MUHAMMAD JUNAID RAZA

Experienced Security Engineer

CONTACT

- mjunaidr3@gmail.com
- linkedin.com/in/mjunaidr
- github.com/frozenstrawberries

CERTIFICATIONS

- Microsoft Certified: Azure Security Engineer Associate (AZ-500), Certified ID: H623-3446
- Microsoft 365 Certified: Security Administrator Associate (MS-500), Certified ID: 996603-M127D4

TRAININGS

- SANS SEC401: SANS Security Essentials.
- SANS SEC501: Advanced Security Essentials - Enterprise Defender.
- Azure Security Technologies, (AZ-500).
- Bash Shell Scripting from Udemy
- Python – Beyond the Basics
- Python Best Practices for Code Quality
- Unit Testing with Python
- Managing Python Packages and Virtual Environments
- AWS Developer - Building on AWS

SUMMARY

An experienced Security Engineer who has helped several mid to large-level organizations establish their Security Operations Center from scratch, currently working to secure organizations and automate trivial tasks by analysts, open for an opportunity to further my experience and knowledge in a challenging and encouraging work environment.

WORK EXPERIENCE

ABN Amro Bank N.V.

Amsterdam, Netherlands

Security Engineer — Jul 2022 – Present

Chief Information Security Office (CISO) – Application Security Monitoring

Working as part of the Security Monitoring team to make sure that security monitoring is in place for bank's 3000+ applications hosted on a mix of Azure, Mainframe and On-Prem.

- Planning and executing strategies for securing the large number of applications by creating engagement methodologies, automated security logs ingestion, automated logs normalization.
- Collaborating with Threat Modelling, Threat Intel, Auditing, and several other teams to create threat profiles for applications and paving a way to create a threat repository.
- Creating Generic and Custom Correlation rules to secure as many applications as possible and for critical/highly sensitive applications respectively.
- Developing/Building/Testing the correlation rules from end to end in an automated DTAP environment.
- Creating SOAR solutions to aid the automated integration of correlation rules, escalations, analysis, and mitigations.
- Creating and implemented SIRP templates for the correlation rules so that the application teams can follow.
- Training new colleagues and supporting the management in audits, reporting etc.

AzuredUK

Lichfield, UK

Freelance Security Consultant — Jul 2021 – Jun 2023

Managed Security Services (MSS)

Managed several multitenancy-based Azure Sentinel SOC setups as a freelance Security Consultant and point of contact. Onboarded several clients to the setup from start to finish. This includes integrations, log pruning, correlation rules creation and fine tuning, dashboarding, SOAR automations, notifications push to mailbox/teams, automated analysis, and automated actions for incidents.

Ebryx Pvt Ltd

Lahore, Pakistan

Team Lead/Sr. Security Engineer — Jan 2022 – Jun 2022

Sr. Security Engineer — Jun 2021 – Dec 2021

Security Engineer — May 2020 – Jun 2021

Managed Security Services Provider (MSSP) – SOC

Managed the Security Operations as a Security Engineer in L3 role, actively involved in deployment of Security Operation Center; and monitoring, containing and responding to known and unknown security threats. Deployed Security Operations Center for several clients including a fortune 300 company.

- 24X7 Cloud/On-Prem SOC monitoring for Azure, AWS, GCP and On-Prem.
- Managing projects from end to end to deploy and kick off Security Operations.
- Created security operations strategies for cloud and on-prem monitoring, including 40+ integration guides for clients to follow and assisted the clients by providing scripts for automated deployment.
- Created hundreds of analytical rules and countless dashboards.
- Created several automation playbooks:
  - to ingest logs/alerts/threat intel feeds etc
  - to sync incident updates between Sentinel and Cherwell/ServiceNow
  - to integrate high priority alerts to Teams for quick visibility
  - to prioritize incidents from critical infrastructure
  - to take commands from analysts through Teams to perform actions like blocking a user /IP/URL/email, scanning, and quarantining a host, blocking execution of a program etc
  - for pre analyzing the files' and entities' reputation using scanning tools.
- Training the teams for investigation, building use-cases / analytical rules and SOAR, dashboarding, KQL queries etc
- Security risk assessment along with vulnerability and threat management, compliance checks against infrastructure for HIPPA, CIS and PCI DSS
- Researching and testing new security tools/products and making comparison matrix along with recommendations of tools to be implemented in the SOC.

Software Engineer
Nov 2018 – May 2020

Security Orchestraction

Worked as a part of DevOps and Security Engineering Team, on an enterprise grade SOAR product to improve response times, reduce risk exposure, and maintain process consistency. The orchestrator automates incident response by consolidating security tools in an organization.

- Develop and manage consistent and coherent DevOps processes and practices to support software development, testing, builds and deployment.
- Automation for Quality Assurance and Security Testing of orchestration platform. Automated around three thousand use cases with 20+ test suites with a mixture of Python Selenium, protractor, and shell scripts for an end-to-end testing with integrations with JIRA, Testrail and GitHub.
- Development of plugins for Orchestration platform to integrate with security platforms like Cuckoo sandbox, Anyrun, Nessus, NMap, OSINT tools etc. All development was done in python.
- Deployment and testing of security tools for integration with the Orchestration platform. These include Wazuh HIDS, Nessus, Cuckoo Sandbox, NMap, VT and other OSINT tools.

EDUCATION

Lahore University of Management Sciences

Lahore, Pakistan

BS Electrical Engineering
Sep 2014 – Jun 2018

Final Project – Smartphone apps fingerprinting using network traffic

In this project we captured Network Traffic being MITM and analyzed the traffic using Machine Learning to guess the Smartphone Application being used. We built a temporal profile of every user connected to our internet service. This profile is helpful in network security forensics and for providing better services by ISP.

TECHNICAL PROFICIENCIES

Security Operations and Intrusion Analysis / NSM / SIEM Tools:

Azure Sentinel, ELK Stack, Microsoft Defender Suite, Carbon Black Defense, Crowdstrike Falcon, Trend Micro Deep Security, QRadar, FireEye HX & NX, Wazuh, Rapid7, Splunk,

Cloud Security, Forensics & Assessments

Azure: Azure Sentinel, Defender Suite (Defender for Cloud, Cloud Apps, Office365, Endpoint, etc)
AWS: CloudWatch, GuardDuty, SecurityHub
GCP: Stackdriver and Security Command Center

Scripting & Automation

Python, BASH, PowerShell, Protractor, FireEye Security Orchestrator, Azure Sentinel Playbooks and Functions, RESTful APIs

EXTRA CURRICULAR

- Medical First Responder (MFR), Emergency Medical Services (EMS) – LUMS

Honors and Awards

- Fully Funded Undergraduate Program at LUMS – 2014-2018
- Summer Research Program Grant - 2017
- Chief Minister's Laptop Award - 2017