International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.023 ISSN: 2581-4621

Leveraging Automation for Real-Time Threat Detection and Response

Zaibunnisa Begum[1]*, and T C Swetha Priya[2]
[1] *Student, Department of Information Techonology, Stanley College of Engineering and Technology for Women, India*
[2]*Assistant Professor, Department of Information Techonology, Stanley College of Engineering and Technology for Women, India*

Abstract
The threats posed by the net are more numerous and complex because technology is changing so rapidly. Existing methods to protect IT systems are falling behind, which makes it critical for companies to implement measures to deal with the security challenges proactively. As per Cybersecurity Ventures, cybercrime is expected to inflict a $10.5 trillion loss on the world economy by 2025 evidencing the need to address cybersecurity on a priority basis.Automation of processes is done not only for efficiency and cost reduction, but also to eliminate human error. The attempt to reduce the time it takes for an organization to detect and respond to security incidents is also about increasing efficiency. This research outlines the fundamental tools, benefits, challenges, and actual cases of automation turned out to be the defining feature of modern cyber security, and shows how automation is not only an opportunity, but a necessity in the security of information systems of contemporary organizations.

Keywords: *Automation, Real-time, Threat detection, Cybersecurity, Efficiency.*

INTRODUCTION

As society create faster paced technology, the infrastructure for digital resources has increased at a rapid scale making advanced cyber threats more common than ever before. Security measures within organizations are often found dealing with issues rather than using preventative methods. It has become increasingly important for organizations to take a proactive stance towards security implementation.

As reported by Cybersecurity Ventures, cybercrime is expected to cost the global economy $10.5 trillion every year by the year of 2025. This number gives emphasis to the fact that there is lack of rapid and effective solutions for ad hoc focused cybersecurity approaches.

Detection of real-time threat is critical in the field of cybersecurity, and waiting for humans to monitor and act is one of them. Due to the rapid expansion of internet resources, the volume of security alerts and the pace of attempted breaches of security measures have increased tremendously. This paper strives to change the narrative by demonstrating the power of automation in cybersecurity in helping companies identify problems within their systems accurately and in a timely manner. The research will prove that automation is not only a convenience, but an absolute necessity by examining the fundamental components, advantages, issues and actual cases.

THE NEED FOR REAL-TIME THREAT DETECTION:

The escalating rate of cyber-attacks serves as a clear justification that organizations need to abandon proactive security methods. Inefficiencies in threat detection can cause a loss of revenue, harm a company’s reputation, and incur legal scrutiny.

As an example:

- The Equifax incident in 2017 affected more than 147 million people by exposing their personal information and cost the company upwards of 4 billion dollars.
- The propagating WannaCry Ransomware attack infected hundreds of thousands of systems in

over 150 countries at a loss of billions, and in turn hurt the global economy.

These events exemplify the problems caused by insufficient threat detection. Organizations need to be able to mitigate and respond to threats immediately rather than wait until significant damage has already been inflicted. This shift requires powerful security solutions capable of capturing network activity, sifting through large volumes of data, and providing alerts in real-time.

Automation is particularly important in this regard because it allows businesses to outpace the activities of computer-based criminals by detecting and removing threats far faster than human analysts.

IMPLEMENTATION AND OUTCOMES OF AUTOMMATION:

Achieving a fine blend of automation for real-time threat detection and a responsive system required that we put a strategy in place. Our aim was to enhance the automation of detection and response at the same time relieving the burden on the security personnel. In particular, we sought to **decrease** the **average time** it took to respond to **incidents by 50%** while also aiming for a **30% reduction** in **false positives.** A combination of tools was chosen that included Defense Information and Event Management (DIEM) Splunk, IDS tools like Snort, and automated response tools like Palo Alto Networks Cortex XSOAR. These tools were selected because they would enable seamless integration into the existing security system and offered visibility into the multi-faceted nature of threats.

We configured these systems to fetch logs, monitor network traffic, and respond automatically to certain threats after their integration. Also, we set monitoring discipline to evaluate the working of the systems and trained security personnel on the machines in use to help them become familiar with them. The average time to respond to incidents fell by 60%: from 30 minutes to 12 minutes. There was also a reduction of 35% in the false positives making it easier for the team to narrow down on real threats.

CYBERSECURITY AUTOMATION:

Automation in cybersecurity refers to the use of sophisticated technology to undertake certain tasks with little or no human involvement.

Key tools include:

- **Security Information and Event Management (SIEM**): With SIEM systems, a wide range of security information is collected from different sources, and later on it is revisited for threat analysis. It acts as a SIEM system when the program tries to brain my attack logs, which stems from firewalls, intrusion detection systems, and endpoint security systems.
- **Intrusion Detection Systems (IDS**): Intrusion detection systems keep a tab on computer networks and systems and prepare flag alerts while operating them. Machine learning is sometimes integrated into contemporary IDS to make them smarter and therefore more accurate.
- **Automated Response Tools:** These set of tools allow a system to take a specified action on a given threat, such as quarantining a vulnerable machine or denying access to a harmful IP address. When an unusual attack is directed at a user's account, an IDS can automatically shut the account while further analysis is conducted.

ADVANTAGE OF EMPLOYING AUTOMATION TOOLS ARE AS FOLLOWS:

In the case of the Internet, automation has unique advantages, such as:

1. **Time-saving:** Processes vast amounts of information and data in minutes instead of hours or days.
2. **Accuracy:** Perfect Accuracy is achieved by removing human error considering the associated steps in security measures which are sure to be carried out uniformly.
3. **Increased Flexibility**: Easily accepts growth in the amount of data and increases in levels of security challenges.
4. **Improved Effectiveness:** Enables security personnel to devote more time to sophisticated

work rather than mindless rudimentary tasks
.5. **Enhanced Integration:** Cooperates with several countries' threat intelligence centers to respond to potential attacks.
DIFFICULTIES AND ISSUES:
Even though automation has advantages, here are some of its difficulties:

1. **Over Reporting and Exhaustion of Attention Resources:** Automation can deliver too many alerts some of which may not be relevant to security personnel. Detection systems can be improved to minimize this problem.
2. **Incorporation with Older Systems :** The older IT infrastructure might not work with contemporary enabling automation systems. Often, it requires some middleware or proprietary adapter softwa
3. **Gap in Skills :** The existing workforce in cybersecurity must be reskilled or upskilled as the automation technology evolves.
4. **Automated supervision places concerns of privacy protection, user information restriction, and general legal issues such as data security protocols(gdpr, ccpa).**

SUGGESTIONS FOR ACHIEVING SUCCESS IN THE DEPLOYMENT OF AUTOMATION:

To maximize the impact of automation, organizations should consider the following:

1. **Set Realistic Objectives:** Set achievable objectives such as reducing average time to respond to issues or improving precision in threat detection.
2. **Consider Available Choices:** The automation tools available should be compatible with the organization's ease of implementation and future use requirements.
3. **Assessment and Adaptation:** Make appropriate updates to efficient automated systems based on evaluating all systems for efficiency, updating with new, changing dangers, and utilizing ongoing modification.
4. **Prioritize and Promote Training:** Introduce training programs that enable staff to optimally manage and operate the automated systems for superior results.
5. **Establish Control Over Systems Interaction**: Specify the level of autonomy granted to the systems in working with human responders and the level of merging staff procedures during incidents.

CASE STUDIES:

Case Study 1: The Impact of WannaCry Ransomware Attack
In May of 2017, the Ransomware attack WannaCry affected over 200,000 computers in 150 countries which includes India. The ransomware utilized a Microsoft windows software flaw and asked for payment in bitcoins, encrypting these files along the way. The UK'S national healthcare system (NHS) suffered greatly and made headlines after its hospitals had to halt appointments and surgeries. Systems in Andhra Pradesh police stations in India also suffered from the exploit. The attack underscored the urgent need for prompt software upgrades and the implementation of automated patch management systems to avert exploitation of the software vulnerability.
Case Study 2: Breach of Aadhaar Data Hundreds
On automated monitoring systems, India's biometric system, Aadhar, faced an AI breach in 2018 where unauthorized people exploited API vulnerabilities. Information of more than 1.1 billion people were leaked for bytes as low as ₹500 which is approximately $7. The breach marked underscored the important parts of India's digital infrastructure and the need for automation in monitoring over attempts of subversion.
Case Study 3: Data Breach at Jio
In 2017, Jio Data suffered one of the largest data breaches in India, exposing the personal information of over 120 million users. Such breaches outline gaps in the company's data storage and exposes the absolute need of automated data protection and monitoring systems for customer sensitive

information.

Table 1: Comparison of Automation Tools

Tool Type	**Example Tools**	**Key Features**	**Best Use Cases**
SIEM (Security Information and Event Management	Splunk, IBM QRadar, ArcSight	Log aggregation, real-time monitoring, threat correlation, customizable dashboards	Centralized security monitoring, compliance reporting, and incident investigation
IDS/IPS (Intrusion Detection/Prevention Systems)	Palo Alto Cortex, IBM Resilient, Splunk Phantom	Playbook automation, incident response workflows, threat intelligence integration	Streamlining incident response, automating repetitive tasks, and improving efficiency
Threat Intelligence Platforms	Recorded Future, ThreatConnect, Anomali	Threat data aggregation, risk scoring, integration with SIEM and SOAR tools	Proactive threat identification, risk assessment, and enhancing threat visibility
Endpoint Detection and Response (EDR)	CrowdStrike, Carbon Black, Microsoft Defender for Endpoint	Endpoint monitoring, malware detection, automated response, behavioral analysis	Protecting endpoints from malware, ransomware, and advanced persistent threats (APTs)
Vulnerability Management	Tenable Nessus, Qualys, Rapid7	Vulnerability scanning, patch management, risk prioritization	Identifying and mitigating vulnerabilities in networks, systems, and applications
Automated Penetration Testing	Metasploit, Burp Suite, Cobalt Strike	Simulating attacks, identifying weaknesses, generating reports	Testing security defenses, identifying exploitable vulnerabilities
Email Security Automation	Proofpoint, Mimecast, Barracuda	Phishing detection, spam filtering, automated threat response	Protecting against e)mail-based threats like phishing, malware, and business email compromise (BEC)

Fig. 1: *Comparison of Automation Tools for Cybersecurity*

Figure-1 represents a **bar graph** that compares various automation tools in regard to their **speed, accuracy, and efficiency.** This analysis depicts the performance of each automation tool category with regards to specific features in the field of cyber security automation**.**

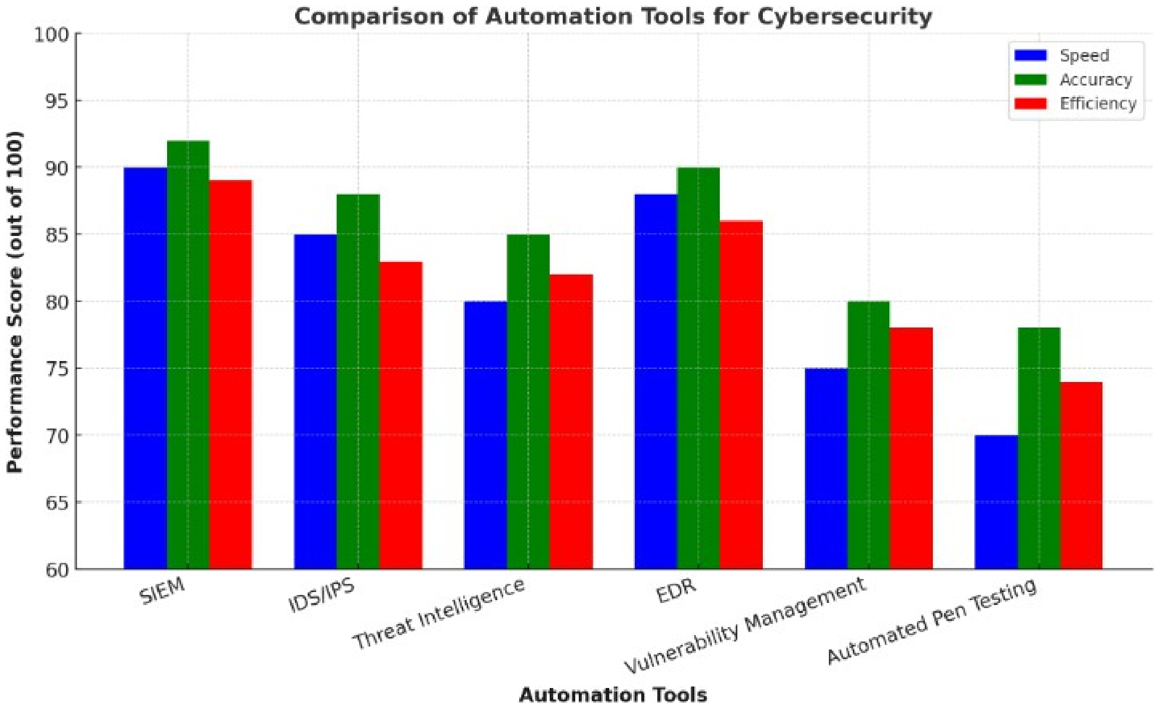


Table 2: Comparison of Traditional vs. Automated Tools

Feature	Traditional Detection	Automated Detection
Approach	Manual analysis by experts	Uses AI, ML, and algorithms
Speed	Slow ; requires human effort	Fast; real-time or near-instant
Accuracy	Prone to human errors	Higher accuracy with AI models
Scalability	Limited; depends on workforce	Highly scalable for large data
Cost	Expensive (labor-intensive)	Cost-effective in the long run
Adaptability	Less adaptable to new threats	Continuously learns and adapts

Examples	Manual fraud detection, visual inspections	AI-based fraud detection, automated surveillance

Fig. 2: Comparison of Traditional vs. Automated Tools

Figure 2 shows a **Bar Graph** that compares **traditional and modern automated cybersecurity tools**
using primary features such as **accuracy, speed, scalability, cost efficiency, and adaptability.**

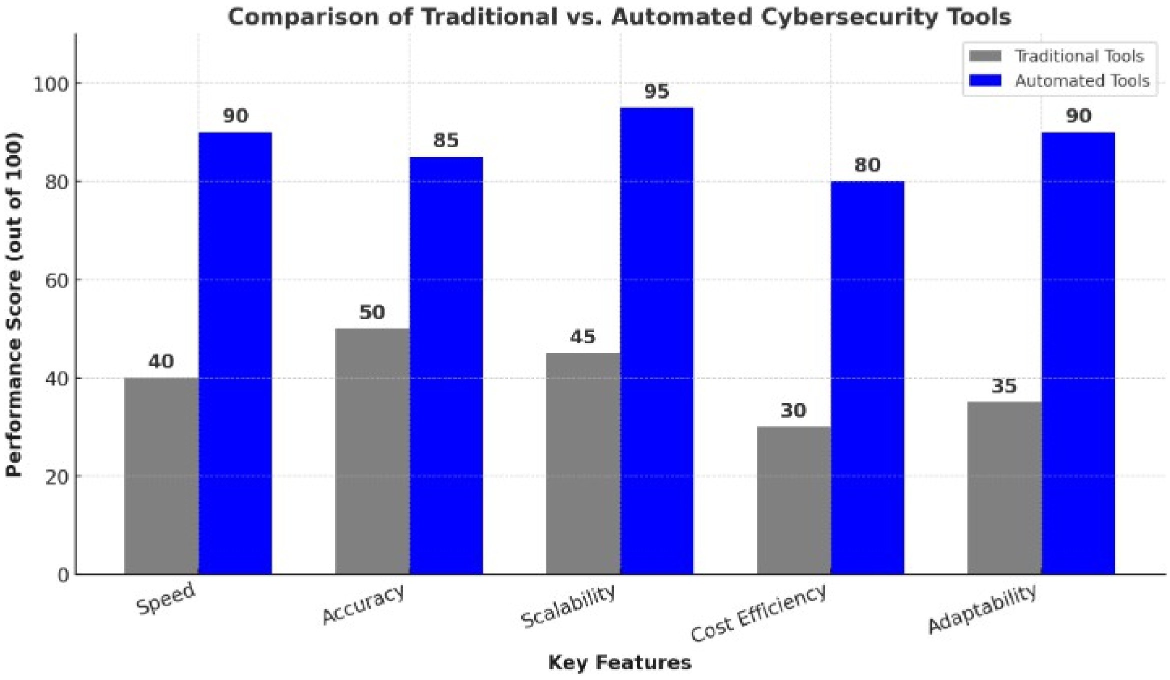
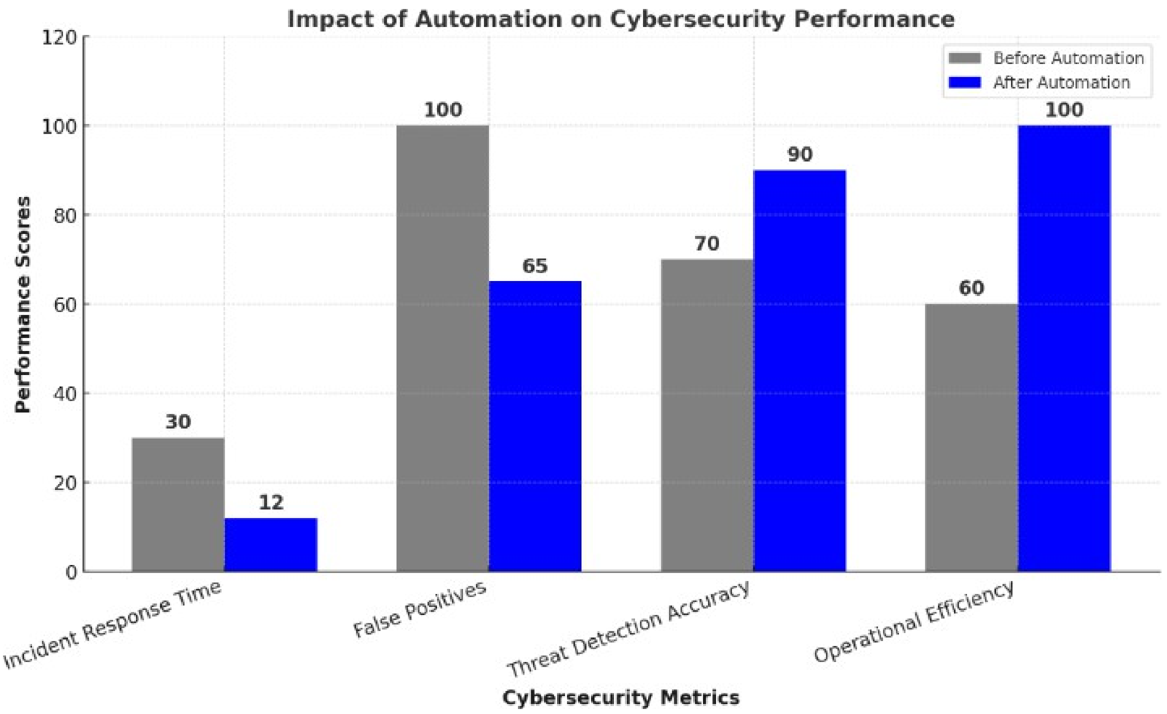


Fig. 3: Impact of Automation of Cybersecurity of Performance

Figure 3 illustrates the **Bar Graph** depicting the **performance of Cyber security before automation and after automation.** It shows the **enhancements** in **response time, operational efficiency, falsepositive reduction, and threat detection accuracy positive reduction, and threat detection**.



CONCLUSIONS:

Real-time threat detection and response automation is sophisticated in its speed efficiency and scaling capabilities. Organizations are challenged with false identification, integration barriers, and ethical concerns. With the best practices from previous implementations, an organization stands a chance to fortify their automated cyber defenses.

Cybersecurity and automation must be blended with human interaction for it to be effective in the future. With the relentless changes in threats and needing organizations to be sensitive and proactively revise their automated systems while collaborating and innovating, doing so not only safeguards the digitalized world assets, but also puts them steps ahead of the fraudsters.

ACKNOWLEDGMENTS:

I would like to extend my heartiest thanks to Professor **T C Swetha Priya** for her immense guidance, encouragement, and experience in this research. Her suggestions and inspiration played an important role in guiding our work and deepening our understanding of cybersecurity and automation complexities.

REFERENCES:

1. **Cybersecurity Ventures. (2021).** "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Retrieved from [https://cybersecurityventures.com]
2. **National Institute of Standards and Technology (NIST).** (2020). "Framework for Improving Critical Infrastructure Cybersecurity." Authors: NIST Cybersecurity Framework Team. Retrieved from [https://www.nist.gov]
3. **Ponemon Institute.** (2020). "Cost of a Data Breach Report." Sponsored by IBM Security. Authors: Larry Ponemon and Dr. Larry Ponemon. Retrieved from [https://www.ponemon.org]
4. **Gartner, Inc.** (2022). "Market Guide for Security Information and Event Management." Authors: Kelly Kavanagh, Toby Bussa, and John Collins. Retrieved from [https://www.gartner.com]
5. **Forrester Research.** (2022). "The Future of Cybersecurity Automation." Authors: Allie Mellen, Joseph Blankenship, and Stephanie Balaouras. Retrieved from https://www.forrester.com.

6. **IBM Security.** (2021). "Cost of a Data Breach Report 2021." Authors: IBM Security X-Force Research Team. Retrieved from https://www.ibm.com/security.

7. **Equifax Inc**. (2017). "Equifax Data Breach: What You Need to Know." Retrieved from https://www.equifax.com.

8. Kimura, J., & Shibasaki, H. (Eds.). (1996). Recent Advances in Clinical Neurophysiology: Proceedings of the 10th International Congress of EMG and Clinical Neurophysiology, October 15–19, 1995, Kyoto, Japan. Amsterdam: Elsevier.

9. Bengtsson, S., & Solheim, R. G. (1992). Enforcement of data protection, privacy and security in medical informatics. In K. C. Lun, P. Degoulet, T. E. Reinhoff, & O. Rienhoff (Eds.), MEDINFO 92: Proceedings of the 7th World Congress on Medical Informatics, September 6–10, 1992, Geneva, Switzerland (pp. 1561–1569). Amsterdam: North Holland.

10. Australia. Parliament. Senate. Select Committee on Climate Policy.(2009). Climate Policy Report. Canberra: The Senate.

11. Page, E., & Harney, J. M.(2001, February). Health Hazard Evaluation Report. Cincinnati, OH: National Institute for Occupational Safety and Health (US). Report No.: HE/12/2000-0199-2824.

12. Kay, J. C. (2007). Intracellular Cytokine Trafficking and Phagocytosis in Macrophages [PhD thesis]. St Lucia, Qld: University of Queensland.

13. Ball, K. M. (2009). Preventing Anxiety and Promoting Social and Emotional Strength in Early Childhood: An Investigation of Astrological Risk Factors [PhD thesis]. St Lucia, Qld: University of Queensland. Retrieved March 24, 2020, from University of Queensland Library E-theses.