



## **AZURE SENTINEL AUTOMATION AND PLAYBOOKS**

**Mrs.R. Sivagami** Assistant Professor Department of Information Technology, SNS College of Engineering, Coimbatore, Tamil Nadu 621107, India, nan24.kumar@gmail.com

**T. Sridhar** Department of Information Technology, SNS College of Engineering, Coimbatore, Tamil Nadu 621107, India, sridharthirupathi199@gmail.com

**R. Tamilselvan** Department of Information Technology, SNS College of Engineering, Coimbatore, Tamil Nadu 621107, India, tamilselvanhacker320@gmail.com

**L. Nivetha** Department of Information Technology, SNS College of Engineering, Coimbatore, Tamil Nadu 621107, India, lnivetha935@gmail.com

**Mr. R. Vinothkumar** Information Security Analyst, Fortuna Identity Pvt Ltd, Hyderabad, TG, India – 500033.

### **Abstract:**

Azure Sentinel is a security information and event management (SIEM) solution that is cloud-native and offers intelligent security analytics at a cloud scale for your entire business in today's world. Security operations teams need to improve their efficiency by streamlining their procedures and automating the actions they take in response to the rising volume of security alerts and incidents. Purplish blue Sentinel mechanization and playbooks offer an answer for this test by empowering security groups to robotize routine errands and coordinate occurrence reaction exercises. Automation and playbooks from Azure Sentinel are potent answers to the growing difficulty of managing security incidents in a threat landscape that is both complex and rapidly changing. Security teams can increase their effectiveness, shorten response times, and better safeguard their organizations from cyber threats by automating routine tasks and orchestrating incident response procedures. Security teams can tailor a solution that meets their organization's specific requirements with Azure Sentinel's adaptability and customization.

Keywords: Azure Sentinel, SIEM, Automation, Playbooks, Incidents, Events, Security.

### **I INTRODUCTION:**

It is becoming increasingly challenging for security teams to keep up with the ever-increasing number of threats and attacks in the world of cybersecurity. Security examiners are confronted with a staggering volume of safety cautions, and the most common way of exploring and answering episodes can be tedious and work escalated. Automation and orchestration come into play here. Azure Sentinel is a cloud native SIEM that offers scalable security analytics. It permits associations to gather, examine, and follow up on security information from across their venture and gives a unified stage to overseeing security episodes. Security teams can automate routine tasks and orchestrate incident response activities with Azure Sentinel automation and playbooks, which can help security analysts focus on more complex tasks and reduce their workload. The automation features of Azure Sentinel include automated incident creation, alert suppression, and response actions. Organizations can reduce the amount of time and effort required to investigate and respond to incidents by using automated incident creation, which enables them to automatically create incidents based on predefined criteria. Organizations can reduce the number of alerts that security analysts must investigate by automatically suppressing alerts that are neither relevant nor actionable. Organizations can automate certain security events, such as quarantining a compromised device or resetting a user's password, with automated response actions. In response to a particular security event, Azure Sentinel playbooks provide a set of predefined actions that can be conducted.



Playbooks can automate a wide range of security tasks, including threat hunting, incident response, and remediation, and they can be customized to meet an organization's specific requirements. Azure Sentinel Automation and Playbooks are two powerful features that allow security teams to automate repetitive and time-consuming security tasks, such as alert triage, incident response, and threat hunting. Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) platform from Microsoft that provides intelligent security analytics and threat intelligence across enterprise networks. It is designed to help security teams detect, investigate, and respond to threats using a centralized, cloud-based platform. The Azure Sentinel Automation and Playbook project builds on this foundation by providing a set of tools and solutions to automate security operations and incident response. The project includes a range of pre-configured playbooks, automation scripts, and integrations with other Microsoft security tools, all designed to help security teams improve their response times and identify threats more effectively. The project includes a range of playbooks that can be customized to meet the specific needs of an organization. These playbooks can be triggered automatically by specific security events, such as a data breach or a phishing attempt. Once triggered, the playbook can perform a range of actions, such as sending alerts to security teams, blocking network traffic, or initiating remediation processes. The Azure Sentinel Automation and Playbook project also includes a range of automation features that can help security teams streamline their operations and respond more quickly to security incidents. These features include automated data collection, analysis, and threat intelligence, all of which can help identify potential threats more quickly and accurately. In addition to these features, the Azure Sentinel Automation and Playbook project also includes a range of integrations with other Microsoft security tools and services, such as Microsoft Defender ATP and Azure Active Directory. These integrations allow security teams to get a more complete view of their security environment and respond to threats more effectively. The Azure Sentinel Automation and Playbook project provides a comprehensive set of tools and solutions to help security teams automate their operations, respond more quickly to security incidents, and protect their organizations against emerging threats. Automation in Azure Sentinel involves the use of logic apps, functions, and other Azure services to automate security workflows and processes.

This can help organizations to reduce the time and effort required to respond to security incidents, allowing security teams to focus on more strategic tasks. For example, automation can be used to automatically triage and respond to low-level alerts, freeing up security analysts to focus on more complex incidents. Playbooks in Azure Sentinel are pre-defined workflows that automate specific security tasks. These workflows can be customized to meet the specific needs of an organization, or they can be used as-is to automate common security tasks, such as incident response, threat hunting, and compliance reporting. Playbooks can be triggered automatically based on certain conditions, such as the receipt of a specific alert, or they can be triggered manually by a security analyst. Azure Sentinel provides a range of built-in Playbooks that cover a range of security scenarios, including incident response, threat hunting, and compliance reporting. These Playbooks can be customized to meet the specific needs of an organization, or they can be used as-is to automate common security tasks. Azure Sentinel Automation and Playbooks are powerful features that can help organizations to automate repetitive and time-consuming security tasks, allowing security teams to focus on more strategic tasks. By automating security workflows and processes, organizations can improve their security posture, reduce the time and effort required to respond to security incidents and improve their overall security operations.

## II. RELATED WORKS

"Azure Sentinel Playbook Automation for Security Operations" by Microsoft: This white paper provides an overview of how to automate tasks, use pre-built playbooks, and create custom



playbooks in Azure Sentinel. The paper covers topics such as Playbooks architecture, Playbooks types, Playbooks authoring experience, and Playbooks testing and deployment.

"Automating Incident Response with Azure Sentinel Playbooks: It provides a detailed overview of how to automate incident response with Azure Sentinel Playbooks. The post covers topics such as how to set up custom Playbooks, how to integrate with other Azure services, and how to handle alert notifications.

"Automating Threat Intelligence with Azure Sentinel": It provides an overview of how to automate threat intelligence with Azure Sentinel. The post covers topics such as how to create a threat intelligence feed, how to automate alert creation, and how to use the feed to enrich security data.

"Azure Sentinel Playbooks – Creating Your Own: It provides a step-by-step guide to creating custom Azure Sentinel Playbooks. The post covers topics such as how to use Logic Apps, how to create custom actions, and how to manage Playbook versions.

"Automating Security Operations with Azure Sentinel": It provides an overview of how to automate security operations with Azure Sentinel. The webinar covers topics such as how to use pre-built Playbooks, how to create custom Playbooks, and how to integrate with other Azure services.

"Azure Sentinel and Playbooks - Demystified": It provides an overview of Azure Sentinel and Playbooks. The post covers topics such as how to set up a basic Playbook, how to use Azure Functions to enrich data, and how to handle automatic remediation.

"Automating Azure Sentinel with PowerShell": It provides an overview of how to automate Azure Sentinel with PowerShell. The post covers topics such as how to create custom Playbooks, how to automate data ingestion, and how to handle alert notifications.

"Azure Sentinel Playbooks Best Practices": It provides best practices for creating and managing Azure Sentinel Playbooks. The post covers topics such as how to create reusable Playbooks, how to use the Azure Sentinel API, and how to handle different types of data.

"Azure Sentinel Automation - Hunting and Response": It provides an overview of how to use Azure Sentinel for hunting and response. The post covers topics such as how to create custom Playbooks, how to use KQL queries to search for threats, and how to handle incident response.

"Automating Azure Sentinel with Microsoft Power Automate": It provides an overview of how to automate Azure Sentinel with Microsoft Power Automate. The post covers topics such as how to create custom Playbooks, how to automate data ingestion, and how to handle alert notifications.

"Automating Azure Sentinel Playbooks with Python": It provides an overview of how to automate Azure Sentinel Playbooks with Python. The post covers topics such as how to create custom actions, how to use the Azure Sentinel API, and how to handle different types of data.

"Azure Sentinel Automation: Best Practices for Streamlining Incident Response": It provides best practices for streamlining incident response with Azure Sentinel automation.

### **III. PROPOSED SYSTEM**



Azure Sentinel Automation and Playbook project is an automated security operations center (SOC) that leverages the capabilities of Azure Sentinel to detect and respond to security threats in real time. The system uses a combination of Azure Sentinel Playbooks, Azure Functions, and Logic Apps to automate security operations and reduce the workload of security analysts.

The system architecture consists of the following components:

**Azure Sentinel:** This is the cloud-native SIEM and SOAR solution from Microsoft that collects, analyzes, and correlates security data from different sources.

**Azure Functions:** This is a serverless compute service that enables the execution of code in response to events or triggers.

**Logic Apps:** This is a workflow automation service that enables the creation of custom workflows and integrations between different Azure services and external systems.

**Playbooks:** These are pre-built or custom workflows that automate different security operations tasks, such as alert triage, incident response, and threat hunting.

**Graph API:** This is the RESTful API used to interact with Azure Sentinel data and resources.

The proposed system uses Azure Sentinel to ingest security data from different sources, such as logs, network traffic, and user activity. The data is then processed and analyzed using Azure Sentinel's built-in machine learning and threat intelligence capabilities. When a security threat is detected, Azure Sentinel triggers a Playbook that automates the response actions based on predefined rules and conditions.

The Playbooks are created using Azure Functions and Logic Apps, which enable the execution of custom code and workflows. The Playbooks can be triggered by different events, such as a new alert, a scheduled task, or a user action. The Playbooks can also interact with other Azure services and external systems using the Graph API.

The proposed system reduces the workload of security analysts by automating repetitive and time-consuming security operations tasks. The system enables faster incident response times, reduces false positives, and provides a more efficient and effective security posture.

#### **IV TECHNOLOGIES USED:**

Azure Sentinel, Azure Logic Apps, Azure Event Grids, Azure Functions, Azure Storage, Azure Active Directory, Azure Monitor, PowerShell, Azure Playbooks, Data Connectors, Azure Data Factory, Azure Data Grid. By using these technologies, we can create Automated rules that can be modified for Automation Purposes.

#### **OVERVIEW OF AZURE SENTINEL:**

An Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) solution from Microsoft. It provides intelligent security analytics at scale, making it easier for security professionals to identify and respond to threats in real-time.

At its core, Azure Sentinel is a centralized platform for ingesting, analyzing, and correlating security event data from various sources across an organization's environment, such as servers, endpoints, applications, cloud services, and network devices. This data can come from both Microsoft and non-Microsoft sources, including popular third-party security products.



Azure Sentinel uses advanced artificial intelligence (AI) and machine learning (ML) algorithms to detect and respond to security incidents in real time. It also provides advanced features such as threat intelligence, security orchestration, and automated response workflows that help organizations quickly identify and respond to security threats.

One of the key benefits of Azure Sentinel is its scalability. It is designed to handle large volumes of data, making it ideal for organizations of all sizes, including those with large and complex IT environments. Azure Sentinel also integrates with other Azure services, such as Azure Active Directory, Azure Security Centre, and Azure Information Protection, providing a seamless end-to-end security solution for organizations.

Azure Sentinel provides a centralized dashboard that displays all security events, alerts, and incidents, making it easier for security teams to manage their environment. The platform also provides customizable workbooks that enable security professionals to create dashboards and visualizations to gain deeper insights into security threats and trends.

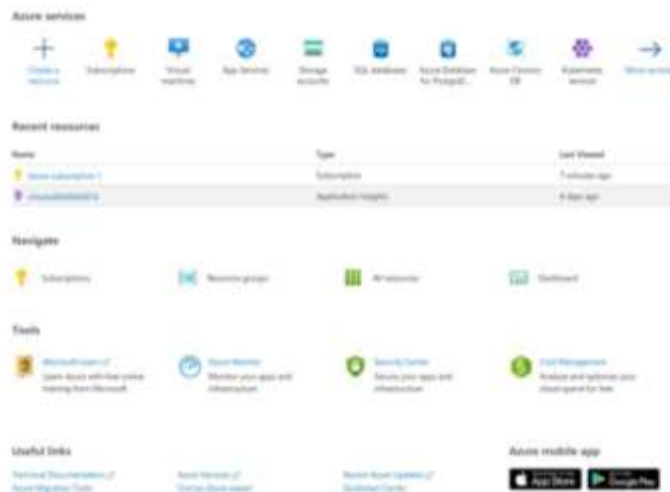
Azure Sentinel is a powerful and scalable SIEM solution that helps organizations to detect, investigate, and respond to security threats quickly and effectively. Its advanced features, such as threat intelligence and security orchestration, make it a comprehensive security solution that can help organizations to better manage their security posture.

## V CREATING AZURE SENTINEL:

### Steps using Azure Portal:

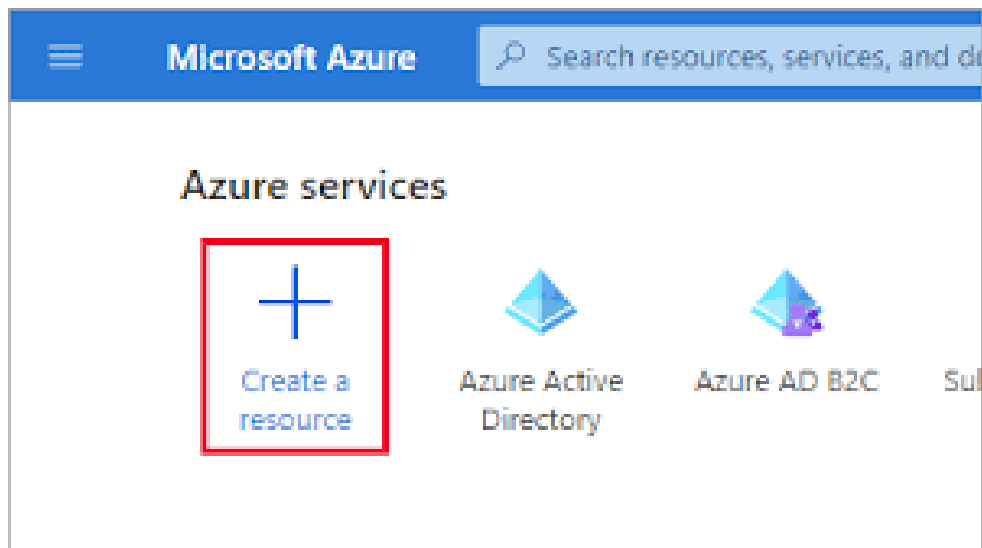
**Step 1:** Use a valid credential to Login into the Azure Portal:

Fig. 5.1.1 Open Azure Portal.



**Step 2:** Select Create a resource link from the Azure Portal to create a new resource for Tenant:

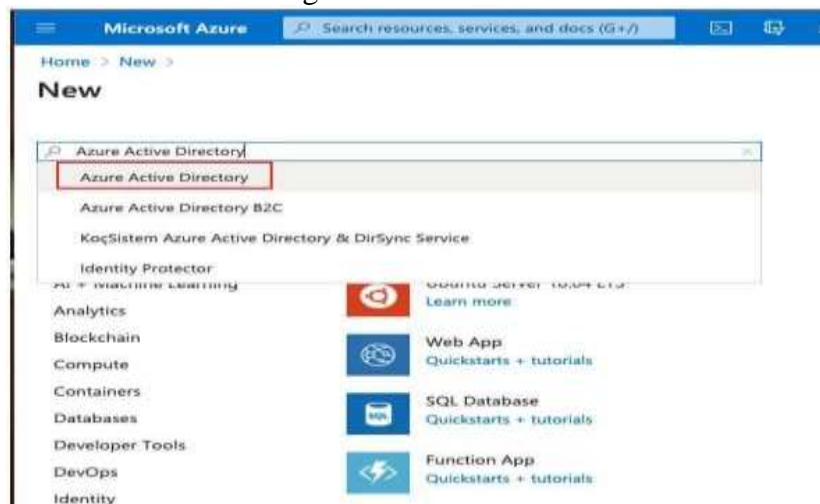
Fig. 5.1.2 Create Recourses



Click on Create a Resource and enter the details.

**Step 3:** In the Search, the Marketplace field enter Azure Active Directory:

Fig. 5.1.3 Search Bar



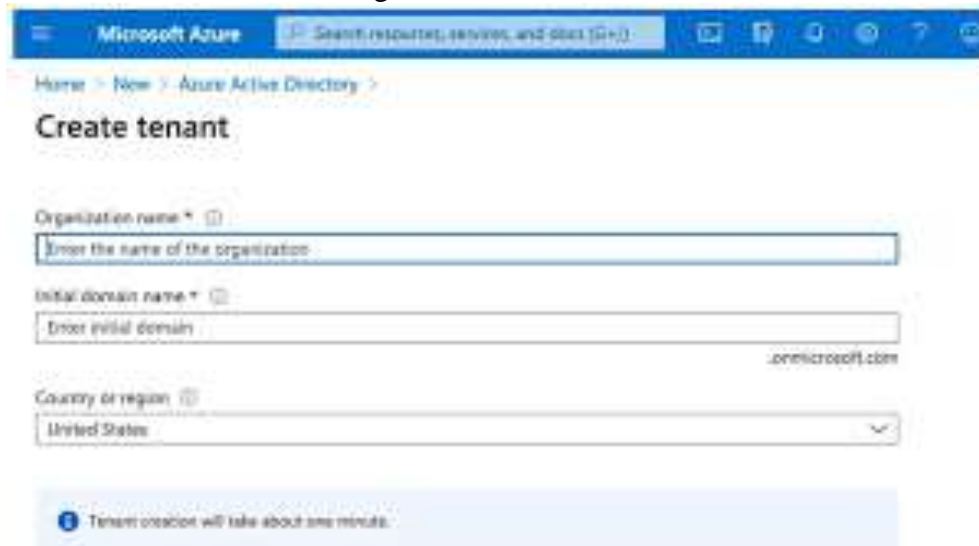
**Step 4:** Click on the Create link from the Azure Active Directory:

Fig. 5.1.4 Azure AD



**Step 5:** Now, a new page will open with Create Tenant:

Fig. 5.1.4 Azure Tenant



**Step 6:** Enter the tenant detail below and Select Create button to create a new Tenant:

- **Organization Name:** Enter the name of the directory for the organization name.
- **Initial Domain Name:** The user can add a customized domain name, and the default domain name is onmicrosoft.com.
- **Country or Region:** The user can select the Geo-region as per the location.

#### VI WORKING OF AZURE SENTINEL:

Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) solution provided by Microsoft. It collects and analyses security data from various sources, such as applications, servers, devices, and network devices. The platform uses advanced analytics and machine learning to detect and respond to security threats in real time.

The working of Azure Sentinel can be broadly categorized into the following steps:

1. **Data Collection:** Azure Sentinel ingests data from various sources, such as Azure Active Directory, Azure Security Center, Azure Data Lake Storage, Microsoft 365, and other third-party security solutions. The platform supports a wide range of data connectors that allow security teams to collect data from different sources. The data collected includes logs, events, alerts, and telemetry data.
2. **Data Enrichment:** Once the data is collected, Azure Sentinel enriches it with additional information, such as geolocation, device type, user identity, and threat intelligence. This enrichment helps in providing context to the data, making it easier for security analysts to investigate security incidents.
3. **Detection:** Azure Sentinel uses advanced analytics and machine learning algorithms to detect security threats in real time. The platform provides a range of built-in detection rules and templates that can be customized based on specific security requirements. Azure Sentinel also allows security analysts to create their own detection rules and alerts.
4. **Investigation:** When a security threat is detected, Azure Sentinel provides security analysts with a range of tools to investigate the incident. The platform provides a single pane of glass for security analysts to view and analyze the collected data. The platform also supports interactive query tools, such as Kusto Query Language (KQL), which allows analysts to search and analyze large datasets.
5. **Response:** Azure Sentinel provides security automation and orchestration features that allow security teams to respond quickly to security incidents. The platform enables security analysts to



automate routine tasks and create playbooks to streamline incident response processes. Playbooks can be triggered automatically based on certain conditions or manually by a security analyst.

6. Reporting and Analytics: Azure Sentinel provides a range of built-in reports and dashboards that provide insights into security incidents and trends. The platform also supports custom reporting and analytics, allowing security teams to create their reports and dashboards based on specific requirements.

Azure Sentinel provides end-to-end security analytics and threat intelligence for the enterprise. The platform uses advanced analytics and machine learning to detect and respond to security threats in real-time, while also providing a range of tools to investigate security incidents and respond quickly to security threats.

## **VII. PLAYBOOKS:**

Playbooks are a key feature of Azure Sentinel, which is a cloud-native Security Information and Event Management (SIEM) solution provided by Microsoft. Playbooks are used to automate routine security tasks and streamline incident response processes, allowing security teams to focus on more critical tasks.

In Azure Sentinel, playbooks are created using a drag-and-drop interface, making it easy for security analysts to create and customize their playbooks. Playbooks can be triggered automatically based on certain conditions, such as a specific event occurring, or they can be triggered manually by a security analyst.

Playbooks in Azure Sentinel can be used to automate a wide range of security tasks, such as creating tickets in a ticketing system, sending email notifications to the security team, and disabling user accounts. Playbooks can also be used to contain threats, such as isolating a compromised device from the network or blocking a malicious IP address.

Playbooks can be customized to meet specific security requirements. For example, a playbook can be configured to trigger only when a specific user is affected or when a certain number of failed login attempts occur within a certain time. Playbooks can also be combined with other features of Azure Sentinel, such as advanced analytics and machine learning, to create highly effective security workflows.

One of the benefits of using playbooks in Azure Sentinel is that they provide consistency in incident response processes. This reduces the risk of errors or omissions, which can occur when tasks are performed manually. Playbooks can also significantly reduce the time taken to respond to security incidents, enabling security teams to focus on more critical tasks.

Another benefit of using playbooks in Azure Sentinel is that they can be shared between different security teams. This can help to improve collaboration and increase efficiency, as teams can reuse playbooks that have already been created and tested.

In summary, playbooks are a powerful feature of Azure Sentinel that allows security teams to automate routine security tasks and streamline incident response processes. By providing consistency in incident response processes and reducing the time taken to respond to security incidents, playbooks can help to improve the overall security posture of an organization.

If We want to stop potentially compromised users from moving around your network and stealing information, we can create an automated, multifaceted response to incidents generated by rules that detect compromised users. You start by creating a playbook that takes the following actions:

1. When the playbook is called by an automation rule passing it an incident, the playbook opens a ticket in ServiceNow or any other IT ticketing system.
2. It sends a message to your security operations channel in Microsoft Teams or Slack to make sure your security analysts are aware of the incident.
3. It also sends all the information about the incident in an email message to your senior network admin and security admin. The email message will include Block and Ignore user option buttons.





4. The playbook waits until a response is received from the admins, then continues with its next steps.
5. If the admins choose Block, it sends a command to Azure AD to disable the user, and one to the firewall to block the IP address.
6. If the admins choose Ignore, the playbook closes the incident in Microsoft Sentinel, and the ticket in ServiceNow.

To trigger the playbook, you'll then create an automation rule that runs when these incidents are generated. That rule will take these steps:

1. The rule changes the incident status to Active.
2. It assigns the incident to the analyst tasked with managing this type of incident.
3. It adds the "compromised user" tag.
4. Finally, it calls the playbook you just created. (Special permissions are required for this step.)

Playbooks can be run automatically in response to incidents, by creating automation rules that call the playbooks as actions, as in the example above. They can also be run automatically in response to alerts, by telling the analytics rule to automatically run one or more playbooks when the alert is generated.

### **VIII WORKING OF PLAYBOOK:**

Playbooks in Azure Sentinel are designed to automate routine security tasks and streamline incident response processes. They work by executing a series of predefined actions in response to a specific trigger, such as a security alert or event.

The following is an overview of how playbooks work in Azure Sentinel:

1. Trigger: The playbook is triggered when a specific event occurs, such as a security alert being generated, or a threshold being reached. Playbooks can also be triggered manually by a security analyst.
2. Condition: Playbooks can be configured to execute only when certain conditions are met. For example, a playbook may be configured to execute only when a specific user is affected or when a certain number of failed login attempts occur within a certain time.
3. Execution: Once triggered, the playbook executes a series of predefined actions, such as creating a ticket in a ticketing system, sending an email notification to the security team, or disabling a user account. These actions can be customized to meet specific security requirements.
4. Workflow: Playbooks can be designed to follow a specific workflow, with each activity depending on the success or failure of the previous action. This can help to ensure that the incident response process is consistent and effective.
5. Integration: Playbooks in Azure Sentinel can be integrated with other security tools and services, such as threat intelligence feeds and automation platforms. This allows security teams to create highly effective security workflows that incorporate multiple tools and services.
6. Reporting: Playbooks in Azure Sentinel can be configured to generate reports and metrics that provide insights into the incident response process. This can help security teams to identify areas for improvement and optimize their incident response processes.

Overall, playbooks in Azure Sentinel provide security teams with a powerful tool for automating routine security tasks and streamlining incident response processes. By providing consistency in incident response processes and reducing the time taken to respond to security incidents, playbooks can help to improve the overall security posture of an organization.

### **IX CONCLUSION**



Automated rules are a critical component of Azure Sentinel's security capabilities, as they provide a way to continuously monitor security events and data sources for specific conditions or patterns that may indicate a security threat. By automating the monitoring process and configuring rules to trigger alerts and actions when specific criteria are met, security teams can more effectively detect and respond to potential security threats. Automated rules can also be customized and adjusted over time to improve their effectiveness and can be combined with machine learning algorithms to enhance their accuracy and efficiency. Overall, automated rules in Azure Sentinel are an essential tool for maintaining the security and integrity of an organization's data and systems.

## **X. FUTURE ENHANCEMENT**

As technology continues to evolve, there may be opportunities to develop more advanced automation capabilities in Azure Sentinel, such as using machine learning algorithms to automatically identify and respond to security threats. Azure Sentinel can be integrated with a variety of other Azure services, such as Azure Security Centre and Azure Active Directory. Future work could explore ways to further integrate these services with Azure Sentinel to create a more comprehensive and cohesive security solution. While Azure Sentinel provides a range of pre-built playbooks, there may be opportunities to develop more customizable and flexible playbooks that can be tailored to specific organizational needs and workflows. Azure Sentinel can also integrate with a variety of third-party security tools and solutions. Future work could explore ways to further integrate these tools with Azure Sentinel to create a more robust and comprehensive security ecosystem.

## **XI. REFERENCES**

- [1] 1. Jafarian, M., & Tavana, M. (2021). Azure Sentinel Security Information and Event Management: An Overview and Directions for Future Research. *Journal of Network and Computer Applications*, 174, 103030. Doi: 10.1016/j.jnca.2020.103030
2. Khan, I. A., & Hussain, M. (2021). A Comprehensive Review of Microsoft Azure Sentinel: Architecture, Features, and Challenges. *Computers & Security*, 106, 102362. Doi: 10.1016/j.cose.2021.102362
3. Kuznetsov, P., & Kuznetsov, P. (2021). *Azure Sentinel Playbooks: A Guide to Automating Security Response*. Security Boulevard.
4. O'Donnell, M. (2021). *Automating Incident Response with Azure Sentinel Playbooks*. TechTarget.
5. Rizwan, M., & Zahoor, A. (2021). Microsoft Azure Sentinel: An Overview of Security Information and Event Management. *Journal of Information Security and Applications*, 60, 102743. Doi: 10.1016/j.jisa.2021.102743
6. Ansari, M. S., & Alshehri, F. (2021). Azure Sentinel: A Cloud-Native Solution for Security Information and Event Management. *Journal of Cloud Computing*, 10(1), 32. Doi: 10.1186/s13677-021-00237-w
7. Babbar, S., & Chaudhary, V. (2021). Microsoft Azure Sentinel: An Efficient Security Information and Event Management Solution. *Journal of Ambient Intelligence and Humanized Computing*, 12, 2463-2477. Doi: 10.1007/s12652-020-02551-5
8. Deka, B., & Bordoloi, D. J. (2021). Azure Sentinel: A Cloud-Native SIEM Solution. *Journal of Cloud Computing*, 10(1), 42. Doi: 10.1186/s13677-021-00252-x
9. Ghaffari, F., & Heidari, M. (2021). Azure Sentinel and Its Role in Cloud Security: A Systematic Review. *Journal of Cloud Computing*, 10(1), 36. Doi: 10.1186/s13677-021-00246-9
10. Islam, S., Islam, M. S., & Wang, G. (2021). A Review of Microsoft Azure Sentinel: A Cloud-Native Security Information and Event Management System. *Journal of Cybersecurity*, 7(1), 1-16. Doi: 10.1093/cubes/tyab001



11. Khatri, N., & Vows, J. (2021). Data Analytics, Artificial Intelligence, and Cybersecurity in a Post-COVID-19 World. *Journal of Management Analytics*, 8(3), 243-255. Doi: 10.1080/23270012.2021.1908406
12. Prasad, S., & Farid, A. (2021). Microsoft Azure Sentinel: A Modern Cloud-Based SIEM. *International Journal of Advanced Science and Technology*, 30(4), 3261-3271. Doi: 10.14257/ijast.2021.30.04.306
13. Radha, R. K., Jeyakumar, T., & Subramanian, V. (2021). Azure Sentinel: A Comprehensive Security Information and Event Management Solution. *International Journal of Recent Technology and Engineering*, 10(3), 2079-2085. Doi: 10.35940/ijrte.C1326.1183P321
14. Sharma, R., & Chakraborty, S. (2021). Microsoft Azure Sentinel: A Cloud-Based Security Information and Event Management System. *International Journal of Engineering Research and Technology*, 14(3), 329-332. Doi: 10.17577/IJERTV14IS030216
15. Varghese, P. J., & George, R. K. (2021). Azure Sentinel: An Overview of Security Information and Event Management in Cloud Computing. *International Journal of Research and Analytical Reviews*, 8(1), 430-435.
16. Makhija, P., & Choudhary, P. (2021). Automating Security Operations with Azure Sentinel. *International Journal of Advanced Computer Science and Applications*, 12(7), 174-180. Doi: 10.14569/IJACSA.2021.0120720.
17. Nguyen, T., Nguyen, T., Nguyen, T., Nguyen, T., Nguyen, T., Nguyen, T., Nguyen, T., Nguyen, T., Nguyen, T., & Pham, T. (2021). Building and Automating Cybersecurity Solutions with Azure Sentinel and Logic Apps. *International Journal of Advanced Computer Science and Applications*, 12(6), 237-245. Doi: 10.14569/IJACSA.2021.0120629
18. Okoli, V. N., & Nwachukwu, A. O. (2021). Leveraging Azure Sentinel and Power Automate for Incident Response Automation. *International Journal of Computer Science and Information Security*, 19(3), 25-33.
19. Singh, P., Sharma, P., & Singh, A. (2021). An Introduction to Azure Sentinel and Its Automation. *Journal of Advances in Cybersecurity*, 4(1), 1-6. Doi: 10.1145/3458884.3458886
20. Vosloo, D., & Robertson, J. (2021). Security Operations in the Cloud with Azure Sentinel and Microsoft Defender. *Journal of Information Warfare*, 20(4), 88-98.