Zamen Shakeel

(703) 220-1446 / **US Citizen** / Northern Virginia / zamen.shakeel@gmail.com/Clearance Eligible

## Education

**George Mason University**, Fairfax, VA**:**

* B.S. Information Technology; **Dec 2021**

**Northern Virginia Community College**, Annandale, VA**:**

* A.S. Information Technology; **Dec 2018**

## Work Experience

Cyber Security Analyst - EY April 2022 – Present

* Participating in detecting, investigating, and resolving network and host-based security events while also developing analytical procedures to improve security incident identification efficiency.
* Utilized Splunk and Microsoft security suite to monitor and analyze network traffic, log data, and security events.
* Developing and implementing incident response plans, including documentation of findings and recommendations for mitigation.
* Conducting detailed security event analysis from network traffic attributes and host-based attributes, such as binary analysis, to identify information security incidents.
* Serving as an escalation point for difficult issues and complex inquiries, providing documentation and further project support.
* Identifying and suggesting areas for improvement within the Cyber Defense Response Center on security control capability gaps based off security intrusion trends.
* Conducted proactive threat hunting to identify and mitigate potential security threats and vulnerabilities.

NOC Engineer - Kymeta June 2021 – Nov 2021

* Diagnosing and resolving network-related issues, including connectivity problems, outages, and performance degradation.
* Configuring, optimizing, and supporting network devices, including routers, switches, firewalls, and load balancers.
* Maintaining accurate and up-to-date documentation of network configurations, topologies, and procedures.
* Assisted in disaster recovery planning, testing, implementation, and documentation.
* Managed ticket queues for various clients/networks and escalations to internal departments/external providers to ensure timely resolution.
* Managed SLAs and provided reporting to NOC leadership around Published SLAs.

IT Support Specialist - Oceana Feb 2020 – June 2021

* Troubleshooting and resolving hardware, software, and network issues for end-users.
* Managing access permissions and security settings for user accounts.
* Performing system administration tasks, such as server monitoring, user account management, and backup operations.
* Creating and updating knowledge base articles to facilitate self-help for end-users.
* Conducting training sessions for end-users on basic IT skills and software applications.
* Assisting in the planning and implementation of technology upgrades and migrations.
* Implementing and enforcing security policies to protect IT systems and data.
* Administering Rapid7 InsightIDR tool for incident detection, authentication monitoring, and endpoint visibility
* Utilizing Trend Micro Apex Central security console to investigate threats.

Certifications

GIAC Security Operations Certified (GSOC) **February 2023**

CompTIA Security+ ce – SY0-601  **July 2024**

## Skills

**Operating Systems**: Windows, Ubuntu, Unix - Kali Linux, MacOS

**Applications**: Cisco Packet Tracer, VMware, Wireshark, Metasploit, Nmap, VirtualBox

**Tools**: ServiceNow, Microsoft Defender, Microsoft Azure AD, Microsoft Defender for Cloud Apps, Palo Alto Cortex XSOAR, Carbon Black, Symantec Endpoint Protection, ThreatGrid, Agari Email Security, Splunk Enterprise, InsightIDR, Microsoft Excel