOAR combines the human and machine power to make analyse and respond to security incidents threats. In traditional the tools were quite limited in scope and only allows minor time savings on select tasks for (security operations centre) SOCs. These platforms have only become more effective and productive with the ability to orchestrate and automate larger and more important operations with more security tools being integrated to SOAR platforms. Processes in SOAR platforms can be done using playbooks and runbooks. Playbooks and runbooks provide a standardized approach to incident response, allowing repeatable, fulfil, and effective incident response. They help with following management as like reporting procedures, automation, and orchestration. The difference between the two is that playbooks it offers more of a step-by-step approach for one type of incident and mean while runbooks have conditional steps depending on the type of incident. The both approaches allow us similar incidents are handled in a similar fashion which simplifies the tasks and it also helps new staff learn and handle tasks quickly in simpler manner.

3. Artificial Intelligence (AI) and Machine Learning (ML)

Automation is like act of programming a machine to perform a repetitious task without mortal intervention but higher usable in advanced situations of security task bear machines to perform dynamic tasks and also learn and analyse the data and this is when AI and ML come into the picture. AI and ML could come veritably important instruments in the field of cyber security and reducing mortal workload while also making systems more flexible to numerous pitfalls. The ML models are trained on advanced incidents and historical data so that they take into accordance when analysing new alerts, so patterns can be detected and predictions can be made based on the patterns and consequently action should be taken. There are numerous use cases of AI and ML in SOAR platforms.

4. Security Operations Centre

SOC is a team of security analysts, whose work is to detect, analyse, respond to, report on and prevent cyber security incidents. There are two types of SOCs firstly, an internal SOC that present within an organization and it is in charge of that organization's security operations and secondly outsourced SOC-as-a-service model which provide by managed security service providers (MSSP). Larger businesses often have internal SOCs workflow, and on other hand mid-size businesses go ahead with hybrid solutions or outsourcing their security operations with MSSPs. The SOC manages all the logged events in the network are monitored and it is responsible on taking action when it is needed. The goal of SOC is to understand the entire threat landscape of the organization and protect with on-premises IT infrastructure and third-party services such as cloud services. Essentially the SOC needs to stay on top of every possible threat and find out how to best protect against, mitigate, and prevent these threats in effective manner.

Case Studies

The case study for identifying how cyber security automation has overcome the problem and resolved.

1. SOAR + PHISHING IR

According to Siemplify, Phishing threats across organizations is becoming increasing challenging as attackers attacking from various side from network. Ransomware are also compromise business email and credential theft continue to be threats.
And Solution for this to, implemented security orchestration, automation, and response (SOAR) platform, and Network team is able to report phishing quickly and determines malicious versus benign. With the help of SOAR High confidence with actions taken to hunt and rectifying phishing threats across the organization become simpler. It also downloads suspicious phishing emails for additional analysis and automated action for future action. Playbook enrichment using phishing attributes to automate rectification.

2. Automate Security Workflows With SOAR

According to Forrester data most top three challenges security teams face is day-to-day Planned/tactical activities taking up too much time. Security operations teams facing struggle with constant alerts and manual investigations and a fainted pool of tools to respond from. SOAR technology provides security teams a way to automate some of these repetitive or mundane tasks. And solution for this and also as commence the goal of SOAR technology is to make security operations faster and less error-prone and more efficient. When they implemented a SOAR, they were expecting following:

1. Classify and merge alerts. Security teams use SOAR to automate alert classification and deduplicate alerts coming from a

variety of different toolsets such as SIEM and email security.

2. Customize enrichment. Security teams use SOAR to enhance detections with additional details such as bringing in threat intelligence and making a determination on the risk level of phishing email.

3. Orchestrate/Automate Response. Security teams use SOAR for automated response actions such as restricting user access or forcing an identity-based action (like a password reset)

Key Benefits of Security Automation: -

1. Faster Security incident response rate.
2. Improved investigation Accuracy.
3. Reduce risks rate to the business.
4. Cost and time savings.
5. Enables Faster Threat Detection.

Conclusion

AI- grounded cyber security results have unmatched performance when compared to signature grounded tools. The AI- grounded systems use artificial intelligence to descry significant diversions that are also identified to identify genuine pitfalls with minimal floods of false cons. The security systems are also able of monitoring, detecting and remediating pitfalls autonomously. The examination of AI- grounded security results shows that they work patented machine literacy technologies to improve their effectiveness. also, the results use an admixture of approaches including behavioural analysis and signature- grounded trouble discovery. While machine learning is used to train the systems and support automation, behavioural analysis is used to combat modern- day malware. Security tools grounded entirely on behavioural analysis are prone to a high number of false cons. This is why AI- grounded tools don't solely depend on the decreasingly imperfect conventional trouble discovery technologies. As advancements are made in computing, AI- grounded tools will come more effective at icing the security of associations without mortal backing.

A deficiency of security chops, combined with the evolving trouble landscape is driving the need for largely sophisticated automated tools. Security risks may no way be cancelled, but they can be minimised if organisations have the capacity to automatically analyse data from their entire digital ecosystem with the environment demanded to make this intelligence practicable. If ever there was a time for brigades to look at administering security process automation, this is it. The en masse relinquishment of multi-public pall is expanding the available attack face for vicious actors to operate on and COVID- 19 has shifted the home to come the new enterprise to secure. During times of profitable query analogous as these, security budgets will be scrutinised further than ever. It's therefore essential that process automation tools can stand up to quantifiable measures to prove their ROI.

References:

1. https://www.siemplify.co/wp-content/uploads/2022/03/Solutions-Brief-Siemplify-Cofense-1-2.pdf

2. https://reprints2.forrester.com/#/assets/2/682/RES177298/report

3. https://swimlane.com/blog/security-automation

4. https://threatconnect.com/what-is-a-soar/

5. https://storage.googleapis.com/stateless-www-cyberbit-com-liv/2021/11/Deloitte-Case-Stady.pdf

6. https://www.redhat.com/rhdc/managed-files/ma-idc-business-value-of-ansible-automation-analyst-material-f30958-202201-en.pdf

7. https://reciprocity.com/blog/the-benefits-of-security-automation/

8. https://www.cynet.com/incident-response/security-automation-tools-process-and-best-practices/