HISHAM AHAMED

Senior Consultant- Cloud Security Solutions

☎ +974-55759546
@ contact@hishamahamed.com
🔗 https://hishamahamed.com
📍 Doha, Qatar

SUMMARY

I am a highly skilled individual working as a Senior Consultant - Cloud Security Solutions at Mannai - Microsoft. My expertise lies in Cybersecurity, including deploying SIEM-SOAR solutions, configuring Azure Sentinel, implementing Zero Trust Policy, and adhering to compliance standards. Additionally, I have a strong background in programming languages such as C, C++, Java, Python, Dart, TypeScript, as well as proficiency in frameworks like Flutter, Angular, NodeJS, and MongoDB. Furthermore, I am experienced in Electronics, specifically Arduino and Raspberry Pi.

PROJECTS

Azure Sentinel Deployment and Optimisation - Hamad Medical Corporation

📍 Barwa Tower, Al Sadd

One of the most notable projects successfully implemented.

- Gained extensive proficiency and hands-on experience of over 700 hours in effectively troubleshooting Linux log collectors, SQL databases, and Oracle databases, with a specialization in resolving issues and enhancing their performance for seamless onboarding to Sentinel.
- Integrated and configured over 300 devices, including Windows/Linux Servers, Databases, and NVA's, both on-premise and on the cloud.
- Developed customized workarounds that 100% onboarded network devices into the system, even those that are not initially supported by Sentinel.
- Designed a custom format for Tipping Point Firewall to ensure its compatibility and proper formatting as Common Event Format (CEF).
- Assisted in the creation of KQL parsers for more than 100 network devices that were in raw syslog format, enabling efficient log analysis and monitoring.
- Developed a custom PowerShell script that retrieves logs from a remote SQL server, stores them locally, and utilizes Sentinel's custom logs for onboarding. Subsequently, the logs were parsed using KQL for analysis and monitoring purposes.
- Implemented a custom filter for network devices by applying a workaround at the source code level of Sentinel's Linux Log Collector, enabling more precise and targeted log collection.
- Contributed to the development of more than 15 custom workbooks/dashboards with multiple tabs by engaging in conversations with subject-matter experts (SMEs) to gather their specific requirements and tailor the solutions accordingly.
- Contributed to the development with the help of Microsoft support for more than 20 custom automation playbooks by engaging in conversations with subject-matter experts (SMEs) to gather their specific requirements and tailor the solutions accordingly.

Azure Sentinel Deployment and Optimisation - Ministry of Social Development and Family

📍 Al Faisal Tower, Westbay

Played a lead role in both Phase 0 and Phase 1 of the project

- Successfully completed the 100% implementation of Sentinel, incorporating a robust zero trust policy to establish a secure and controlled environment for advanced threat detection and prevention capabilities
- Achieved a complete 100% onboarding of out-of-the-box (OOTB) analytical rules and workbooks, ensuring comprehensive coverage for efficient monitoring and analysis within the system
- Developed and delivered 5 customized workbooks tailored to specific customer requirements, ensuring seamless monitoring and analysis of relevant data within the Sentinel platform
- Designed and implemented 5 custom automation playbooks based on specific customer requirements, streamlining and automating various security operations within the Sentinel platform
- Complete migration of Sentinel from Western Europe to Qatar Central, achieving a 100% relocation
- Conducted knowledge transfer (KT) sessions with the customer, providing step-by-step guidance and training throughout the onboarding process of Sentinel to ensure a smooth and well-informed adoption

PROJECTS

Azure Sentinel Deployment and Optimisation - Qatar News Agency

Diplomat Tower, West bay

Successfully onboarded Sentinel and actively participated in the SOC Team.

- Gained extensive proficiency and hands-on experience of over 160 hours in effectively troubleshooting Linux log collectors, NVA's, with a specialization in resolving issues and enhancing their performance for seamless onboarding to Sentinel
- Conducted a series of focused 4-hour training sessions for the SOC team, enabling them to proficiently perform investigation and reporting tasks within the Sentinel platform
- Implemented analytical rules sourced from GitHub,tailored to use cases identified during conducted investigations, to enhance the detection and analysis capabilities within the system
- Conducted interviews as part of the hiring process to assemble a skilled and competent SOC team
- Provided valuable support to the SOC team as a subject-matter expert (SME) in leveraging threat intelligence for proactive threat hunting activities

Azure Sentinel Deployment and Optimisation- Civil Service and Government Development Bureau

Al Faisal Tower, Westbay

Played a lead role in both Phase 0 and Phase 1 of the project

- 100% integration and configured over 100 devices, including Windows/Linux Servers, Databases, and NVA's, both on-premise and on the cloud.
- Played a key role in 100% integration and collecting logs from the SQL Database, focusing on the access logs of the designated application.
- Optimized customer's workbook and playbook requirements by analyzing and refining them to ensure efficient and effective monitoring, analysis, and automation within the Sentinel platform.
- Complete migration of Sentinel from Western Europe to Qatar Central, achieving a 100% relocation.
- Conducted knowledge transfer (KT) sessions with the customer, providing step-by-step guidance and training throughout the onboarding process of Sentinel to ensure a smooth and well-informed adoption.

Azure Sentinel Deployment and Optimisation- Al Meera

Al Meera Head Office (Qatar Tower)

Basic streamlined Onboarding for Enhanced Protection

- Successfully completed the 100% implementation of Sentinel, incorporating a robust zero trust policy to establish a secure and controlled environment for advanced threat detection and prevention capabilities
- Successfully onboarded 100% of on-premises and cloud-based devices onto the Sentinel platform
- Achieved a complete 100% onboarding of out-of-the-box (OOTB) analytical rules and workbooks, ensuring comprehensive coverage for efficient monitoring and analysis within the system
- Complete migration of Sentinel from Western Europe to Qatar Central, achieving a 100% relocation

Azure Sentinel Deployment and Optimisation - Public Prosecution

Al Jassimya Tower

Sentinel Implementation: Empowering Security with a Zero Trust Policy

- Achieved 100% implementation of Sentinel with a zero trust policy, complete onboarding of devices, and comprehensive coverage of OOTB rules and workbooks for advanced threat detection and monitoring.

Azure Sentinel Deployment and Optimisation - Al Rayyan For Media and Marketing

Abdullah bin Jasim St.

Sentinel Implementation: Empowering Security with a Zero Trust Policy

- Achieved 100% implementation of Sentinel with a zero trust policy, complete onboarding of devices, and comprehensive coverage of OOTB rules and workbooks for advanced threat detection and monitoring.

Azure Sentinel Deployment and Optimisation - Qatar Development Bank

Grand Hamad Street

Sentinel Implementation: Empowering Security with a Zero Trust Policy

- Achieved 100% implementation of Sentinel with a zero trust policy, complete onboarding of devices, and comprehensive coverage of OOTB rules and workbooks for advanced threat detection and monitoring.

Azure Sentinel Deployment and Optimisation - State Audit Bureau

West Bay, Doha

Sentinel Implementation: Empowering Security with a Zero Trust Policy

- Achieved 100% implementation of Sentinel with a zero trust policy, complete onboarding of devices, and comprehensive coverage of OOTB rules and workbooks for advanced threat detection and monitoring.

PROJECTS

Azure Sentinel Deployment and Optimisation - Primary Health Care Corporation

📍 Barwa Tower, Al Sadd

Seamless Onboarding of Access Switches Sentinel

- Ongoing

Azure Sentinel Deployment and Optimisation - Baladana

📍 Baladna Staff Gate And Offices, Al Khor

Sentinel Migration from West Europe to Qatar Central and Optimisation

- Ongoing migration of Sentinel from Western Europe to Qatar Central, targeting a 100% relocation.

Azure Sentinel Deployment and Optimisation - Nakilath

📍 Shoumoukh Towers B, Doha

Sentinel Migration from West Europe to Qatar Central and Optimisation

- Ongoing migration of Sentinel from Western Europe to Qatar Central, targeting a 100% relocation.

Azure Sentinel Deployment and Optimisation - Qatar Gas

📍 West Bay, Doha

Sentinel Migration from West Europe to Qatar Central and Optimisation

- Ongoing migration of Sentinel from Western Europe to Qatar Central, targeting a 100% relocation.

ADDITIONAL PROJECTS

Swift Cleaning Application

📍 Swift cleaning services, Ad Dawhah

Comprehensive Software for Company-wide Management and Financial Processes

- 100% Customer-consulted UI design in Figma, tailored to perfection
- From design to frontend, meticulously crafted to meet customer expectations. Translated the precise design into code using Angular, Bootstrap, and custom CSS
- Developed a secure backend using Node.js, crafting custom APIs and integrating third-party APIs while ensuring robust security measures to safeguard against breaches
- Employed MongoDB as the database solution of choice
- Deployed the software on Azure utilizing containerization for both the frontend and backend components

Planet Organic World E-Commerce Website

📍 Building 1, Zone 3 Wadi Musheireb

🔗 https://planetorganicworld.com/

An E-commerce Platform for Buying/Selling Organic Products

- A comprehensive website built 100% on the WordPress platform, Leveraging the full capabilities of WordPress for a seamless web development experience, A complete website development using the versatile WordPress framework.

EXPERIENCE

Senior Consultant- Cloud Security Solutions

Mannai Microsoft Solutions

01/2022 - Present Doha Qatar

Main Activities

- **Azure Sentinel Implementation:** 100% of implementation of Azure Sentinel, Microsoft's cloud-native Security Information and Event Management (SIEM) solution, for more than 13 organizations to centralize and streamline their security operations.
- **SIEM Configuration:** Configured Azure Sentinel to collect, correlate, and analyze security logs and events from various data sources, including cloud services, on-premises systems, and third-party applications.
- **Threat Detection and Response:** Developed custom detection rules and queries in Azure Sentinel to identify and respond to security threats and incidents effectively. Implemented threat intelligence feeds and threat hunting techniques to proactively detect and mitigate potential threats.
- **Automation and Orchestration:** Leveraged Azure Logic Apps and Azure Functions to automate security workflows and orchestrate incident response processes, improving the efficiency and speed of security operations.
- **Integration with Security Solutions:** Integrated Azure Sentinel with other security solutions, such as Azure Active Directory, Azure Security Center, and third-party tools, to enhance the overall security posture and enable comprehensive threat visibility and response.
- **Incident Investigation and Reporting:** Conducted thorough investigations of security incidents, analyzed log data, and generated comprehensive reports for stakeholders, providing insights into the incident details, root cause analysis, and recommended remediation actions.
- **Compliance and Governance:** Assisted organizations in achieving and maintaining regulatory compliance by configuring compliance monitoring and reporting capabilities in Azure Sentinel, aligning with frameworks like PCI DSS, ISO 27001, and industry-specific regulations.
- **Threat Intelligence Management:** Managed and utilized threat intelligence sources to enrich security analytics, stay up-to-date with emerging threats, and enhance the overall threat detection and response capabilities of Azure Sentinel.
- **Continuous Improvement:** Stayed abreast of the latest trends and developments in the cybersecurity landscape and actively participated in knowledge sharing and continuous improvement initiatives to enhance Azure Sentinel implementation methodologies and best practices.

Full Stack Developer and Azure Cloud Administrator

ZAASH IT Consultancy

01/2019 - 12/2021 Doha Qatar

Main Activities

- **Azure Cloud Administration:** Managed and administered Azure services, including virtual machines, virtual networks, storage accounts, and Azure Active Directory. Utilized Azure Portal and PowerShell for provisioning and configuration.
- **Infrastructure as Code:** Implemented Infrastructure as Code (IaC) using Azure Resource Manager (ARM) templates to automate resource provisioning and management.
- **Security and Compliance:** Configured and maintained security measures within Azure, including RBAC, NSGs, Azure Security Center, and Azure Policies. Ensured compliance with industry standards and regulations.
- **Full Stack Development:** Developed and maintained web applications using front-end technologies such as HTML, CSS, and JavaScript, and back-end technologies like Node.js and Express.js. Utilized frameworks like Angular for building dynamic and responsive user interfaces.

Web Designer

Xeoscript Technologies

08/2016 - 12/2018 Kerala, India

Main Activities

- **Web Design:** Created visually appealing and user-friendly website designs using industry-standard tools like Adobe Photoshop, Illustrator, and Figma. Developed wireframes and prototypes to demonstrate the layout and functionality of web pages.
- **Responsive Design:** Designed websites with a focus on responsive design, ensuring optimal user experience across various devices and screen sizes.
- **HTML/CSS Coding:** Converted design mockups into pixel-perfect HTML and CSS code. Implemented modern web standards and best practices ensuring cross-browser compatibility and accessibility.
- **Front-End Development:** Worked closely with front-end developers to implement interactive elements, animations, and dynamic content using JavaScript and frameworks like jQuery.

EDUCATION

Electronics and Communication Engineering

Anna University, India

PROFESSIONAL SKILLS

Microsoft Sentinel

KQL Ninja · SIEM-SOAR Optimisation · Code level Knowledge of Linux Collector · Custom Workbook · Custom AR · Custom Automation Playbook · Threat Hunting · Scripting · Powershell

Languages and Frameworks

KQL · C · C++ · JAVA · DART · JavaScript · TypeScript · Python · Flutter · Angular · Node JS · Express Js · MongoDB

LANGUAGES

English ●●●●●
Native

Malayalam ●●●●●
Mother Tongue

Hindi ●●●●○
Proficient

Tamil ●●○○○
Intermediate

Arabic ●○○○○
Beginner

AWARDS

Best Performer Award - 2022, Mannai Microsoft Solutions

DIC-Qatar, Code camp -2019 Winner

REFERENCES

Tarek Hadla - Senior Section Head, Mannai Microsoft
tarek.hadla@mannai.com.qa

Ashwin Venugopal - Microsoft most Valued Personnel
ashwin@ashwinpro.com

Bilal Hansrod - Cloud Solution Architect, Microsoft
bilalhansrod@microsoft.com