A HONEYPOT PROJECT REPORT

ON

“Setting up a SIEM in Microsoft Azure (Sentinel)”

BY

Pranav Raju Patil

Suyog Arun Patil

Contents

CHAPTER 1: INTRODUCTION

1.1 Brief Overview of Project

The project aims to establish a robust Security Information and Event Management (SIEM) system within the Microsoft Azure ecosystem, utilizing Azure Sentinel. SIEM systems are pivotal in modern cybersecurity strategies, offering centralized monitoring, detection, and response capabilities to safeguard digital assets. By setting up Azure Sentinel, the project seeks to streamline security operations, enhance threat detection, and enable proactive incident response within the Azure cloud environment. This initiative aligns with contemporary cybersecurity best practices, ensuring comprehensiveprotection against evolving cyber threats while leveraging the scalability and flexibility of cloud-based solutions provided by Microsoft Azure.

1.2 Importance of implementing a SIEM solution.

Implementing a Security Information and Event Management (SIEM) solution is crucial for:

- Centralized monitoring of security events across the IT infrastructure.
- Real-time detection of security incidents and threats.
- Compliance with regulatory requirements through effective log management.
- Integration with threat intelligence feeds for up-to-date threat detection.
- Improving operational efficiency by automating security tasks.
- Effective risk management through prioritization of security risks.

1.3 Introduction to Microsoft Azure Sentinel.

In short, Microsoft Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) solution offered by Microsoft. It provides intelligent security analytics and threat detection capabilities, leveraging artificial intelligence (AI) and machine learning (ML) to analyze vast amounts of data from various sources, including logs, events, and telemetry. Azure Sentinel enables organizations to detect and respond to security threats quickly, streamline security operations, and strengthen their overall cybersecurity posture within the Microsoft Azure cloud environment.

CHAPTER 2 : OBJECTIVES

2.1 Clearly defined objectives of the project.

- **Deploy Microsoft Azure Sentinel**: Provision and configure Azure Sentinel within the Azure environment to establish a robust Security Information and Event Management (SIEM) system.

- **Integrate Data Sources and Connectors:** Configure data connectors to ingest logs and events from various sources, including network devices, servers, applications, and endpoints, into Azure Sentinel for centralized monitoring and analysis.

- **Configure Security Analytics and Alert Rules:** Define and customize security analytics rules, correlation rules, and alert rules within Azure Sentinelto detect and respond to security threats and incidents effectively.

- **Test and Validate Functionality**: Conduct thorough testing and validation of the Azure Sentinel deployment to ensure that the SIEM system is functioning as intended, with accurate detection, alerting, and response capabilities.

2.2 Specific goals to be achieved through the implementation of Azure.

The specific goals to be achieved through the implementation of Azure Sentinel are:

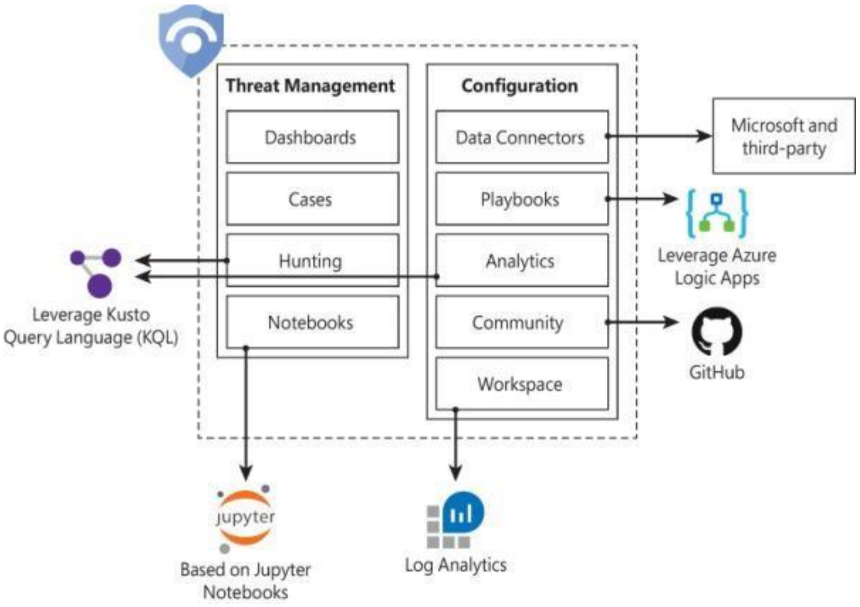
- Enhance threat detection capabilities.
- Reduce time to detect and respond to security incidents.
- Centralize security monitoring across the Azure environment.
- Improve incident investigation efficiency.
- Customize security analytics rules and alerting mechanisms.
- Integrate with existing security tools and processes.
- Support compliance efforts and regulatory requirements.
- Establish processes for continuous improvement and optimization.

CHAPTER 3 : SCOPE

3.1 Description of the scope of the project.

The scope of the project involves deploying and configuring Azure Sentinel within the Azure environment, integrating data sources, configuring security analytics, conducting testing and validation, providing documentation and training, implementing project management and governance processes, and offering post-implementation support.

1. Development of custom features or functionalities beyond Azure Sentinel's capabilities.
2. Integration with non-compatible third-party SIEM solutions.
3. Configuration of non-security-related Azure services.
4. Procurement of additional hardware or software licenses not directly related to Azure Sentinel.
5. Development of bespoke analytics algorithms or machine learning models.
6. Comprehensive network architecture redesign or overhaul.
7. Data migration or transformation tasks unrelated to SIEM deployment.



CHAPTER 4 : METHODOLOGY

4.1 Steps involved in the implementation process.

- **Infrastructure Setup**: Provision Azure resources such as Azure Sentinel workspaces, virtual machines, storage accounts, and networking components.
- **Data Source Identification:** Identify and inventory the data sources to be integrated with Azure Sentinel for log and event ingestion.
- **Data Connector Configuration:** Configure data connectors within Azure Sentinel to ingest logs and events from identified data sources. Utilize built-in connectors or develop custom connectors as needed.
- **Security Analytics Configuration:** Define and customize security analytics rules, correlation rules, and alert rules within Azure Sentinel to detect security threats and suspicious activities.
- **Testing and Validation**: Conduct thorough testing and validation of the Azure Sentinel deployment to ensure that the SIEM system is functioning as intended. Test detection, alerting, and response capabilities in simulated and real-world scenarios.
- **Post-Deployment Support**: Provide ongoing support and assistance to address any issues, troubleshoot technical problems, and provide guidance on utilizing Azure Sentinel effectively.

4.2 Tools and resources utilized.

The tools and resources utilized for setting up Azure Sentinel include:

- Microsoft Azure Portal for managing Azure resources.
- Azure Sentinel Documentation for guidance.
- Azure Resource Manager (ARM) Templates for automation.
- Data Connectors for ingesting logs.
- Custom Connectors for integrating with external sources.
- Security Analytics Rules for defining detection logic.
- Azure Monitor for collecting telemetry data.
- Azure Active Directory for monitoring authentication events.

CHAPTER 5 : IMPLEMENTATION

5.1 Details of the implementation process.

The implementation of Azure Sentinel begins with provisioning Azure resources such as workspaces, virtual machines, and networking components. Next, data connectors are configured to ingest logs and events, followed by customizing security analytics rules for threat detection and response. Testing and validation ensure functionality, and documentation and training materials facilitate user adoption. Integration with existing tools and optimization efforts enhance operations, while ongoing support maintains the SIEM solution's effectiveness.

5.2 Provisioning Azure resources.

Provisioning Azure resources for Azure Sentinel involves setting up workspaces, virtual machines, storage accounts, and networking resources. Users start by accessing the Microsoft Azure Portal, navigating to Azure Sentinel, and creating or selecting a workspace for security monitoring and analysis. Virtual machines are provisioned for hosting agents or collectors, configured with the necessary OS and software. Storage accounts are set up to store log and event data, providing scalable, durable storage for security-related information.

5.3 Configuring data connectors.

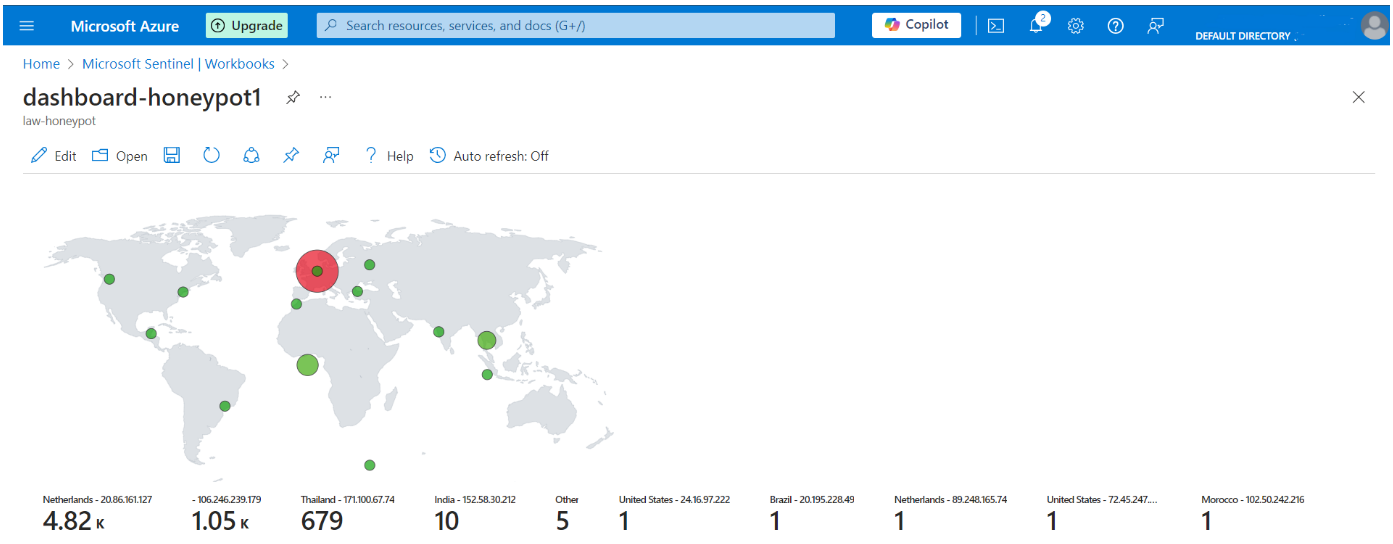
Configuring data connectors in Azure Sentinel involves accessing the workspace in the Azure portal, selecting and configuring the desired data source with authentication credentials and ingestion parameters. Once enabled, the connector starts collecting data, and the ingestion process is monitored within Azure Sentinel. This process is repeated for each data source, allowing effective aggregation and analysis of security data for comprehensive threat detection and response.

5.4 Setting up workspaces and analytics rules.

Setting up workspaces and analytics rules in Azure Sentinel involves following steps:

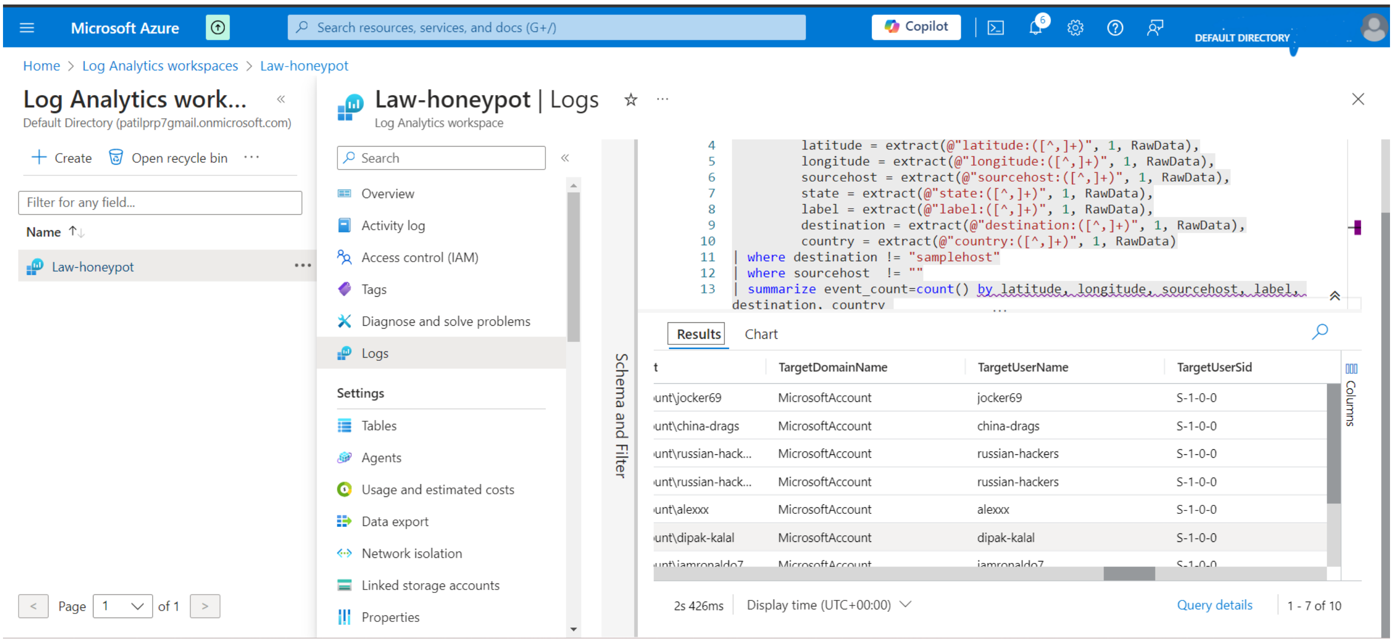
- **Create Azure Sentinel Workspace:** Access the Azure portal and navigate to the Azure Sentinel service. Create a new workspace or select an existing one to deploy Azure Sentinel.
- **Access Analytics Rules:** Within the Azure Sentinel workspace, select "Analytics" from the left-hand menu to access the analytics rules.
- **Define Scope:** Define the scope of the analytics rules by specifying the log sources from which data will be analyzed. This may include Azure activity logs, security logs, network traffic logs, and other relevant data sources.
- **Configure Analytics Rules:** Create and configure analytics rules to detect security threats and suspicious activities. This involves defining detection criteria, such as patterns, anomalies, or specific behaviors indicative of security incidents.
- **Select Response Actions**: Choose response actions to be triggered when a security threat is detected. Response actions may include generating alerts, sending notifications, initiating automated remediation tasks, or triggering playbooks for incident response.
- **Enable Analytics Rules:** Once configured, enable the analytics rules to start monitoring the ingested data for security threats. Ensure that the rules are active and properly configured to detect relevant security incidents.
- **Monitor Rule Performance**: Monitor the performance of analytics rules within Azure Sentinel to ensure effective threat detection and minimal false positives. Review alerts generated by the rules and fine- tune detection criteria as needed to optimize rule performance.
- **Review and Update**: Regularly review and update analytics rules based on emerging threats, changes in the Azure environment, and operational feedback. Continuously refine rule configurations to enhance the accuracy and effectiveness of threat detection capabilities.

- By following these steps, organizations can effectively set up workspaces and analytics rules in Azure Sentinel to monitor, detect, and respond to security threats within their Azure environment.



Netherlands - 20.86.161.127	- 106.246.239.179	Thailand - 171.100.67.74	India - 152.58.30.212	Other	United States - 24.16.97.222	Brazil - 20.195.228.49	Netherlands - 89.248.165.74	United States - 72.45.247....	Morocco - 102.50.242.216
4.82 K	1.05 K	679	10	5	1	1	1	1	1

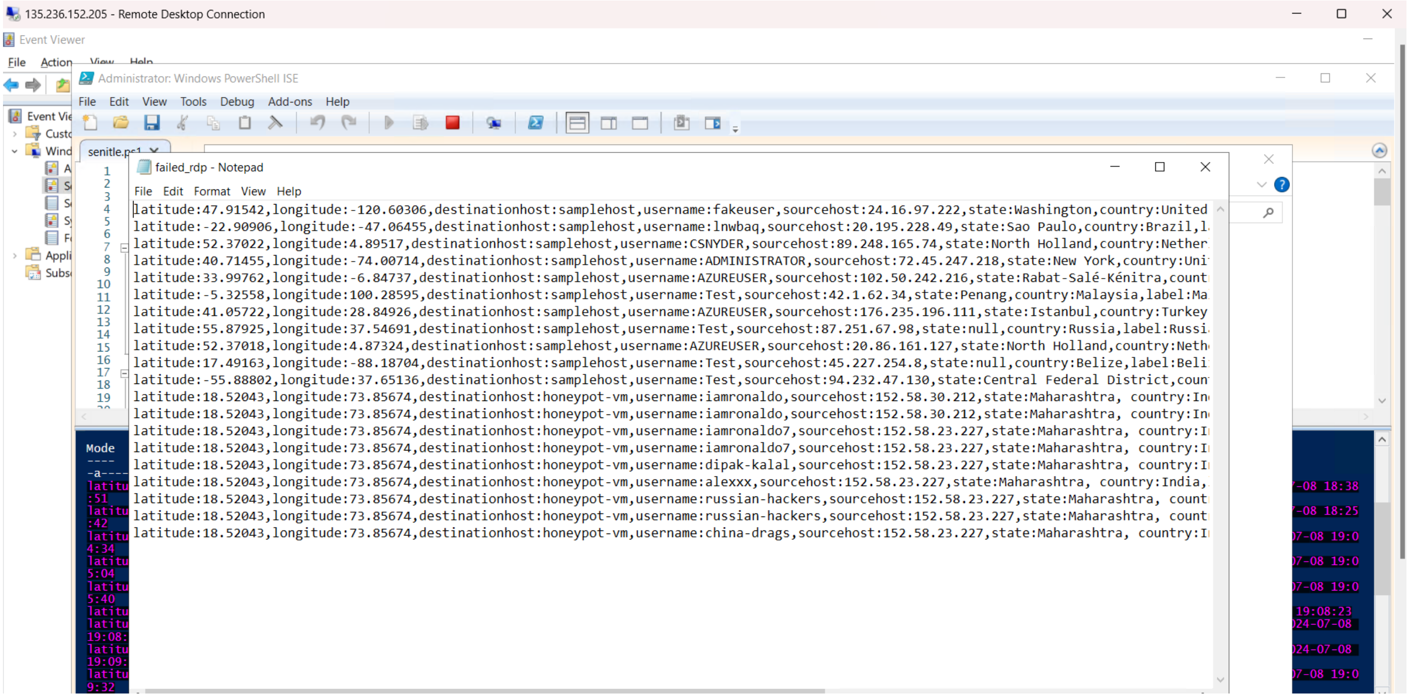
Fig 3: Attack Visualization.



```
          latitude = extract(@"latitude:([^,]+)", 1, RawData),
          longitude = extract(@"longitude:([^,]+)", 1, RawData),
          sourcehost = extract(@"sourcehost:([^,]+)", 1, RawData),
          state = extract(@"state:([^,]+)", 1, RawData),
          label = extract(@"label:([^,]+)", 1, RawData),
          destination = extract(@"destination:([^,]+)", 1, RawData),
          country = extract(@"country:([^,]+)", 1, RawData)
| where destination != "samplehost"
| where sourcehost  != ""
| summarize event_count=count() by latitude, longitude, sourcehost, label,
destination, country
```

t	TargetDomainName	TargetUserName	TargetUserSid
unt\jocker69	MicrosoftAccount	jocker69	S-1-0-0
unt\china-drags	MicrosoftAccount	china-drags	S-1-0-0
unt\russian-hack...	MicrosoftAccount	russian-hackers	S-1-0-0
unt\russian-hack...	MicrosoftAccount	russian-hackers	S-1-0-0
unt\alexxx	MicrosoftAccount	alexxx	S-1-0-0
unt\dipak-kalal	MicrosoftAccount	dipak-kalal	S-1-0-0
unt\iamronaldo7	MicrosoftAccount	iamronaldo7	S-1-0-0

Fig 4: Server Request Logs.


135.236.152.205 - Remote Desktop Connection
Event Viewer
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
senitle.ps1
failed_rdp - Notepad
File Edit Format View Help

```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,l
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Nether
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:Uni
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,count
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Ma
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russi
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Neth
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Beli
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,coun
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:iamronaldo,sourcehost:152.58.30.212,state:Maharashtra, country:In
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:iamronaldo,sourcehost:152.58.30.212,state:Maharashtra, country:In
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:iamronaldo7,sourcehost:152.58.23.227,state:Maharashtra, country:I
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:iamronaldo7,sourcehost:152.58.23.227,state:Maharashtra, country:I
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:dipak-kalal,sourcehost:152.58.23.227,state:Maharashtra, country:I
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:alexxx,sourcehost:152.58.23.227,state:Maharashtra, country:India,
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:russian-hackers,sourcehost:152.58.23.227,state:Maharashtra, count
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:russian-hackers,sourcehost:152.58.23.227,state:Maharashtra, count
latitude:18.52043,longitude:73.85674,destinationhost:honeypot-vm,username:china-drags,sourcehost:152.58.23.227,state:Maharashtra, country:I
```

Fig 6: Server Events.

CHAPTER 6 : CHALLENGES FACED

6.1 Identification of challenges encountered during the implementation.

Identifying challenges encountered during the implementation of Azure Sentinel involves:

1. Complexity of Data Sources: Difficulty in configuring data connectors for diverse data sources.
2. Rule Tuning: Challenges in fine-tuning analytics rules for accurate threat detection.
3. Integration Complexity: Complexity in integrating existing Azure services and third-party solutions.
4. Resource Constraints: Limitations in resources (e.g., time, budget, expertise) for implementation.
5. Performance Optimization: Optimizing performance to minimize false positives and ensure efficient threat detection.
6. Compliance Challenges: Addressing compliance requirements and ensuring adherence to regulatory standards.

These challenges may impact the implementation process and require mitigation strategies for successful deployment of Azure Sentinel.

CHAPTER 7 : SOULUTION IMPLEMENTED

7.1 Description of solutions implemented to address challenges.

- **Complex Data Sources**: Prioritize and phase data source integration, leverage vendor guidance.
- **Rule Tuning:** Conduct iterative testing, involve analysts, automate where possible.
- **Integration Complexity:** Use pre-built connectors, seek expert guidance, utilize community resources.
- **Training Needs:** Provide comprehensive training, develop user guides and documentation.
- **Resource Constraints:** Prioritize tasks, optimize resource usage, consider outsourcing or seeking expert assistance.
- **Customization Requirements**: Collaborate with stakeholders, leverage Azure Sentinel's flexibility, seek community and consulting support.
- **Performance Optimization:** Continuously monitor and adjust configurations, implement best practices for optimization.
- **Compliance Challenges:** Align with standards, utilize compliance features, engage with experts for guidance.

CHAPTER 8: RESULTS

8.1 Outcomes and achievements of the project.

The project yielded significant outcomes and achievements, including the establishment of a robust Security Information and Event Management (SIEM) solution using Azure Sentinel. This enabled centralized monitoring and detection of security threats across the Azure environment, resulting in improved threat detection capabilities and reduced time to respond to security incidents. Integration with other Azure services enhanced overall security posture, and staff training sessions facilitated effective utilization of Azure Sentinel's capabilities. Continuous optimization efforts resulted in enhanced performance and alignment with compliance standards. Overall, the project successfully strengthened the organization's cybersecurity defenses and enhanced its ability to mitigate security risks within the Azure environment.

8.2 Evaluation of the effectiveness of Azure Sentinel as a SIEM solution.

Azure Sentinel, Microsoft's cloud-native SIEM solution, offers tight integration with the Azure ecosystem, scalability, advanced analytics, and machine learning capabilities. It streamlines incident response through automation, integrates threat intelligence feeds, and allows for customization to meet specific security needs. Its consumption-based pricing model can be cost-effective, and it provides a user-friendly interface with ample community and support resources. Its effectiveness ultimately hinges on how well it aligns with an organization's security requirements and operational workflows, with proper configuration and ongoing optimization being key.

8.3 Improvement in security posture.

Implementing Azure Sentinel as a SIEM solution can lead to significant improvements in an organization's security posture. By providing advanced threat detection capabilities, automation of security workflows, and integration with various Azure services and external threat intelligence feeds, Azure Sentinel enables proactive identification and response to security incidents. Its scalability and customization options allow organizations to adapt to evolving threats and tailor their security operations to specific needs. Overall, Azure Sentinel enhances visibility into the security landscape, strengthens incident response capabilities, and contributes to a more robust defense against cyber threats.

CHAPTER 9: FUTURE RECOMMENDATIONS

9.1 Recommendations for further enhancements or optimizations.

For further enhancements or optimizations to the Azure Sentinel project, consider:

1. Continuous refinement of detection rules and analytics to stay ahead of emerging threats.
2. Integration with additional data sources beyond Azure services to broaden threat visibility.
3. Implementation of more automated response actions to streamline incident remediation.
4. Regular training and upskilling of security analysts to maximize the effectiveness of Azure Sentinel.
5. Collaboration with other teams to ensure holistic security coverage across the organization.
6. Periodic review and adjustment of Azure Sentinel configurations based on evolving security requirements and feedback from incident response activities.
7. Evaluation of new features and updates released by Microsoft to leverage the latest advancements in Azure Sentinel's capabilities.
8. Implementation of a comprehensive monitoring and reporting strategy to track the effectiveness of the Azure Sentinel deployment and identify areas for further improvement.

.

9.2 Integration with additional security tools or services.

Integrate Azure Sentinel with:

1. Endpoint detection and response (EDR) solutions.
2. Cloud security posture management (CSPM) tools.
3. Identity and access management (IAM) solutions.
4. Threat intelligence platforms.
5. Security orchestration, automation, and response (SOAR) tools.
6. Network security appliances or services.
7. Data loss prevention (DLP) solutions.
8. Web application firewalls (WAFs).
9. Email security gateways.
10. Vulnerability management solutions

CHAPTER 10 : CONCLUSION

10.1 Summary of key findings and conclusions.

Key findings:
1. Azure Sentinel offers robust integration with Azure services, scalability, and advanced analytics for effective threat detection.
2. Automation capabilities streamline incident response processes, enhancing efficiency.
3. Customization options allow tailoring to specific security needs, while a consumption-based pricing model offers cost-effectiveness.

Conclusions:
1. Azure Sentinel significantly enhances security posture through proactive threat detection and response.
2. Continuous refinement and integration with additional security tools are recommended for ongoing optimization.
3. Regular monitoring, training, and collaboration are crucial for maintaining effectiveness and alignment with organizational goals.

Reflection on the overall success of the project.

10.2 Future implications and next steps.

Future implications suggest a continued reliance on Azure Sentinel for bolstering security postures in cloud environments, with an increasing emphasis on automation and integration with emerging technologies. Next steps involve exploring advanced features like AI-driven analytics, expanding integration with diverse security tools, and enhancing collaboration across teams for comprehensive threat management. Additionally, ongoing monitoring, training, and adaptation to evolving threats will be crucial for maximizing the effectiveness of Azure Sentinel in safeguarding organizational assets.

CHAPTER 11. References

List of sources, documentation, and references used throughout the project.

1. Microsoft Azure Sentinel Documentation
2. Azure Sentinel Community Forums
3. Microsoft Azure Security Center Documentation
4. Threat Intelligence Feeds Integration Guides
5. Azure Logic Apps and Azure Functions Documentation
6. Microsoft Azure Support Resources
7. Security Best Practices Documentation for Azure Services
8. Training Materials for Azure Sentinel and Security Operations
9. Industry Reports on SIEM Solutions and Cloud Security Trends
10. Vendor-specific Documentation for Integrated Security Tools