IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Security automation in Information technology

Sikender Mohsienuddin Mohammad, Surya Lakshmisri

[#]*Department of Information Technology & Wilmington University*
419 V ST, APT D, Sacramento, CA 95818

Abstract

Security automation has been a major issue for many companies in the fight against rising cyber threats enabled by new cloud network attacks and proliferating the Internet of Things. A recent survey by the threat detection and hunting company Fidelis Cybersecurity has revealed this trend among 300 CISOs, CIOs, CTOs, architects, engineers, and analysts studied in a range of industries. More than half of the professionals analyzed (57 percent) said that their companies are concerned with a lack of automation [21]. Cybersecurity automation is one of the developments in information technology. Automating human-driven, and repeatable processes will focus on the more productive problem - solving tasks within organizations and individuals. Focusing on these issues will foster innovation and contribute to a more robust organization from a cyber-security point of view. Automation also adds to the complexity of information systems in an organization and as malicious targets grow, cybersecurity initiatives must be prepared to implement automated cybersecurity solutions. As long as the information is available, the confidentiality, integrity, and availability of the cybersecurity programs must be safeguarded [2].

In most industrial industries, automation is the main force of transition. By 2030, the automation industry is expected to completely replace over 800 million workers and technology transforms our way of working and organizing and communicating with others. The almost constant occurrence of data breaches suggests that it does not stop so that organizations are unable to have long-term reservations regarding security automation concepts and capabilities. Security automation of IT security infrastructure is a priority and keeping information systems safe [9]. Automating policy enforcement, warning control, and prioritization and the preparation of incidences will increase the efficiency of businesses and reduce costs significantly. Through automating the analysis, response, and remediation of threats in its entirety, businesses can replicate the expertise and reasoning of seasoned cyber experts on an international basis, ensuring a greater overall degree of protection and compliance [7]. That is never the case today. For example, most organizations, due to the huge resources needed for performing audits, only audit a representative sample of their processes. For example, it is common practice in an organization to the only audit a few of them or even to audit the basic security configuration they all need to have if 50,000 laptop computers would be similarly configured. Given the audit tools required, these approaches are understandable.

Methodologies have been developed over the years to safeguard data but the complexity required to ensure security still hasn't been changed. Analysts need to manually address threats without security automation. This often involves investigating and comparing the issue to the threat of information from the company to identify its validity, agree on a course of action, and then manually solve the problem – all with possibly millions of signals and often incomplete information [5]. Moreover, many of them are repetitive. Analysts also waste valuable time on repeated tasks, which preclude them from identifying more critical problems. Security automation works a great deal for the information technology team. If an alert appears, it determines instantly whether an action based on previous responses to similar incidents-is required, and if so, it can remedy the problem automatically [2]. Meanwhile, security analysts have a longer time in which they can focus on strategic planning, threats, and more thorough research, which adds value to the company.

Keywords —*Security automation, Information security, management, security, configurations, cybersecurity, automation, information technology, IT security*

I. INTRODUCTION

Security automation consists of 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 occur and then acting on them on a timely basis. Security automation works effectively for the security team, so they don't have to wear through any warning anymore manually. Automated security detects threats in the workplace environment [10]. It also can triage potential vulnerabilities and risks by step by step process, guidelines, and decision-making defined by security professionals to evaluate the incident and ascertain if it is a serious problem. All this can occur in seconds without any staff action [3]. Repetitive, time-consuming tasks are lessened for the security analysts when their systems are automated so that they can focus on greater value-adding work. Security automation can also easily identify threats. According to the ESG study, IT departments ignore 74% of security incidents or alerts – even though security solutions are in place because of its volume. Security automation not only can detect and address these common problems but can also eradicate human error, including inexperience, fatigue, and carelessness [6].

Initially, discussions have explored how cybersecurity systems are designed to automate certain common processes, and you are likely to have automation tools already put in place in many companies. In many company information systems, for example, information security products can be already set up for detecting and scanning devices automatically [1]. They can carry out an evaluation based on an organization-approved set of security checks. Upon completion of the evaluation, vulnerabilities identified may be fixed. When addressing new automation strategies, industry experts typically refer to the resources that automate as well as evaluate processes, such as security automation and orchestration (SOAR), custom-developed

applications, robotic process automation (RPA), and personalized applications. SOAR products are purpose-built tools that interlink activities and perform specific automated actions with other safety tools in response to defined threats. RPA instruments are a wider range of automation tools for the automation of a broad range of processes [12]. In the HR and Finance fields, the use of RPA tools has increased significantly but cybersecurity teams are also able to leverage them. Custom software and code can automate any form of analysis and are frequently used in the face of a shortage or a specific problem in an enterprise without a resource outside the box tool. All of the above methods communicate with the instruments of an organization, gather data, interpret and act automatically or advise a team member to take more action [8]. What will be expected in this essay is the concept of security automation and its significance to the information technology.

II. LITERATURE REVIEW

A. Elements of security automation

Barak states that security automation goes beyond prevention, identification, and other essential components to secure organizations more efficiently. Four of the most current and relevant elements to consider when implementing security automation are:

1. Implementation of policies. Despite networks becoming much more complex, it has become almost impossible to manually handle the security policies involved. Join automated policy execution that refers to the automated process of all IT security administrative work. According to Barak Numerous vendors are offering tools for automating network security policy implementation, to help you fulfill domestic or regulatory protection requirements more easily. Most also provide automated systems for administrative tasks such as onboarding / offboarding as well as control of the User Lifecycle [16]. Automation of the provision, supply, and application security can enable IT, teams, to gain better control of data, costs and time, and tools offering businesses are often referred to as security automation.

2. Prioritization and monitoring of alerts. According to Barak, many people see the automation role through the control lens and priority warnings. Warning management and priority setting was usually a manual task, which was rather repetitive [17]. A group of analysts at a Security Centre, to determine the important data points, would have to compile alarms and look at the monitor every day. There are today different methods for automating alert monitoring and prioritization. For example, rules and thresholds may be developed, threatened intelligence may be used, or advanced conduct analysis or learning machines may be introduced.

According to Barak, the establishment of rules and thresholds is declining ineffectiveness, because it is dependent on a person's manual effort to assess which warnings are relevant and which are not. And it also demands that these guidelines be updated periodically, as information security threats tend to evolve and hackers also know precisely which businesses are searching for alerts. In other words, it is a little more reliable to rely on the intelligence of the threat [24]. This type of automation relates to threat information gathering from different sources that can allow companies to determine which alerts they are looking for and which ones are relevant. For example, if a company can handle networks from different intel sources and utilize them, it could know if a certain kind of attack takes place worldwide. Automatic intelligence of threats will help the organization plan itself before the attack is too late to defend itself from this future attack. According to Barak behavioral analysis and machine learning are some of the most advanced types of automated warning monitoring and priority-control since they don't concentrate on rules and thresholds or "established risks" rather than using the new technology to know what typical network responses like.

3. Planning for incident response. The planning of accidents is also known as health automation. One way of thinking about these emerging technologies is to use an intelligent ticketing system that allows businesses to track and organize steps needed to respond to the evolution of a safety event. Providers in this field help businesses build playbooks for various types of threats, so that when every second count, portions of their response can be automated [2]. Barak also mentions that workflow is automated to ensure that businesses connect with the relevant internal and external stakeholders, adhere to legislation for subjects such as privacy alerts, and set up a clearly defined audit trail.

4. Analysis, intervention, and remedy. According to Barak automating research, action and cyber threat remediation involves using technology to accomplish activities as a competent cyber-analyst. In some ways, the other components of security automation – politics, priority setting, planning – work to quickly identify and shut down threats before they affect operations. In analysis, action, and restoration there are different aspects of what a business might automate [2]. For instance, some of these components could only tackle one, while others might concentrate on a certain function, for instance automating the confinement of compromised devices. Some businesses use automation and artificial intelligence as a cyber analyst to carry out the entire process from end to end. All these security technologies unlock overcharged safety resources, supporting security teams to concentrate solely on global but critical tasks, and to focus mostly on organizational strategies that make their business safer [2].

According to a study done by Metheny, the implementation of security automation in information technology focuses on the quality of safety checks in information systems. Automated CM practices include knowledge of the procedures the company may use, including the techniques and technology used to capture and review security information more regularly [4]. The enterprise will, therefore, have to guarantee that the CM plan involved a set of measures and mechanisms used to effectively respond to collected data. Automation may change the nature of safety assignments, but they will not be removed soon. Although for certain tasks, other tasks are better left for the citizens, as an additional resource. Metheny says that when you decide to automate depends where the benefits outweigh the risks. And the level of risk you experience depends upon the approach you take to the process and the tasks you decide to automate. Whilst automation tools have come a long way, space for improvement is still open [4]. Decisions remain as to how they will grow and how they integrate into the business. The technology works fine for easy tasks in its current form but has not been able to address complex tasks.

Haq and Khan mention that given that smartphones can access information from the internet, their security threats for sensitive information are increased [2]. Smartphones have in turn made access to knowledge simple and quick, as they have become personal computers that people move at all times. They suggest that this takes consistent and proactive monitoring to identify attack trends and raise awareness for organizations. The oil and gas industry, where authors are involved, is no different when it comes to taking cybersecurity measures. It's a cache full of useful and sensitive information, at times. Haq and Khan also mention that a new study of cybersecurity in the oil and gas sector carried out by Fox-IT and Oil & Gas IQ has revealed some very troubling findings [2]. Although oil and gas companies know that they will need to take precautions against cyber menaces like Advanced Persistent Threats (APTs) or hacktivism, with 90% agreeing that it is important to respond within hours to a cybersecurity event, the majority have not taken decisive steps to safeguard themselves[2].37 percent claim that they "do not trust" in their cybersecurity measures and 45 percent claim that they "somewhat trust." 23 percent suggest that they don't track their network regularly and 19 percent don't distinguish their IT (IT) network from their OT (Operational Technology) network. It should therefore not be shocking that the numbers of cyber-attacks against

oil and gas companies registered in 2013 were over 6,500–a 179% higher than in the past year, as a study by PwC showed [2]. Numerous computers, especially when used in many locations, but these approaches are very risky. They are based on a generally wrong assumption that security controls are not changed or removed once they have been implemented. In several cases, security checks can be modified [2]. The introduction of new features, improvements to existing features, and restart protection settings by the default values of software fixes, enhancements, and other updates. The introduction of a new application may change settings for the configuration used by another application, particularly when components are shared. Any user with the privilege of administrators can alter, disable, or delete security controls, particularly when a user believes that security controls prevent or otherwise irritate the user. Another malware or other attack part that disables a device [2].

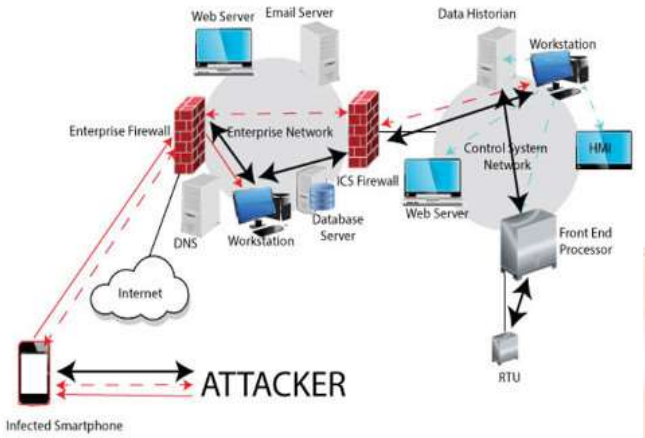

Fig i: Intech process automation [1].

B. 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 [5]. 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

Nguyen and Graham mention that over the last four to five years, safety automation has become a specific area. It focuses on safety operations centers (SOCs) and speeds up analysts' ability to alert disposal and start remedying. It, therefore, becomes an important component of safety and the response to incidents [5].

The technology of automation and orchestration helps to address the worldly; it collects and enriches the warnings. But it begins to evolve to increase the intelligence of threats so that we can deduce more precisely the right decision and best action in a particular scenario. Instead of merely gathering and presenting data, a brain is added — AI and computer education are used to help analysts make better decisions from better information [5]. A normal analogy is when you determine what to wear, check your weather, and choose clothes based on the forecasts of the meteorologist.

In space there is confusion. Solutions-seeking businesses have a list of 20 to 30 suppliers. To minimize the options and concentrate on the one that best fits for the company, it is necessary to evaluate the providers. Some automation can be implemented quickly, reducing the time it takes to integrate into your environment with existing solutions significantly. There are different implementation approaches; some are easier than others. Some suppliers make it as simple as possible to replicate an implementation of the Drag & Drop workflow to start and run your playbooks. Others may need more development backgrounds, scripting, and coding skills that your operating team may not have. All the solutions are needed to understand what your processes are and how your analysts can simplify these processes today.

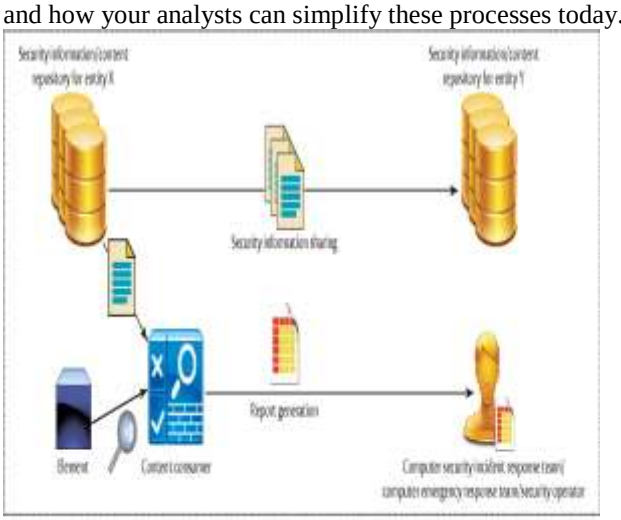

Fig ii: Security automation and threat sharing options [5].

The framework for connecting products with third-party products through their APIs should be open to consumers. Nguyen and Graham state that the truth is, APIs alter and the integrations on the other hand don't always have you. If the APIs shift, the support infrastructure of the orchestration and automation system must be able to upgrade plug-ins or integrations quickly and avoid any disconnections in service to the company. Various vendors have chosen different architectures [5]. To choose one product that is shown to handle the scale and speed with which the market is beginning to develop in large-scale environments is something to take into consideration so that it can extend over the long term with your environment. Nguyen and Graham state that security Automation is a framework; specialists are needed who fully understand safety and can lead knowledge from the front line and implement best practice [5]. Either it is prebuilt for use from the box, or a home expert designs them to work either together or automate the process, the company needs the right playbooks.

Nguyen and Graham suggest that the journey to automation must be completed in steps. It's not an excellent way to start developing complex playbooks and processes that you can find the coolest [5]. Concentrate on the low-hanging fruit. Start with easy to deploy and low-regret case applications. The "assault mailbox" is a common initial scenario. A lot of companies do not know if they should open a mailbox for clients and users who think that they receive suspicious emails with URLs or attachments [5]. Firms need to examine URLs and attachments to see whether they are malicious or not. This is easy to handle for automation tools as only "yes" are wrong or "no" is not bad. No services need to be shut down or anything can be remedied. Map the processes you wish to automate for the first twelve to twenty-four months, with a focus on low effort cases, low regrets, and low time savings [5]. It is necessary to protect your solution in addition to selecting the right case for use. The integration and credentials into your various technology from third parties in automation and orchestration instruments will be the only way that they can truly orchestrate. Therefore, you will have some sort of SkyNet by nature — the universal control of one area — and the profile of the threat changes somewhat.

Nguyen acknowledges that Though automation is not a new topic, it is becoming increasingly important because of intensive, ongoing attacks on organizations in all industries. The

latest Cyber-Security Jobs report states that 3.5 million unfulfilled cyber-security jobs will be held by 2021; the threats of today are simply insufficient by qualified security professionals [5]. To boost their ability, hackers have turned to automation. We have to do the same to keep up with them. Your organization will make better decisions from the best data, improve efficiency, and enhance overall safety by selecting the right automation and orchestration approach and by using the cases.

III. DISCUSSION

More frequent and advanced cyber-attacks are becoming increasingly difficult to avoid and mitigate. The thousands of alerts created with different security tools are often not effectively handled by security teams [23]. Analysts will need to complete manual, repetitive activities to analyze these possible risks. In addition to the burden of inadequate time and resources, many businesses simply cannot cope with the amount of safety work. The exponential rise in cyber-attacks has contributed to the emergence of safety automation as a hot subject for organizations and safety teams [21}. Security analysts had to battle, evaluate, and act on all alerts before automation, a technology that eventually proved unattainable. The huge number of threats required an automated response in the event of a cyber-attack or security violation to be identified and reacted more quickly. Together with automated emergency management, a more proactive approach was increasingly required to resolve safety concerns. Safety automation came from there and provided a systems-oriented approach to machines [22]. In effect, it has evolved into safety automation and orchestration, which makes it possible to link security instruments to workflows. Providers currently sell SOAR solutions that automate responses and corrections. Security orchestration, automation, and response solutions. Providers use various and contradictory terminologies to define their devices [5]. Make sure you know what features a security automation platform needs before you begin searching for vendors.

A. Cybersecurity automation tools and platforms

Types of process automation and information security applications include:

1. Robotic Process Automation

1. Robot process automation typically defined as a process of automating routine tasks utilizing robots — either physical or virtual like application bots. In cybersecurity, this refers generally to the automated systems' ability to conduct tasks like testing, tracking including low-level emergency response. It simply involves collecting and compile data, analysis, and detection methods for simple breaches and other limited-cognitive tasks [20].

2. Response and Security Incident and Event Management and Security Orchestration Automation-They apply to a variety of approaches that leverage your Security Operations Center 's capabilities and productivity without connecting your human resources to low-level tasks. This helps simplify three key information security activities – protection structure, protection automation, and safety response – by enhancing the management of risks, vulnerabilities, and security incidents. By nature, SIEM is more manual [13]. This bundled solution system includes manual responses to warnings and periodic updates and modifications to systems, regulatory sets, and signatures to automate, efficiently, and accurately identify them [19]. However, the main objective of this strategy is to identify known threats and to identify new or unknown threats that are less successful.

The use of SOAR internally or externally is a little more complex and takes certain SIEM warnings and automatically responds to them when needed for triage and remediation. This uses the cognitive tools and methods used for learning from current threats through artificial (AI) and machine learning (ML) to help classify new ones. SOAR and SIEM are close in several ways — after all, both collect and use the same information from different sources to examine anomalies [19].

3. Certificate Management

Due to Google's demand for encryption, extensive use of SSL certificates and keys led to the establishment of many hazardous weak spots. The lack of penetration in the network as well as public key infrastructure is one of the greatest challenges for security measures — and for the success of a business. Certificate management systems and certificate detection applications help handle more than just web certificates. They can help discover all of the network's X.509 digital certificates, irrespective of brand, type, issuance, date or expiry dates — including certificates for signature code, customer certificates, IoT, SSL / TLS and device certificates. A clear example is the Sectigo Certificate Manager (SCM) or the Comodo CA Certificate Manager (CCM) [14].

4. Custom Automation Solution Development

The idea of designing custom automation systems is another category that we should not consider at least. We recognize that all businesses are different and that organizations in different sectors have different needs [20]. Although some current techniques for cyber-security automation can always be effective, it can be advantageous for a specific company to create tailored solutions that suit your business's needs. It can be handled by your internal development team, but you will most probably like to hand it over to a third-party provider.

B. The Need for Continuous Security Management

Security monitoring has historically been largely carried out according to strict routines are observed. Modern security fixes must be mounted once a quarter in computers, except for emergencies. Computers are subject to authentication in many organizations perhaps only once every couple of years. Nevertheless, these timelines are not adequate to meet the security needs of today. Every day new, exploitable software vulnerabilities are discovered, several thousand of which are publicly recorded each year [14]. Every year. Given the number of fixes that need to be implemented within a corporation, companies also have to prioritize the patching to make sure that the most critical vulnerabilities are patched faster than other vulnerabilities. Sometimes for weeks or months less serious vulnerabilities remain unpatched, or never patched at all. We need a way to recognize when new patches are available, to prioritize their installation, and to ensure they are installed quickly and to take support actions such as rebooting of patch installations off hours [25]. Attacks can misconfigure software security or exploit vulnerabilities in security checks. Mitigating attacks aimed at these types of security issues often involve the ability of an organization to easily restore security checks or device safety settings. In the worst case, a company could have to carry out drastic measures immediately, such as removing a service indefinitely to avoid its compromise [18].

You also need to be able to quickly check that the system is properly protected as well as to adjust the security status of a system on request. It takes much time for someone to test all security elements of a system — that any patch is present and installed and that the security configuration of all software is correctly configured, etc [6]. A single device can give its operating system and applications thousands of security settings [11]. There are now far more audit compliance requirements than before.

IV. CONCLUSION

It is very dependent on your industry and company how you can support you with security automation. If it's retail, healthcare, manufacturing, financial services, the public sector, or another industry, the resources and processes can rely heavily upon. Retailers for instance deal in unpredictable ways with ransomware and phishing attacks. Automation is effective in clearing the deck of repeated attacks and false positives, which will make security analysts better able to research these cases and find

a long-term solution. It is important to work with an IT team and other organizational leaders to recognize issues that need to be addressed before any vendor is considered [12]. Automation is on the list of priority areas as businesses understand that it eliminates risks, makes their networks transparent, and leverages their security stacks. The reduction of human error is one of the greatest threats. If an engineer is called upon to perform the same task each day, searching for needles in the same haystacks, they eventually make a mistake. Many business security technologies and services are analyzed to understand automated controls, particularly those which allow central management operations to be automated.

The management of information security is a very complicated and ultimately costly problem. Although SMEs do not have the financial resources to implement sufficient information management programs, large enterprises are faced with growing uncertainty in their information technology industry. Security automation will lower the costs and complexity of safety operations without human interaction. Automation is not a scientific joke or a joke. It is embraced by both small and large businesses. The cybersecurity department will focus on more complex tasks by introducing automation in the framework of an enterprise. This means that the machine can perform the mundane, repetitive work, and cybersecurity project managers can work more critically, creatively and technically to solve issues, improve the corporate risk positioning and manually examine systems and data to find out unintended behavior and compromise or defect indicators [15]. For a modern enterprise, this is a losing idea that information security automation will lead towards addressing. Automation may also assist in addressing small or inefficient information security teams (with the organization's increasing digital footprint). Regardless of human mistakes and the sheer amount of data to handle, a possible threat is unavoidable. The assumption that teams will catch future cybersecurity incidents accurately is inherently unrealistic. Automation could be vital to safeguard your organization 's reliability and guarantee reliability in robust and repetitive processes.

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-automation-smartphone-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/explaining-security-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/computer-science/security-automation

[5] P.Nguyen and A.Graham, "Enhancing Security with Automation and Orchestration, "Serious Edge,2015.Retrieved from: https://edge.siriuscom.com/security/enhancing-security-with-automation-and-orchestration

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] S. Radack, "Security Content Automation Protocol (SCAP): Helping organizations maintain and verify the security of their information systems", September 2010.

[12] S. Hanna and D. Waltermire, "Security Automation Webinar: Protecting Your Enterprise with Security Automation", May 2013.

[13] G. Koschorreck, "Automated audit of compliance and security controls", *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*, 2011.

[14] P. Dwivedi and S. C. Diana, "Analysis of automation studies in the field of information security management", *International Journal of Engineering Research and Development*, vol. 6, no. 12, pp. 60-63, 2013.

[15] V. Antonie, R. Bongiomi, A. Borza, P. Bosmajian, D. Duesterhaus, M. Dransfield, B. Eppinger et al., *"Router Security Configuration Guide"*, December 2005.

[16] W. M. Fitzgerald and S. N. Foley, "Avoiding Inconsistencies in the Security Content Automation Protocol", 2013, [online] Available: http://www.cs.ucc.ie/~simon/pubs/safeconfig2013.pdf.

[17] M. N. Alsaleh and E. Al-Shaer, "SCAP based configuration analytics for comprehensive compliance checking", *Configuration Analytics and Automation (SAFECONFIG) 2011 4th Symposium on*, pp. 1-8, Oct. 31 2011-Nov. 1 2011.

[18] R.P. Lippmann, J.F. Riordan, T.H. Yu, and K.K. Watson, "Continuous security metrics for prevalent network threats: introduction and first four metrics", *MIT-LL*, May 2012.

[19] R. Struse, *comments at 8th Annual Information Technology Security Automation Conference (ITSAC)*, October 2012.

[20] R. Montesino and S. Fenz, "Information security automation: how far can we go?", *2011 Sixth International Conference on Availability Reliability and Security (ARES)*, pp. 280-285.

[21] E. Kogan and E.M. Haber, "Security and usability: Designing secure systems that people can use", *Security administration tools and practices*, pp. 357-378, 2005.

[22] A. Kott and C. Arnold, "The promises and challenges of continuous monitoring and risk scoring", *IEEE Security & Privacy*, vol. 11, no. 1, pp. 90-93, Jan. 2013.

[23] H. Holm, T. Sommestad, J. Almroth, and M. Persson, "A quantitative evaluation of vulnerability scanning", *Information Management &Computer Security*, vol. 19, no. 4, pp. 231-247, Oct. 2011.

[24] S. Pfleeger and R. Cunningham, "Why measuring security are hard", *IEEE Security & Privacy*, vol. 4, pp. 46-54, Mar. 2010.

[25] A. Malin and G. Van Heule, "Continuous monitoring and cybersecurity for high-performance computing", *Proceedings of the first workshop on Changing Landscapes in HPC Security*, pp. 9-14, 2013.

[26] T. AlSadhan and J.S. Park, "Leveraging information security continuous monitoring for cyber defense", *Proceedings of the 10th International Conference on Cyber Warfare and Security*, pp. 401, March 2015.