# Improving Cloud Security Posture with Azure Sentinel A Real-Time Threat Detection Solution

**Authors**:

Pravin Raja, Ashrith Bhooka Ravinandan, Bojja Sathwik Reddy, Muthyala Tushaar Reddy, Sai Charan Thallapelli, Sri Rohit Yadlapalli, Mani Kumar Edukoju, Sai Amartya Maruth Mandedi

**Course**: AIT-670: Cloud Computing Security

**Abstract**

The increasing reliance on cloud computing introduces significant security challenges, particularly in real-time threat detection, analysis, and mitigation. This project explores the capabilities of Azure Sentinel, a cloud-native Security Information and Event Management (SIEM) platform, to address these challenges. By implementing automated processes for log ingestion, threat detection, and incident response across six real-world use cases, the project demonstrates Sentinel’s potential to transform cloud security operations. This report details the project’s methodology, results, and lessons learned, providing a comprehensive guide to leveraging Azure Sentinel for improved security postures.

Table of Contents

[Improving Cloud Security Posture with Azure Sentinel A Real-Time Threat Detection Solution 1](#_Toc184304989)

[1. Introduction 3](#_Toc184304990)

[2. Problem Statement 3](#_Toc184304991)

[3. Objectives and Research Questions 3](#_Toc184304992)

[4. Tools and Technologies 4](#_Toc184304993)

[5. Methodology 4](#_Toc184304994)

[1. Data Ingestion and Integration 4](#_Toc184304995)

[2. Analytics and Threat Detection 4](#_Toc184304996)

[3. Incident Management 4](#_Toc184304997)

[4. Threat Hunting 4](#_Toc184304998)

[5. Automation and Compliance 4](#_Toc184304999)

[6. Key Security Use Cases 4](#_Toc184305000)

[1. Blocking Malicious IP Addresses 4](#_Toc184305001)

[2. Revoked User Privileges 4](#_Toc184305002)

[3. Infected Virtual Machine Logs 5](#_Toc184305003)

[4. MFA Analysis 5](#_Toc184305004)

[5. Entra ID Logs 5](#_Toc184305005)

[7. Results 5](#_Toc184305006)

[8. Lessons Learned 6](#_Toc184305007)

[9. Conclusion 6](#_Toc184305008)

[10. References 7](#_Toc184305009)

## 1. Introduction

This project focuses on utilizing **Azure Sentinel**, a cloud-native Security Information and Event Management (SIEM) tool, to address these challenges. Azure Sentinel provides centralized visibility, advanced threat detection, and automated incident response capabilities, making it an ideal choice for modern cloud environments.

Through the implementation of real-world use cases, such as monitoring malicious IP addresses, analyzing MFA anomalies, and investigating virtual machine infections, this project evaluates Azure Sentinel’s ability to detect and mitigate security incidents in real time.

## 2. Problem Statement

In today’s cloud security landscape, organizations face the following key challenges:

* **Fragmented Security Systems**: Traditional security tools often operate in silos, making it difficult to gain a comprehensive view of the threat landscape.
* **Delayed Response Times**: Manual monitoring and intervention slow down the ability to detect and respond to incidents, increasing the risk of damage.
* **High Alert Volumes**: A high number of false positives can overwhelm security teams, diverting attention from critical threats.
* **Compliance Demands**: Keeping up with evolving regulatory requirements adds to the complexity of maintaining a secure environment.

This project aims to address these issues by implementing a unified security solution using Azure Sentinel.

## 3. Objectives and Research Questions

This project aimed to design and implement a robust, scalable cloud security solution using Azure Sentinel to enhance real-time threat detection and incident response. The project explored practical use cases to evaluate Sentinel's capabilities in addressing security challenges.

**Project Objectives**

1. Centralize and streamline security data management across multiple sources.
2. Enable proactive threat detection through advanced analytics and automation.
3. Reduce response times with automated playbooks and alerts.
4. Minimize false positives and improve the accuracy of threat detection.
5. Ensure compliance with regulatory and organizational security standards.

**Research Questions**

1. What cost implications and scalability challenges does Azure Sentinel present for organizations of different sizes?
2. How can Sentinel’s features, such as dashboards and reporting, improve collaboration among cybersecurity teams?
3. What strategies can effectively minimize false positives without compromising threat detection?

## 4. Tools and Technologies

The successful implementation of this project relied on the following tools and technologies:

* **Azure Sentinel**: A cloud-native SIEM and SOAR platform used for security event monitoring, incident management, and automated response.
* **PowerShell**: For log ingestion and conversion of data from CSV to JSON format compatible with Azure Sentinel.
* **KQL (Kusto Query Language)**: For querying and analyzing log data to detect anomalies and security incidents.
* **Microsoft Power BI**: For creating visually rich dashboards to interpret log data and generate insights.
* **Microsoft Excel**: Used as a data preprocessing tool to prepare raw logs before ingestion into Sentinel.

These tools were integrated to ensure seamless workflows for data ingestion, analysis, and response automation.

## 5. Methodology

The project followed a structured approach with the following key steps:

1. Data Ingestion and Integration:
   * Logs from six security use cases, such as malicious IP blocking and MFA anomalies, were ingested into Azure Sentinel.
   * PowerShell scripts automated the ingestion process by converting CSV files to JSON format for Sentinel compatibility.
2. Analytics and Threat Detection:
   * Logs were queried using KQL to identify suspicious activities.
   * Dashboards and visualizations were created to monitor trends and anomalies.
3. Incident Management:
   * Alerts were categorized by severity (low, medium, high, critical) and sent to designated email recipients using action groups.
4. Threat Hunting:
   * Sentinel's advanced hunting tools, coupled with the MITRE ATT&CK framework, were used to investigate and prioritize incidents.
5. Automation and Compliance:
   * Sentinel’s playbooks automated repetitive tasks, such as isolating compromised systems or blocking suspicious accounts.
   * Compliance reports were generated to ensure adherence to industry standards and best practices.

## 6. Key Security Use Cases

1. Blocking Malicious IP Addresses

* **Objective**: Identify and block botnet, phishing, and web shell activities originating from malicious IPs.
* **Outcome**: Dashboards and alerts were created to provide real-time insights into suspicious activities, enabling swift threat mitigation.

1. Revoked User Privileges

* **Objective**: Monitor and analyze unauthorized privilege escalations and access violations.
* **Outcome**: Detected and revoked risky privilege escalations to mitigate insider threats.

1. Infected Virtual Machine Logs

* **Objective**: Identify and isolate virtual machines infected with malware or unauthorized access attempts.
* **Outcome**: Implemented isolation protocols for compromised VMs, preventing further damage.

1. MFA Analysis

* **Objective**: Analyze multi-factor authentication logs to detect anomalies indicative of brute force or credential stuffing attacks.
* **Outcome**: Generated insights into suspicious authentication patterns, enabling focused security actions.

### Entra ID Logs

* **Objective**: Investigate anomalies in Entra ID logs, such as unauthorized permission changes and failed login attempts.
* **Outcome**: Identified misconfigurations and potential account compromises, leading to policy updates.

## 7. Results

The project successfully demonstrated Azure Sentinel’s capabilities in real-time threat detection and response across multiple use cases.

**Key Achievements**

1. **Seamless Data Integration**
   * Successfully ingested and processed log data from six distinct security use cases.
   * Utilized PowerShell scripts to convert raw CSV logs into Sentinel-compatible JSON formats.
2. **Enhanced Threat Detection and Monitoring**
   * Identified patterns of malicious activity, such as repeated login failures and suspicious IP connections.
   * Dashboards and visualizations provided clear, actionable insights into security incidents.
3. **Proactive Incident Management**
   * Alerts categorized by severity levels (low, medium, high, critical) allowed for efficient triaging.
   * Automated workflows reduced response times significantly.
4. **Improved Compliance**
   * Generated detailed compliance reports, ensuring adherence to regulatory and organizational standards.
   * Audits highlighted areas for policy improvement, particularly in MFA usage and user access controls.

**Quantifiable Outcomes**

* **Log Ingestion Success Rate**: 100% across all six use cases.
* **Reduction in False Positives**: Custom alert thresholds and dynamic whitelists reduced alert noise by over 40%.
* **Incident Response Time**: Reduced by an estimated 30% due to automated playbooks.

## 8. Lessons Learned

The project provided valuable insights into implementing and optimizing Azure Sentinel in a real-world security environment:

**1. Cost and Scalability**

* Azure Sentinel’s **pay-as-you-go** model proved cost-efficient for smaller data volumes but required careful planning for larger datasets.
* Employing selective log ingestion (e.g., only high-priority data types) can help organizations balance costs with performance.

**2. Collaboration and Team Efficiency**

* Shared dashboards, standardized reporting, and centralized incident management improved cross-team coordination.
* Streamlining workflows through action groups and shared KQL queries reduced redundancies.

**3. Reducing False Positives**

* Whitelisting trusted entities and fine-tuning alert thresholds proved effective in reducing false alarms.
* Establishing baseline activity profiles for normal user and system behaviour further enhanced accuracy.

**4. Automation and Threat Hunting**

* Automating repetitive tasks, such as account isolation and IP blocking, freed up resources for higher-priority activities.
* The integration of MITRE ATT&CK techniques in threat hunting improved the precision of investigations.

## 9. Conclusion

The project successfully highlighted Azure Sentinel’s potential as a comprehensive cloud security solution. By addressing real-world use cases, such as blocking malicious IPs and analyzing infected VM logs, the project demonstrated Sentinel’s capabilities in real-time threat detection, incident response, and compliance monitoring.

**Key Takeaways**:

1. Azure Sentinel’s automation and analytics tools significantly improve an organization’s ability to respond to evolving threats.
2. Proper optimization and cost management are essential to ensure scalability without exceeding budgets.
3. Proactive threat hunting and dynamic compliance measures enhance an organization’s overall security posture.

**Future Recommendations**

1. **Integration with Threat Intelligence Feeds**: Incorporate external threat intelligence to enrich Sentinel’s data analytics capabilities.
2. **Advanced Machine Learning**: Use Azure’s ML services to develop predictive threat models.
3. **Periodic Policy Updates**: Regularly review and update security policies based on new insights and threats.

This project serves as a blueprint for organizations aiming to adopt Azure Sentinel as their primary SIEM solution, enabling them to achieve a more secure and resilient cloud infrastructure.

## 10. References

* Microsoft. "Data Collector API." *Azure Monitor Logs*, Microsoft, [https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-collector-api?tabs=powershell#alternatives-and-considerations](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-collector-api?tabs=powershell). Accessed 16 Nov. 2024.
* Tutorials Dojo. "How to Set Up Alerts Rules and Action Groups in Azure Monitor." *Tutorials Dojo*, <https://tutorialsdojo.com/how-to-set-up-alerts-rules-and-action-groups-in-azure-monitor/>. Accessed 16 Nov. 2024
* Trull, Jonathan, et al. *Microsoft Azure Sentinel: Planning and Implementing Microsoft’s Cloud-Native SIEM Solution.* Microsoft Press, 2020.
* Falode, Elijah. *Microsoft Power BI Demystified: Step by Step Guide on How to Create Interactive Dashboard and Reports Using Power BI.* M-POWER CORPORATE, 2021.
* "Use KQL to Master Sentinel Data." *Practical 365*, <https://practical365.com/use-kql-to-master-sentinel-data/>. Accessed 16 Nov. 2024.
* "Conditional Access Policies for Entra Joined Devices." *Scalefusion Help Center*, <https://help.scalefusion.com/docs/conditional-access-policies-for-entra-joined-devices>. Accessed 16 Nov. 2024.
* Van der Woude, Derk. "Web Attacks Prevented by Azure WAF and Detected by Azure Sentinel." *Medium*, 19 Aug. 2021, <https://derkvanderwoude.medium.com/web-attacks-prevented-by-azure-waf-and-detected-by-azure-sentinel-a4d78f46100b>. Accessed 16 Nov. 2024.
* University of New Mexico. "What Is Azure Multi-Factor Authentication (MFA) and How Does It Work at UNM?" *UNM IT Services*, University of New Mexico, 2023, <https://unm.custhelp.com/app/answers/detail/a_id/7823/~/what-is-azure-multi-factor-authentication-%28mfa%29-and-how-does-it-work-at-unm%3F>.
* "How to Check Azure Firewall Logs." *MS Codes*, 2024, ms.codes/blogs/internet-security/how-to-check-azure-firewall-logs?srsltid=AfmBOooGHu1z94ydTJpl7zxNl9en68Ib4nJqvO5D4daVYM\_wsid8sH0w. Accessed 14 Nov. 2024.