MUHAMMAD ASAD JAVED

Pen **T**ester | **SOC A**nalyst **L1** | **C**yber **T**hreat **A**nalyst | **C**yber **T**hreat **D**etection **E**ngineer

Geo-Location: Lahore, Pakistan
Contact Number: +92 341 3188833
Email: javed.asad959@gmail.com
LinkedIn Profile: https://pk.linkedin.com/in/maj-rav3n
Upwork Profile: https://www.upwork.com/freelancers/~010848e4c9991f48df

WHOAMI

Muhammad Asad Javed is a Cyber Security Enthusiast with 3+ years of experience in cyber domain. He specializes in both offensive and defensive security focusing on strengthening IT infrastructure security against advanced threats. He is well versed with offensive security including OSINT, reconnaissance, pen testing, vulnerability assessment, and vulnerability mitigation. He has a strong background in cyber security frameworks and compliance standards (NIST, PCI DSS, ISO, CIS, MITRE ATTACK, STIG DISA) and has hands-on experience with SIEM deployment (Splunk), threat intelligence, penetration testing, vulnerability management, and risk assessment. Asad is also skilled in implementing robust security mechanisms, such as strict authentication, endpoint security configurations, and granular access controls, and has developed custom vulnerability and endpoint misconfiguration scanners. He is passionate about optimizing security while maintaining resilience against cyber risks. He has trained 30 beginners in cyber security and thrives in diverse, challenging roles associated with cyber domain.

TECHNICAL EXPERTISE

- Network & Endpoint Pen Testing
- Web & Mobile App Pen Testing
- Vulnerability Assessment & Management
- Scripting (Bash, PowerShell, Python)
- Cyber Threat Simulation & Emulation
- Risk Assessment & Management
- Threat Modelling (Threat Modeler & Irius Risk)
- Blue Teaming
- Purple Teaming
- Cyber Threat Intelligence
- Cyber Threat Detection & Response
- Cyber Threat Hunting (MITRE ATT&CK)
- Vulnerability Assessment (Nessus) Deployment, Configuration, and Reporting
- SIEM (Splunk, Sentinel & CrowdStrike Falcon) Deployment, Configuration, and Administration
- Network Security (L2, L3, L5, L6, L7)
- Patch Management
- Endpoint Security Benchmarking (CIS)
- MITRE ATTACK, MITRE DEFEND, OWASP, Cyber Kill Chain, ISO 27001, ISO 27002, ISO 27007, NIST
- CVE, CPE, CWE, CVSS

UPWORK PROJECTS / ACHIEVEMENTS

- Executed penetration tests (Black Box, White Box) on networks, web apps, and mobile apps. Engaged with vulnerability assessments to meet business objectives as per compliance requirement (ISO, NIS, PCI DSS).
- Organized, planned, and responded to identified vulnerabilities during penetration testing. Mitigations were implemented within the context of cyber risks, time, and cost.
- Triaging (True/False Positives), investigating and responding to cyber incidents being a SOC Analyst. Providing recommendations to minimize overall potential risk and enhance cyber resiliency against cyber threats.
- Designed network connecting to branch networks via site-to-site IPsec VPN on Cisco edge routers (OSPF). Implemented Cisco IOS zone-based firewall (DMZ, Internal, External), extended ACLs, AAA server, and layer 02 security.
- Designed 3-Tier Campus Area Network with capabilities at core layer (EtherChannel, EtherGroup, NAT, PAT, EIGRP), distribution layer (RPVST, HRSP, EIGRP, DHCP, Inter-VLAN, RADIUS/TACACS), access layer (VLAN, Port Security, BPDU, Link/Port Aggregation, DHCP Snooping, Dynamic Arp Inspection).
- Designed 500+ Sigma cyber threat detection rules capable of being converted into various SIEM products.
- Conducted operational and tactical cyber threat intelligence (CTI) transforming raw data into proactive cyber threat response data.
- Optimized SOC processes and procedures incorporating MITRE ATTACK framework to detect and respond to cyber threats.
- Designed threat cases leveraging MITRE ATT&CK framework to detect cyber threats within the organization. Threat detection cases were tested, validated, and optimized against adversary emulations to analyze and enhance current SIEM threat detection surface for proactive cyber threat detection. The adversary emulation payloads were selected appropriately leading the payloads being under the SIEM radar. The new threat cases were developed, and the existing threat cases were optimized within the context of proactive detection data models for logs and their configuration. The threat cases were also mapped with MITRE ATT&CK framework matrices to identify the missing threat cases for sub-techniques as defined in MITRE ATT&CK framework.
- Designed STRIDE threat model based on Infrastructure as a Code. Integrated STRIDE threat modelling scheme with MITRE ATTACK, CAPEC, and CWE.
- Deployed CrowdStrike (EDR & SIEM) for Home Network. Simulated external and internal cyber-attacks to measure the overall security posture of Home Network.

EXPERIENCE

03/2023 – CONTINUE

INFORMATION / NETWORK SECURITY ANALYST, UPWORK

RESPONSIBILITIES & TASKS – SOC ANALYST L1

- Triaging incidents and classifying as true/false positives.
- Investigating incidents and alerts via MS Sentinel, MS Defender 365 for Endpoints, MS Defender 365 for Office, MS Entra ID, MS XDR.
- Providing feedback to each incident or alert for automation and tuning / optimization.
- Escalating incidents to clients as per SLA.
- Maintaining the SLA by prioritizing the response to incidents based on severity level.

RESPONSIBILITIES & TASKS – THREAT ANALYST & DETECTION ENGINEER

- Executing internal penetration testing (Black Box & White Box).
- Analyzing the latest APTs tactics, techniques, and procedures.
- Mapping latest APTs tactics, techniques, and procedures with MITRE ATTACK framework.
- Simulating the APTs' TTP trends.
- Designing and developing Sigma threat hunting **(**Breach Specific**)** rules and Sigma threat detection **(**Breach Agnostic**)** rules for breach articles publicly available.
- Testing and validating the Sigma rules to avoid false positives.
- Reviewing Sigma rules of peers to ensure detection framework is followed throughout threat detection life cycle.

01/2022 – 03/2023

SECURITY PRODUCT ENGINEER, EUNOMATIX

My focus is integrated with defensive security and offensive security as well.

RESPONSIBILITIES & TASKS

- Automated log management and ensured consistency, simplifying **50-250** endpoint management by configuring the Splunk deployment server.
- Optimized data ingestion, improving **20%** SIEM performance and reducing 10% resource utilization by implementing efficient log forwarding and preprocessing rules.
- Enhanced the organization's ability to detect and respond to security incidents by conducting research on data models for proactive endpoint log configuration.
- Optimized **10%** storage requirements and facilitated threat detection by establishing raw data filtering and formatting rules.
- Contributed to reduce **2-5** seconds data analytics response time within the organization by streamlining Splunk cluster configurations.
- Detected and responded to cyber-attacks, minimizing security breaches with lightweight SIEM queries.
- Enhanced cyber threat resiliency by integrating **6** open-source threat intelligence platforms and fortifying the organization's defenses.
- Provided a comprehensive understanding of potential threats and vulnerabilities by analyzing and mapping **150+** cyber threats to the MITRE ATTACK framework.

- Identified threat detection gaps and mitigated security incidents by designing and executing test payloads.
- Validated **450** threat detection rules and enhanced security posture through adversary emulations.
- Achieved a proactive response to evolving threats by optimizing threat detection cases with **35** custom-defined payloads.
- Ensured the security and observability of containerized applications by monitoring the Kubernetes environment with cilium, Hubble, Prometheus, Grafana advanced tools.
- Shared insights and best practices with industry peers and stakeholders by presenting project demos at various public sectors and expos, including the defense expo in Karachi.

06/2021 – 01/2022

JUNIOR CYBER SECURITY AUDITOR, EUNOMATIX

As a Junior Cyber Security Auditor, my responsibilities and tasks were to analyze the incorporated cyber security policies and controls within licensees' IT infrastructure as per defined in PTA cyber security standard.

RESPONSIBILITIES & TASKS

- Integrated cyber security procedures with industry standards, ensuring compliance of licensee with PTA best practices.
- Ensured strict adherence to PTA cyber security guidelines, safeguarding critical infrastructure and data.
- Increased licensee compliance with PTA cyber security guidelines, reducing vulnerabilities and strengthening security.
- Demonstrated commitment to customer-specific needs by developing tailored cyber security policies meeting PTA compliance standards.
- Provided comprehensive guidance for efficient implementation and maintenance of PTA cyber security standards, enhancing cyber resilience.
- Consulted and implemented cost-effective cyber security policies, ensuring compliance while optimizing resources.
- Leveraged proactive measures that improved cyber resilience and reduced the potential impact of security incidents.
- Communicated complex concepts to non-technical audiences, enhancing customer cyber literacy.
- Produced detailed audit reports with actionable recommendations, helping clients enhance their security postures.
- Received client commendations for the quality and clarity of audit reports, fostering stronger partnerships and client trust.

12/2020 – 05/2021

IT & Network Support Intern, NIMIR Resins Limited

Being an intern, I worked on IT & Network support, and cyber security related tasks.

RESPONSIBILITIES & TASKS

- Installed and configured new hardware, ensuring seamless integration into the network infrastructure.
- Resolved **15-30** hardware and software issues, minimizing downtime, and optimizing productivity.
- Streamlined user access while maintaining security through user account policies and permissions and enhancing data security and access control.
- Delivered prompt and effective technical support to **6** internal departments and **50** employees, maintaining user satisfaction and system functionality.
- Improved system visibility and allowed for continuous maintenance and optimization through PRTG deployment.
- Enhanced **80%** network and end system observability for data-driven decision-making using monitoring tools.
- Mapped network architecture of **120** network assets, facilitating a better understanding of the network's structure and dependencies.
- Implemented network security improvements, reducing vulnerabilities, and strengthening overall security by configuring network/web scans using NESSUS PRO.
- Monitored, investigated, and responded to SOPHOS alerts, enhancing system resilience.

EDUCATION

03/2015 – 06/2019

- **BS Electrical Telecom Engineering,** COMSATS University Islamabad

TRAININGS & CERTIFICATIONS

CONTINUE
CCT - Certified Cyber Security Technician
EC-Council

03/2023
CEHv12: Certified Ethical Hacker
IP Specialist

03/2023
Practical Ethical Hacking
TCM Security

03/2023
Web Hacking Expert: Full Stack Exploit
Code Red (EC-Council)

03/2023
Kubernetes Security Specialist
IP Specialist

03/2023
Kubernetes Administrator
IP Specialist

03/2023
CompTIA Cloud Essentials
IP Specialist

09/2022
Certified Hacking Forensic Investigator
DigiPakistan

09/2022
Associate Penetration Tester
DigiPakistan

09/2022
National Cyber Secure
NIAIS

02/2022
Python
NIAIS

09/2021
Ethical Hacker Trainee
Programmers Force

09/2021
SOC Analyst L1
Cybrary

11/2020
Cisco CCNA
PNY Trainings

01/2021
Network Monitoring System Workshop
PNY Training

ACTIVITIES

I utilize some of my time in doing random activities.

- Reading Books (Defensive & Offensive Security), official documentations, guides, cookbooks.
- Web and mobile application pen testing.
- Learning malware development, defense evasion.
- Digging into depth of operating systems (Windows, MAC OS, Android).
- Researching and exploring open-source platforms that can be utilized with defense and offense.
- Exploring cyber security frameworks and mapping the use cases with my experience.
- Exploring open-source tools that can be incorporated with organizations' requirement and operations.
- Cooking
- Gaming (SONY Playstation 5)