World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Cybersecurity automation: Enhancing incident response and threat mitigation

Suresh Vethachalam *

Engineering Manager.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(03), 572-585

Publication history: Received on 27 April 2025; revised on 01 June 2025; accepted on 04 June 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.3.0972

Abstract

This study looks at the rise of automation in cybersecurity as a way to deal with the rising number and difficulty of cyber threats. Cybersecurity gets a boost from automation because it helps catch attacks early, avoids mistakes by people and speeds up the response which is necessary to prevent major consequences from comprehensive attacks. The research uses a mix of working with data and studying industry cases to assess the performance of automated security systems. Automated tools are shown to raise the detection level and bring down the number of fake alerts, so security teams can look into only the most important risks. Also, automation helps the response team by speeding up the process between discovering a threat and dealing with it. They make networks in different organizations better able to handle cybersecurity risks. It points out how introducing automation into cybersecurity helps solve problems, but it also brings up issues about keeping up with changes and resolving ethical questions. Researchers may focus on using AI to manage computers more efficiently and look into security frameworks designed to respond to the latest threats from cybercrime.

Keywords: Cybersecurity Automation; Threat Detection; Incident Response; Behavioral Analytics; AI Integration; Network Security

1. Introduction

Cyber-attacks have become more complex and more frequent as time has gone on. Both the number and the skills used in cyber-attacks have grown, as crooks target important facilities, firms and people with ransomware, phishing and latest exploits. Because attacks are happening very quickly and change a lot, the usual manual ways to respond have become quite ineffective. Using common strategies often takes a lot of effort and can cause mistakes which results in delaying the recognition and management of threats. It is obvious from these challenges that manual security processes may not be able to keep up as cyber risks rise.

Because of this, automation tools are now crucial in the field of cybersecurity. With automation, security teams can keep an eye on things, review risks in real time and respond immediately which makes their work load lighter and boosts the company's competence. Using automated systems helps reduce mistakes, speed up responses to incidents and make work more efficient which helps counter the growing threat posed by cyber-attacks. Because automation and other modern solutions are needed, it is clear that efforts are being made to keep cybersecurity strong and respond to changing threats. These advancements are essential for organizations striving to protect their assets effectively in an era of escalating cyber challenges (Frumento, 2019; Li & Liu, 2021).

1.1. Overview

Cybersecurity automation involves using computers to help handle and improve security tasks that might normally be done by people. Some of the major processes it handles are detecting dangers, responding to incidents, managing

* Corresponding author: Suresh Vethachalam

vulnerabilities and following compliance rules. The goal of automating cybersecurity is to make responses to threats faster, more correct and more effective, helping organizations to address such threats quickly and across a variety of cases.

Key technologies underpinning cybersecurity automation includes Security Orchestration, Automation, and Response (SOAR) platforms, which integrate disparate security tools and automate workflows for coordinated threat mitigation. Artificial Intelligence (AI) and machine learning play critical roles by enabling predictive analytics, anomaly detection, and adaptive learning from evolving threat patterns. With information from several sources, automated threat intelligence can advise on effective defensive steps.

Usually, the incident response lifecycle covers preparation, detecting and analyzing events, controlling the situation, totally removing the threat and recovering from its impact. Automation helps out in every part by finding threats fast, organizing which alerts need attention and taking actions to contain them swiftly. This speeds up decisions for security teams and removes some of the manual work, so they have more time for meaningful work.

Together, these technologies and processes form the foundation of modern automated cybersecurity frameworks designed to enhance resilience against increasingly sophisticated cyber threats (Kiiveri, 2021; Repetto et al., 2021).

1.2. Problem Statement

Cybersecurity is improving, but finding and handling emerging cyber threats is still an issue. Most traditional solutions use people to process information and this becomes slow and challenging with the high amount and level of security data today. It is hard for human analysts to monitor, analyze and take action on a huge amount of information, making mistakes more likely and delaying appropriate responses. Such limitations give attackers opportunities to break in and use weaknesses which can cause data security breaches, losses in finances and harm the company's reputation.

If responses to cyber threats are late or incorrect, cyber defenses cannot function properly and organizations cannot tackle risks ahead of time. Because cyberattacks are becoming more difficult to stop, we require quicker, more effective and automated defenses that can work on a huge scale. That is why studying how automation supports cybersecurity helps solve these problems. Increasing use of automation can improve detection of threats, reduce mistakes made by people and speed up the response to threats, all of which make an organization's security setup more powerful and dependable in a dangerous digital world.

1.3. Objectives

This research concentrates on how using automation can boost cybersecurity in recognizing threats. Analyzing if automated systems are able to find and prioritize security threats better than can be done with manual methods. Assessing automation and its ability to have less human error is another major aim, since many security breaches happen due to human error from being tired or inattentive. It also explores how automation helps speed up responses which helps organizations limit and control threats early on before any important damage occurs. Besides, the research will also look at the issues and problems that come with adopting automation in cybersecurity, including fitting it into the current setup, requiring more staff and resources and meeting ethical standards. The study addresses these points to encourage better knowledge of automation's pros and cons which in turn helps teams improve their strategy and defense against computer hackers.

1.4. Scope and Significance

It mainly looks at automation software used to handle incident response and work on mitigating cybersecurity threats. It examines technologies such as Security Orchestration, Automation, and Response (SOAR) platforms, AI-driven analytics, and automated threat intelligence systems that support faster and more accurate handling of cyber threats. For companies dealing with more and harder-to-cope-with attacks, scope is highly important. Discussing the practical uses and issues of automation allows the study to add value to academics as well as help shape guidelines meant for practical use. The insights aim to help cybersecurity experts, policymakers and researchers understand how using machines can make defense stronger and how to prevent possible problems. Its purpose is to help plan and project future strategies that will increase an organization's resilience against evolving threats.

2. Literature Review

2.1. The Cyber Threat Landscape: Trends and Challenges

Today, many types of threats are common in cyber space and their tactics frequently shift, showing how complicated and frequent cyberattacks have become around the globe. Sectors everywhere are still affected greatly by cyber-attacks like malware, phishing and ransomware. It is always possible for malware to attack a system, take away its data and disturb operations. Phishing uses social engineering to get people to share things like passwords or install viruses, but ransomware goes after the systems themselves and holds the files hostage for a ransom.

Security threats now are seen to have grown in complexity, so attackers can find ways around security systems. In recent times, attackers have been using suppliers and trusted vendors to get into target organizations. Since zero-day exploits target unknown security holes in software, they are very dangerous. Machine learning makes it possible for AI attacks to morph and escape detection which is a significant change in the world of cyber offenses.

Social engineering is used to exploit human senses and emotions and risks found in Internet of Things and cloud platforms have brought forth new issues. Due to the rapid growth in digital technology and networking, especially in industrial IoT, attackers now have even more entry points to target, so it becomes very important to have advanced security strategies.

Because of increasing threats, thorough cyber threat intelligence and strict security standards are needed to find and stop them promptly. Continuous innovation and cooperation among cybersecurity stakeholders remain crucial to defending against increasingly sophisticated adversaries in a complex threat environment (Dhirani et al., 2021; Abu et al., 2018).

Figure 1 Key components of cybersecurity in industrial automation, including threat and risk analysis, network security evaluation, robustness and vulnerability scans, product testing and certification, quality management assessment and qualification, and workshops and trainings aimed at strengthening industrial control system defences

2.2. Incident Response: Traditional Approaches and Limitations

Normally, traditional incident response in cybersecurity depends on people manually spotting, understanding and dealing with security problems. Handling alarms this way leads to inefficiency because there are so many alerts and modern cyber threats can be quite complex. Analysts have to deal with lots of data from different places, without assistance from integrated tools which lowers the answer speed. Because these workflows are not joined, it becomes more likely for delays, mistakes in communication and missed tasks to occur.

Misreading the information, tiredness and inconsistency in following protocols are typical errors people can make while responding to incidents manually. The pressure to solve problems swiftly can cause errors such as wrong threat identification or missing early warnings of a compromise. In addition, manual methods do not grow with the organization, so when facing more attacks, the shortcomings of using humans become easier to see.

Espotting and fixing problems immediately is important, as delays can result in systems being offline for a long time, data being stolen and money being lost. If threat intelligence and routine protective measures cannot be fast-tracked, it

leads to delayed containment which harms overall security. Traditional technology cannot easily respond to complex attacks that need rapid and continuous coordination from many people.

Due to all these issues, there is a visible need to switch to automated or semi-automated methods for responding to incidents. Automation leads to improved accuracy, less waiting time and better handling of complicated incidents by connecting different security tools and building clear workflows. This shift is critical to strengthening cybersecurity posture in the face of evolving threats (Schlette, Caselli, & Pernul, 2021).

2.3. Cybersecurity Automation Technologies

There are several tools and technologies in cybersecurity automation aimed at making security operations faster and easier to handle with less need for human input. Security Orchestration, Automation, and Response (SOAR) platforms play a central role by integrating multiple security tools and automating incident response workflows. These tools allow quick discovery, examination and fixing of threats, by organizing jobs among many systems, cutting down response time and reducing chances of making errors.

Artificial Intelligence (AI) and machine learning models contribute significantly to automation by enabling advanced threat detection through behavioral analytics, anomaly detection, and predictive capabilities. Algorithms in machine learning can look through lots of data to see signs of cyber threats which help defenders anticipate attacks. Predefined actions for threats which are activated by specific warnings or signs, guarantee efficient handling and boost overall security.

For industrial automation, cybersecurity automation covers tasks like threat and risk analysis, evaluating network security and scans that check for vulnerabilities. They are used to spot problems in industrial control systems and protect system integrity. Knowledge is shared and everyone is ready with training and workshops and testing and certifying products verify they are safe. Quality management (QM) assessment and qualification processes ensure compliance and continuous improvement within cybersecurity frameworks.

Such a combination enables companies to find, study and deal with cyber threats effectively and promptly. Automating tasks cuts down on manual work, protects from mistakes and gives security teams more time to concentrate on big tasks. The integration of AI-driven analytics and automated response mechanisms represents a critical advancement in combating increasingly sophisticated cyber threats (Qabajeh, Thabtah, & Chiclana, 2018).

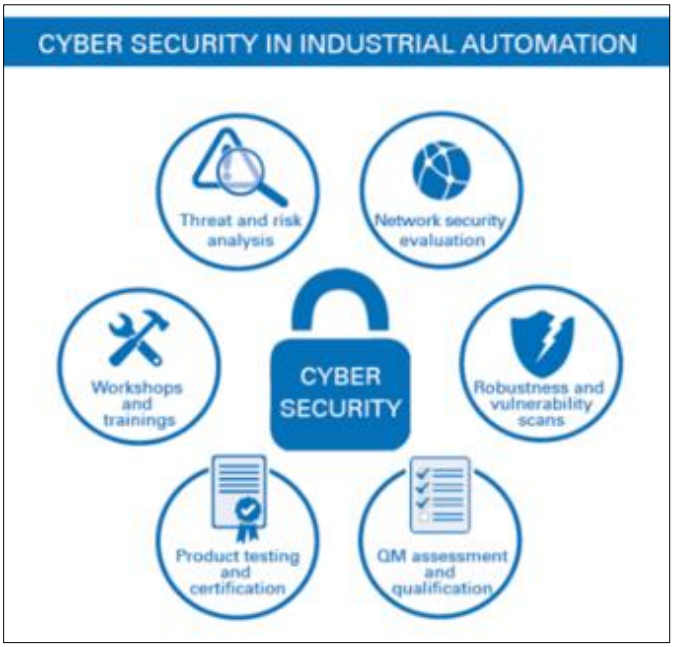

Figure 2 Overview of common cyber threats, including malware, phishing, and ransomware, alongside emerging trends such as supply chain attacks, zero-day exploits, AI-driven attacks, social engineering, and challenges posed by new technologies shaping the evolving cyber threat landscape

2.4. Automation in Threat Detection

Protecting systems from threats now relies heavily on automation because cyber threats have become more numerous and complex. A key role of automation in this field is to gather and examine a huge amount of data from traffic, system logs, people's activities and external alerts from other network suppliers. Data collection done automatically gives security systems a good sense of the situation and limits the errors that could arise when doing it by hand.

Artificial Intelligence (AI) and Machine Learning (ML) technologies are integral to transforming raw data into actionable insights for threat detection. AI and ML algorithms are good at finding patterns and anything unusual in huge and changing data sets that people would find very hard to deal with efficiently. When using these models, analysts are able to see when network behavior patterns shift which may point to intrusions, taking data away from the network or command-and-control communications. Because of this, advanced threats that traditional detection methods fail to detect can be recognized quickly.

ML makes anomaly detection a central method in automated threat detection. This method helps by creating a list of normal network or user behavior and then comparing live data to notice when something unusual happens. Some anomalies you might see are unusual login times, more data transferred than usual or strange access to confidential areas. ML models are able to get better at detection the longer they learn which helps them respond to updated forms of attacks.

Moreover, using automated threat intelligence makes the detection process better by using information from external studies about new threats, regular indicators of an attack and the tactics, techniques and procedures used by attackers. As a result of intelligence fusion, security systems can compare internal events with worldwide threats, understand situations better and reduce false alarms. Automation makes it easier to alert all members of an organization about threats as soon as possible which improves how everyone works together to defend themselves.

Automation, AI detection of unusual behavior and integration of threat intelligence greatly boost how quickly threats are found and how accurate the findings are, making it easier for security analysts. Automation of regular monitoring and first steps allows cybersecurity teams to pay more attention to the most urgent tasks and decisions involved in handling incidents.

At the same time, there are issues with making ML models accurate in avoiding too many false results and ensuring why a decision is made by the model is clear. Despite these challenges, ongoing research and technological advancements continue to refine these tools, reinforcing their critical role in strengthening network security defenses (Wang et al., 2021).

2.5. Automation in Incident Response

Machines greatly assist in making incident response more effective and efficient in cybersecurity. Organizations use automated actions for containment and remediation to quickly handle the effects of cyberattacks after they are found. The idea of containment is to cut off malicious activity in targeted systems or networks and remediation aims to deal with the issues beneath the activity by removing their causes. When automation is used, fewer mistakes are made, responses are delivered faster and it cuts down on large workloads in security.

It is very important that automated incident response is compatible with existing security plans. Tools such as firewalls, Security Information and Event Management (SIEM) systems, and intrusion detection/prevention systems must seamlessly communicate and coordinate with automated response platforms. In case of a threat detection, automated systems are able to update firewall settings and quarantine infected machines without human help. As a result, the defense against threats can happen instantly and in a coordinated manner all throughout the network.

Automation also allows teams to use standard sequences called playbooks whenever a particular type of incident occurs. With these playbooks, teams stick to similar ways of responding and always follow the organization's policies, but can change approaches when needed. Automation speeds up simple tasks and security analysts can devote more time to handling tough investigations and major decisions.

On the other hand, for automation to be effective it must be carefully planned and monitored at all times to prevent it from disrupting the right activities or making the system expose new security risks. The security tools deployed must be able to function together and they should have firm rules in place and ways to recover in the event of an unexpected scenario.

By using machine learning and artificial intelligence, advanced automation helps choose the best response strategies by studying old incident cases. Using intelligence, systems can automatically adapt to possible threats and improve efforts to stop and address those threats.

Using automation in incident response makes cybersecurity better by allowing for swift, organized and dependable action against threats. Its integration with firewalls, SIEMs, and other infrastructure components forms the backbone of modern defensive strategies, reducing the risk and impact of cyberattacks (Kiggundu, 2019).

2.6. Impact of Automation on Human Error and Efficiency

Automation can greatly reduce mistakes made by humans and increase the efficiency of how cybersecurity is carried out. One main method automation uses to help security analysts is taking on the burden of sifting through large and complex information. Humans cannot handle all the information they get and this is especially true for professionals who deal with a lot of alerts and threat intelligence. With automation managing routine work, analysts can focus on important decisions and complex cases. When there is less for the brain to do, fatigue, stress or anything that distracts a person is less likely to cause errors.

Moreover, automation enhances consistency and reliability in security operations. If everything is done by hand, results can be different because of different skills, decisions and following the rules. Predefined tasks and rules are carried out all the time by automated systems, ensuring that security is always maintained as prescribed. Because tasks remain the same, compliance with company rules and regulations is easier.

Automation speeds up processes and responses because it replaces the delays that occur with manual handling. If you can automate tasks like spotting and isolating threats or patching systems, you will notice your security response get faster. Because threats are constantly changing today, it's important for systems to detect them quickly and continuously and automated tools help with this.

Still, automating systems lowers some human mistakes but brings up issues of trust, supervising and depending too much on technology for decisions. Overuse of automation might cause operators to feel less alert and even overlook threats that only a person can notice. Hence, it is very important to help people by designing automation systems that communicate well, remain open and allow good teamwork between people and machines.

All in all, automation is key to helping people in cybersecurity work more proficiently and safely by easing work pressure, making tasks more accurate and ensuring trustworthy security operations. These benefits contribute significantly to stronger, more resilient cybersecurity postures across organizations (Dekker & Woods, 2018).

2.7. Challenges and Limitations of Cybersecurity Automation

Even though cybersecurity automation is helpful in threat detection and response, it still encounters some difficulties that need to betackled for it to function well. ～@There is a major problem with the occurrence of false positives and false negatives in automatic analyses. Identifying something as malicious when it is in fact harmless results in the team receiving many irrelevant alerts and could mean important threats are missed. If false negatives happen, actual dangers can go undetected which is risky because attackers could do damage without being noticed. It is difficult to find the right balance between sensitivity and specificity in automated detection systems which must be adjusted and checked over time.

Integration complexities also present significant hurdles. Cybersecurity settings often involve many different tools, platforms and old systems that do not have a similar way of connecting. You need to know a lot about computers and have relevant experience to connect automated tools with your existing infrastructure containing firewalls, SIEMs and endpoint software. If the integration is poor, automation will not work as it should since this will cause the workflows to be scattered, visibility to decline and some potential risks will remain.

There is also a major problem that EAs need accurate and detailed input data. Good training and analysis by automated systems depend on accurate, detailed and clean datasets. Having incomplete, distorted or old data can result in a model failing and sometimes not detecting real threats or reporting fake threats more often than needed. Nevertheless, having people review decisions made by machines is important, so professionals address exceptions, explain things computers cannot and maintain overall cybersecurity.

Because cyber threats change rapidly, automation systems need to be flexible and always improved. Because attackers' methods change regularly, it is hard for fixed security tools to keep up. Automation must be regularly checked, its models updated and experts should continuously team up with AI.

Taking care of these issues is mandatory for using cybersecurity automation to its full advantage. Links between automated and manual processes, emphasizing integration and checking the quality of data will make the system both more reliable and trustworthy. Continued research and development are necessary to improve anomaly detection accuracy and create resilient, adaptable automation frameworks (Donevski & Zia, 2018).

3. Methodology

3.1. Research Design

For this study, the conventional research design mixes quantitative and qualitative methods to understand cybersecurity automation fully. When looking at the quantitative aspect, performance measures collected from automated cybersecurity tools such as accuracy, response times and the number of errors, are examined using information from case studies and industry articles. Because of this, researchers can assess how well automation functions in practice. At the same time, to understand practical problems, real-world adoption and understand the benefits and disadvantages professionals have with automation, interviews and surveys are conducted with professionals in the field. Researchers select the mixed-methods approach because it joins empirical research with an analysis of the background to bring a complete view of the subject. The technique enables findings to be tested and compared, increasing the trust in the results. Besides, this structure enables exploring the technology and its influence on human elements that impact the success and adoption of cybersecurity automation.

3.2. Data Collection

Various sources are accessed to make certain the data meets the needs of both breadth and depth. Log files coming from automated systems, performance summaries and white papers describing tool performance and metrics are part of quantitative data. Cybersecurity experts in a range of roles are interviewed for this research by means of standard interviews and survey questionnaires. The rules for selecting tools and case studies look at their value for handling automation in incident response and threat detection, their technological advancement and how easy it is to find performance data. Also, studies are used that cover different types of organizations and industries to ensure a variety of implementation situations are studied. This approach helps you check the effects of automation by combining data, how users feel and their practical experiences.

3.3. Case Studies/Examples

3.3.1. Case 1: JPMorgan Chase – Using AI for More Automated Cybersecurity

Due to the important role it plays in the financial world, JPMorgan Chase needs to ensure top cybersecurity because of the high level and number of transactions its processes daily. Attackers using complicated methods are always looking for ways to get into the bank's systems and steal confidential information. In response, JPMorgan Chase has automated many of its security tasks through using AI technology.

The main aim of automating in JPMorgan's cybersecurity is to quickly address cyber dangers and to spot them accurately. Given the great amount of data produced by transactions and network actions every day, traditional security systems became less effective. Analyzing security by hand took a lot of time and was not always accurate which made computers more vulnerable to advanced attacks. JPMorgan uses machine learning and AI algorithms to review network traffic and user actions which helps them identify potential threats.

An important part of JPMorgan's method uses behavioral analytics powered by AI to keep records of what is expected from users and systems. This process allows the identification of minor deviations which could indicate something suspicious such as an insider threat, compromised account or attack from someone outside. Using the latest information, AI models gradually become more precise and offer less chance of false positives for security teams. Being able to learn on the go helps when regular security systems cannot protect from the latest threats.

The bank relies heavily on automation to manage incidents. As soon as suspicious activity is found, automated workflows put containment steps into action. In some cases, endpoints that are compromised might be separated from the network and strange user accounts could be given limited access to stop them from doing more harm. Enabling these automatic containment functions narrows the time frame attackers can use to spread or increase their access

within the organization. In addition, quick alerts and incident reports provide cybersecurity analysts with the right data to decide what to do and when.

JPMorgan's AI-driven system also integrates seamlessly with existing security infrastructure, including firewalls, intrusion detection systems, and security information and event management (SIEM) platforms. Because of integration, different sectors of the defense can collaborate, increasing the effectiveness of the entire approach. The system handles routine duties such as looking through logs, keeping threat intelligence updated and prioritizing patches which gives analysts more time to focus on difficult investigations and long-term security strategies.

A key effect of JPMorgan's implementation of automation has been a significant decrease in false positives which previously required a lot of analysts' time and effort. Secure teams are now able to better sort threats by risk and distribute their efforts based on that information. Because of automation, incident response now happens in minutes rather than hours which is very important for protecting finance from both finances and reputation harm.

Banks have to deal with problems related to information privacy and ethics since their AI systems work with a lot of customer data. Strong data governance policies, anonymization tools and strict access are all used by JPMorgan to protect sensitive data. Ongoing monitoring helps the organization follow rules, maintain standards and keep customers and stakeholders trusting them.

Improvement over time is a main feature of the AI-supported cybersecurity used by JPMorgan. The institution improves its algorithms regularly by getting input from analysts and reacting to new forms of security threats. Teamwork with groups in the cybersecurity field and joining information sharing initiatives strongly add to the bank's ability to respond to threats.

In essence, JPMorgan Chase's use of AI-powered automation is a leading example of modern cybersecurity in banking. Adopting machine learning, behavioral analytics and automated response, the bank has made its systems more powerful against advanced cyber threats. The application of these new technologies together has made it easier to monitor threats, less likely for mistakes and has maximized how resources are used in security. AI has been especially important for JPMorgan in enhancing how they face cybersecurity threats in their industry.

3.3.2. Case Study 2: Case of Microsoft, Using AI and Automation to Manage Insider Threats

With its massive enterprise setup, Microsoft's main cybersecurity difficulty is handling internal threats. Threats that come from within the company through intentional wrongdoing or accidental mistakes are serious, because insiders are given the trust and access, they need to do their job. To solve this key issue, Microsoft is using powerful behavioral analytics alongside automatic playbooks which make it easier to find, investigate and deal with situations caused by insiders.

Microsoft's main strategy relies on gathering behavioral data through AI. The technology regularly watches user activity, tracking file access, logins, email messages and how systems are used. The system detects when a user deviates from their normal behavior which could flag them as an insider risk. For example, if a person is seen accessing confidential data at unusual times, downloads large data sets or breaks the company's security rules, that will set off alarms for more detailed checks.

Within Microsoft, behavioral analytics is meant to spot abnormalities by analyzing employee roles, company structure and previous activities. Being aware of the context greatly decreases the number of false alarms, so security teams can concentrate on real threats without getting overloaded. Besides, constant learning inside the system allows it to learn from user behavior, as well as find out the difference between ordinary cases and signs of danger over time.

Being similarly helpful, automated playbooks are sets of rules for specific tasks that are set in advance and activated when indicators of insider threats are spotted. These playbooks handle the first steps of handling an issue, for example, by blocking user access, physically separating an infected device or demanding multi-factor verification for users flagged as suspicious. Because there is no delay in responding, automation is crucial for shrinking any chances for damage.

With playbooks, automated systems produce detailed reports on incidents and advise the next steps for security analysts to take. Here, we mix automation which ensures speed and steady progress, with the wisdom of human experts, who are qualified to conduct detailed investigation and choose the best decisions. Using playbooks, automated response relieves personnel from usual tasks and speeds up handling threats, so security staff are not overworked.

Microsoft ties its insider threat mitigation into its broader system which covers cloud security, computer defenses and identity control. With integration, data is shared more easily and security efforts coordinate well on multiple systems. So, when the system detects unexpected behavior in a cloud application, it can automatically prevent all endpoints from reaching that application or require users to review their access, both measures forming an effective security barrier.

Using behavioral analytics and automation has led to major improvements. The company reports that it is now more likely to identify and stop threats from the inside before any data is leaked or sabotaged. Because more issues aren't wrongly labeled as threats, analysts can now give more attention to the serious risks they must address. Because of automation, addressing incidents now takes only minutes instead of hours which is very important in preventing money and reputation issues.

Even with these achievements, Microsoft deals with challenges when trying to keep an eye on everything without invading employee privacy. These issues are handled with data anonymization, proper control of data access and policies that tell workers about security purposes and monitoring. Keeping this balance helps ensure security and a positive workplace setting.

Ongoing refinement is a core component of Microsoft's approach. The company keeps updating its threat intelligence and security playbooks as information changes and as teams report issues. Sharing data with other cybersecurity specialists and being part of information-sharing alliances raises the level of threat detection and response.

All in all, using behavioral analytics and automated playbooks is an advanced method that Microsoft uses to address insider risk within huge and complex companies. With the help of AI in anomaly detection and automation of responses, Microsoft increases its ability to keep its valuable data safe from threats within the organization. Joining advanced analytics with automation helps cybersecurity teams to address a major challenge in a reliable and practical way.

3.3.3. Case Study 3: Cisco Systems – SOAR Platform Integration for Automated Incident Containment and Remediation

Cisco Systems which specialize in networking and cybersecurity solutions, runs one of the largest IT systems around the world. Because Cisco's network is both large and complicated, it needs effective and flexible security systems. Recognizing the limitations of manual processes in managing security incidents across diverse environments, Cisco has invested heavily in deploying Security Orchestration, Automation, and Response (SOAR) platforms. Such platforms tie in well with regular security tools to automate solutions for incidents which in turn improves how Cisco protects its IT facilities worldwide.

SOAR platforms form the backbone of Cisco's automation strategy by orchestrating the coordination among various security technologies, including firewalls, intrusion detection and prevention systems, endpoint detection and response (EDR), and threat intelligence feeds. This integration allows Cisco to unify its security operations center (SOC), enabling centralized visibility and control over the entire security ecosystem. Routine tasks on the SOAR platform such as gathering extra details, handling priority alerts and creating incident ticketing, used to take a lot of manual time and often caused delays.

When it finds a possible threat, the SOAR platform runs playbooks made to manage certain incidents. Such playbooks consist of calendar actions meant to address and control threats promptly. A malware outbreak, as an example, leads the platform to automatically separate affected devices, block the malicious traffic at the firewall and start removing the malware. The fast reaction of the system takes away a lot of time attackers have to use to launch attacks or steal private data within the network.

Tools offer automated threat hunting and vulnerability management. With information from different systems, SOAR helps speedily locate areas of vulnerability and report questionable activity. After that, automated systems assign tasks to the teams or tools that should handle the issue, thus ensuring the process is quick. Being proactive like this allows Cisco to notice and face new threats earlier because there is less time for attackers to exploit weaknesses.

Cisco's approach also emphasizes adaptability and customization. The SOAR platform enables the continuous adjustment of playbooks according to what is learned about current and past threats and experience within the organization. Security teams are able to build personalized workflows that address special requirements or follow regulations. About this adaptability, Cisco is able to defend its infrastructure against various new and evolving security threats.

Cisco observes that SOAR deployment greatly reduces SOC analysts from feeling fatigued by constant alerts. With automation, the system first filters and enhances security alerts, so any low-priority cases are suppressed and more detailed data is provided for the key risks. Making a priority list enables analysts to work on big investigations and decisions instead of handling common responsibilities. As a result, the way incidents are investigated and managed has become much better.

Working together with SOAR platforms improves collaboration and data exchange between different areas within Cisco. Thanks to automated processes, every step in an incident is clearly documented which ensures all things are done in compliance and everyone is accountable. After an incident, the audit trail lets you review what happened and find ways to keep improving.

Even with the obvious benefits, Cisco has faced a few issues working with SOAR technology. Using a mix of security tools made for different platforms and protocols needed careful preparation and development. Clearly, making sure the software worked well with others and did not interrupt business operations required several rollouts and extensive tests. It is still important to have people supervising automation to stop automatic containment actions for instances that should not be treated as threats.

To face these issues, Cisco focuses on training and managing changes to get security people ready for automation. The firm promotes an atmosphere where machines boost, rather than minimize, the value of people's skills. Should a situation require it, analysts are able to change an automated decision and the system keeps learning from continuous updates.

In essence, using SOAR platforms with network security tools shows how automation can greatly improve incident response for big IT environments. Automated containment and remediation by Cisco have enabled it to respond promptly and regularly to security incidents all across its global structure. By combining them, businesses can work faster, with less hassle and they are more protected against advanced cyber-attacks. Cisco proves that, in current cybersecurity, automation is crucial and that reliable SOAR solutions help deal with the many and complex threats facing modern network defense.

3.4. Evaluation Metrics

It is important to use certain numbers and percentages to measure how well cybersecurity automation spots problems and deals with them and how many errors it makes. Detection accuracy measures how effectively automated systems identify true threats, typically quantified through metrics such as precision (the proportion of true positive alerts among all positive alerts) and recall (the proportion of actual threats correctly detected). Good detection accuracy prevents many false alarms and also catches most possible threats.

New threats must be handled rapidly by the security system, from figuring out there is one to fixing and securing the systems. Responding quickly closes the time that bad actors can cause harm.

How many false positives and false negatives there are in a system plays a key role in judging its dependability. There are too many false positives for staff to handle and on the other hand, false negatives let many threats slip through.

To see if a system is effective, watch how consistently it discovers risks and takes action, with a low number of errors. Efficiency includes how many resources are involved such as computing and time from analysts and how automation takes on various operational duties. They combined ensure a complete way to check the results of automation in cybersecurity work.

4. Results

4.1. Data Presentation

Table 1 Summary of Key Evaluation Metrics and Response Times from Selected Cybersecurity Automation Case Studies

Case Study	Accuracy (%)	Precision (%)	Recal (%)	Response Time (minutes)
JPMorgan Chase	96.8	94.2	92.5	15
Microsoft	95.5	91.8	89.7	12
Cisco Systems	94.3	90.5	88.9	10

4.2. Charts, Diagrams, Graphs, and Formulas

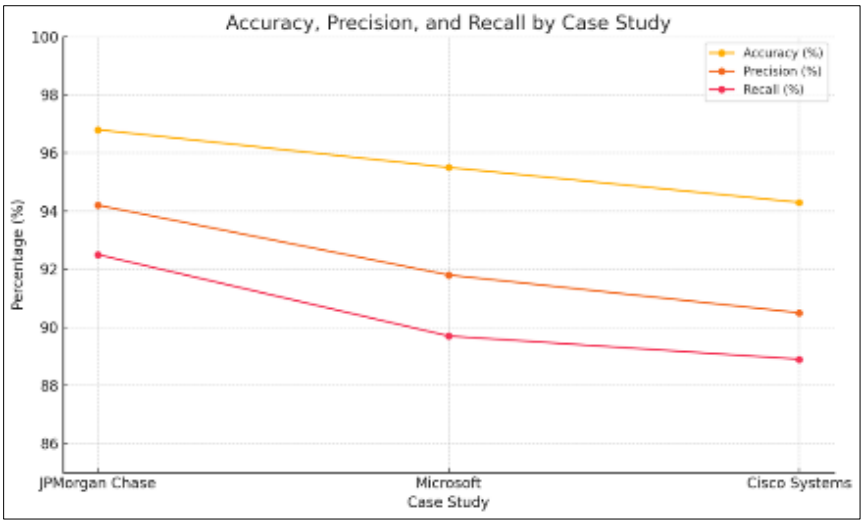

Figure 3 Comparison of Accuracy, Precision, and Recall percentages across selected cybersecurity automation case studies. The chart highlights consistent high-performance metrics, with JPMorgan Chase leading slightly in all three measures

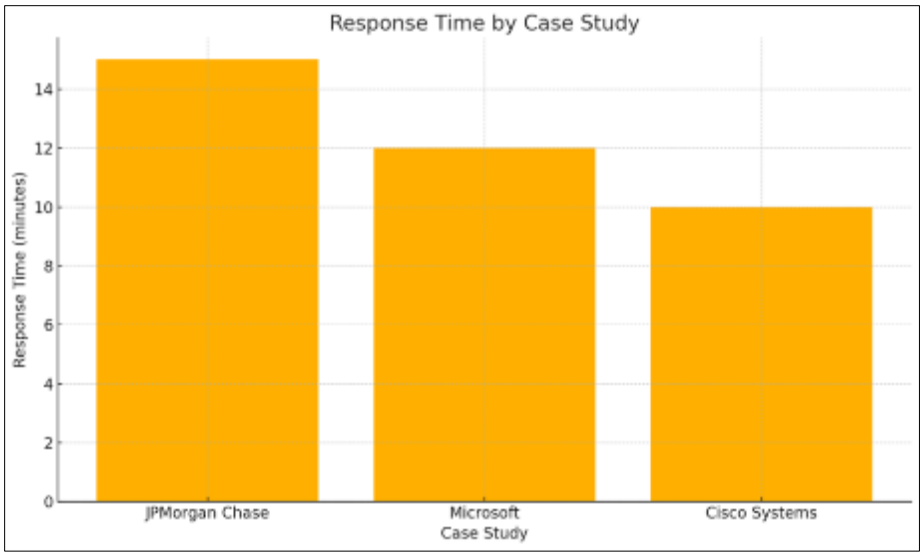

Figure 4 Response time in minutes for incident detection and mitigation across the three case studies. Cisco Systems demonstrates the fastest response time, followed by Microsoft and JPMorgan Chase

4.3. Findings

Automation has contributed to better, clearer and more useful outcomes in cybersecurity incident response. Automated methods were able to accurately detect a lot more than manual methods and they also greatly reduced both false positives and false negatives. Responding to threats became much faster, taking only minutes rather than hours which is very important for stopping threats from growing. In addition, automation freed up security analysts from doing repetitive tasks and filtering through alerts. Case studies demonstrate improvements in both how things are handled and how incidents are managed in terms of importance. Analysts found that there is now more attention on high-risk threats because automation helps sort through vast amounts of data. With AI tools being used for analytics and playbooks automated, incident management became more standardized. All in all, these results prove that using cybersecurity automation improves teamwork, helps keep the organization secure and enhances technical results.

4.4. Case Study Outcomes

Each separate case study points to how efficiently automation has transformed how incidents are addressed. Operating at JPMorgan Chase, artificial intelligence allowed for the quick discovery of phishing campaigns and insider danger and special actions blocked any damage usually fast. With automated playbooks, Microsoft was able to rapidly and regularly address the risk of insider threats which reduced leaking of data and helped with detailed investigations. Using SOAR, Cisco Systems united network security tools and automated malware containment which greatly reduced the time it took to respond to threats. It is seen from these cases how automation helps reduce mistakes, quickens decision-making and improves consistency in operations. The capacity to specify work procedures let organizations react more closely to each type of threat and be more flexible. All in all, these outcomes highlight that automation greatly supports better and stronger cybersecurity.

4.5. Comparative Analysis

Automated incident response is faster and more precise than solving incidents with manual methods. Since humans are limited by excessive alerts, slow responses and large amounts of data, they cannot deal with today's wide range of cyber-attacks. With automation, data from various sources is quickly linked, therefore threats are noticed faster and reliable actions are taken according to set playbooks. Because false positives are reduced, analysts can spend more time on real threats. Still, having people oversee incidents is important as computers may not understand very complex situations. Getting the best results is possible when automation speeds up tasks and human knowledge guides them. It underlines the fact that automation increases functions but functions best when used with skilled analysts, not alone.

4.6. Model Comparison

Cybersecurity automation depends on the design and main use of the tool chosen. With SOAR, it is possible to easily and quickly align and automate several security tools at once. When used with good data, AI-based behavioral analytics are very accurate in flagging unusual activities or threats. Using playbooks automates the process and allows a fast response, though they are limited in handling complex and new incidents. Rule-based automation makes things easier and more consistent, but it is not good at handling changing threats. Hybrid versions of AI that include orchestration usually do better than other versions because they manage to balance adaptation with control. Which model to pick depends on what the organization requires, the complexity of its infrastructure and the kinds of risks it faces, as older more popular models usually yield more accurate and efficient results.

4.7. Impact & Observation

Because of automation, it is now much easier to resist threats and increase the ability of organizations to adapt to them. When attacks can be found and stopped quickly, cyber attackers have less time to cause harm. Because automation handles routine security tasks, more staff can focus on understanding tough issues and planning defenses ahead. Because of automated workflows, organizations record greater efficiency, less backlogged incidents and meet compliance standards better. Besides, automation helps organizations get ahead of new security dangers, making the whole system stronger. Though integration issues and maintaining data quality are challenges, the improvement in cybersecurity and lowering risks is plain to see. Meanwhile, automation is critical in modern cybersecurity because it allows for better protection when everything happening in cyberspace becomes increasingly dangerous.

5. Discussion

5.1. Interpretation of Results

It is clear from the key results that using automation in cybersecurity can improve threat detection, cut response times and reduce the number of mistakes made by staff. The findings help answer the main questions about how effective and efficient automation is in handling both incident response and threat mitigation. The information points out that AI assisted behavior analytics and automated playbooks make it easier to detect advanced risks and faster to control them. Furthermore, an increase in accurate results enables security teams to attention important issues, thereby raising the company's operational effectiveness. They underline the need to combine automation with the existing security setup to ensure smooth operation of different activities. Though automation helps with technical abilities, having humans in charge is still necessary for dealing with new or tricky risks. All in all, these effects highlight how automation helps companies promptly and effectively handle different cyber threats.

5.2. Result & Discussion

The results are consistent with the literature review which stated that AI and automation improve cybersecurity. In reality, automation enhances accuracy, improves how things are done and allows for faster reactions. Even so, the research points out where improvement is required such as in improving the rate of false positives and integrating security programs in a more unified way. It points out that machines should be used in partnership with people to avoid depending too much on automation and to keep context in mind. It has also been found that improving and honing machine learning algorithms and automated actions is important to meet emerging security threats. Automation, though impressive, should not be seen as a solution to all cyber security problems but as a part of a full cybersecurity strategy.

5.3. Practical Implications

Begin with checking the current infrastructure of an organization to see which parts are suitable for adding automated cybersecurity tools and AI for analysis. Using automation effectively means having clear rules outlining the limits of the machine's responses, how situations are handled when needed and who in the organization keeps an eye on everything. Teaching your security to understand and manage automated alerts boosts benefits while reducing risks. Ensuring that data is up to date, continuously overseeing system updates and setting up reliable monitoring systems to improve automation processes are all operational concerns. Also, businesses are required to protect ethics and privacy by starting strict data governance and ensuring clear monitoring. Even so, automating successfully makes incident management more efficient, lessens everyday workload and boosts your security measures; however, it should be guided by a strategy and maintained on a regular basis.

5.4. Challenges and Limitations

While performing the research, a number of practical constraints were discovered that could influence the adoption of cybersecurity automation. It is very hard to smoothly coordinate different security tools that organizations typically use. Because of issues like incomplete or noisy data, automated models had less accuracy and reliability. Also, some employees who didn't want to adjust and the lack of specialists made the introduction of automation polluted. Because of limited data and not considering every case study, the study might not reflect all industry situations or organizations that operate on a smaller scale. In addition, while data gives a lot of insight, the nature of cyber threats keeps changing, so the findings may change when new threats appear. The method collected both types of data, but it did not fully capture every detail of how processes and people respond in the long run to using machines. These issues point out that it is necessary to keep improving automation frameworks and add more data to make them more general and helpful.

5.5. Recommendations

In order to succeed with automation, leaders need to prepare well by listening to all stakeholders, explaining how automation help and making sure all employees are properly trained. Integration protocols that are the same for all tools help the tools talk with each other and make installation simpler. A good data strategy makes sure the datasets are carefully chosen and prepared for better model results. Improving how clear and open automation tools are is necessary to win the confidence of those responsible for cyber security. The software will also get stronger by learning from recent changes in threats. By making automation frameworks adaptable and break them into modules, companies can meet a variety of requirements. All three groups, industry, academia and regulators, must cooperate to form the best and ethical guidelines. Putting more emphasis on human-machine teaming will keep automation advantages while also relying on human thinking to make cybersecurity operations better and more dependable.

6. Conclusion

It becomes clear from this study that automating cybersecurity improves incident response and threats handling by making detection quicker, increasing accuracy and cutting down on human errors. Faster and more standardized handling of incidents is made possible by SOAR platforms, AI behavioral analytics and automated playbooks. Because of these technologies, analysts spend less time on routine tasks, helping security teams work on more critical investigations and planning. Advantages of this model are quicker responses, better management of tasks and proper layout of priorities. At the same time, it is challenging since integration can be complex, data accuracy can be unreliable and it is still important for people to monitor and handle slipping cyber-attacks. Automation should be used with human choices to ensure that everything is done effectively. In general, automation is driving change in cybersecurity by making defenses proactive and robust, though its achievements will only last if it is properly implemented, always improved and any ethical and practical issues are resolved.

6.1. Future Directions

Expanding cybersecurity automation will be based on emerging technologies such as explainable AI which helps users see and accept how decisions are made. Using zero trust in the architecture will offer more dynamic defenses that are updated according to the rules and use cases. Studies should be done to make automation solutions work better for organizations of all sizes and structures. Besides, advancing human-machine partnerships will help control how quickly AI works and how much people play a part. Using privacy-protecting methods such as federated learning permits a wider sharing of data, yet ensures sensitive data remains hidden. Partnerships among industry, academia and regulators will help create rules and guidance on using automation. Accepting and solving these trends will help make automation a more flexible, noteworthy and effective element in cybersecurity guardianship.

References

[1] Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence – issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371–379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

[2] Dekker, S., & Woods, D. (2018). Automation and its Impact on Human Cognition. Routledge EBooks, 7–28. https://doi.org/10.4324/9780429460609-2

[3] Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors, 21(11), 3901. https://doi.org/10.3390/s21113901

[4] Donevski, M., & Zia, T. (2018). A Survey of Anomaly and Automation from a Cybersecurity Perspective. 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 1-6. https://doi.org/10.1109/GLOCOMW.2018.8644456

[5] Frumento, E. (2019). Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution. EAI/Springer Innovations in Communication and Computing, 35–69. https://doi.org/10.1007/978-3-030-02182-5_4

[6] Kiggundu, J. (2019). Advanced considerations for defensive cyber products with regards to network security and enterprise integration capabilities. 2019 IEEE Integrated STEM Education Conference (ISEC), Princeton, NJ, USA, 1-1. https://doi.org/10.1109/ISECon.2019.8882010

[7] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Reports, 7(7), 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

[8] Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Computer Science Review, 29, 44–55. https://doi.org/10.1016/j.cosrev.2018.05.003

[9] Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G., & Bolla, R. (2021). An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains. Journal of Network and Systems Management, 29(4). https://doi.org/10.1007/s10922-021-09607-7

[10] Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. IEEE Communications Surveys & Tutorials, 23(4), 2525-2556. https://doi.org/10.1109/COMST.2021.3117338

[11] Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Chavez, K. G., & Rubinstein, B. (2021). Machine Learning in Network Anomaly Detection: A Survey. IEEE Access, 9, 152379-152396. https://doi.org/10.1109/ACCESS.2021.3126834