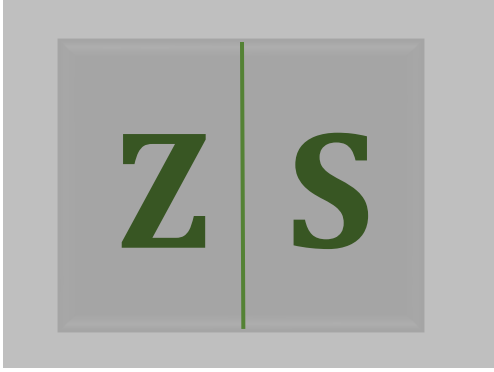
ZAIM SHAIKH



Phone: 469-233-7049

Email: Zash23@Outlook.com

Location: Dallas

LinkedIn: linkedin.com/in/zaims/

A detailed, analytical, results-driven Cybersecurity Analyst with a diverse background in network security management, incident response, vulnerability remediation, and compliance enforcement. Recognized as a security-focused professional and trusted support specialist – integrating and executing comprehensive strategies to fortify organizations against evolving cyber threats, leveraging cutting-edge tools and best practices to detect, prevent, and respond to incidents while significantly enhancing organizational resilience and overall security posture. A quick learner who thrives in fast-paced environments, with a keen ability to translate complex security challenges into practical solutions, strengthen defense-in-depth strategies, and contribute effectively to mission-critical security initiatives.

PROFESSIONAL EXPERIENCE

CYBERSECURITY ANALYST

InfoDefense **June 2025 – Present**

- Responded to incidents, led rapid detection, containment, and eradication of threats.
- Spearheaded cross-team tabletop exercises to fortify organizational readiness against sophisticated attacks.
- Managed FortiGate firewall architectures and FortiClient VPN solutions, and resolved critical connectivity and security issues.
- Strengthened cloud and endpoint security by administering Microsoft 365 portals (Defender, Intune, Entra, Exchange).
- Performed advanced threat hunting across multiple customer tenants, while uncovering hidden attack vectors, neutralizing emerging threats, and reinforcing enterprise-wide defenses.
- Neutralized high-risk phishing and email-borne threats through deep-dive investigations, advanced filtering strategies, and enterprise-wide awareness campaigns.
- Elevated vulnerability management programs by conducting targeted scans, issuing customer-specific vulnerability alerts, and delivering remediation strategies that closed high-priority gaps across infrastructures.
- Ensured regulatory compliance by developing and enforcing security policies and SOPs aligned with CMMC standards and supporting frameworks like NIST.
- Delivered executive-level reports, including SIEM analyses, endpoint protection summaries, security awareness, and compliance readiness reports to equip leadership with actionable intelligence for risk-based decisions.

CYBERSECURITY ANALYST

Petmate **August 2023 – June 2025**

- Monitored, identified, and responded to network/security related events from various sources to determine the appropriate course of action, including troubleshooting, mitigation, resolution, or escalation.
- Designed a ransomware response playbook, and led incident response procedures, including detection, analysis, containment, eradication, and recovery to minimize the impact of security breaches and ensure the timely restoration of systems and services.
- Bolstered the organization's cyber resilience by overseeing a cross-functional security team to remediate critical vulnerabilities identified during penetration testing and risk assessments.
- Supported security audits, including PCI DSS and cyber insurance assessments, by implementing and documenting security controls aligned with NIST CSF and CIS benchmarks to ensure compliance and reduce risk.
- Researched and tracked emerging threats and maintained up-to-date expertise through continuous training to anticipate and counter evolving attack vectors.
- Authored and enforced robust security policies, including vulnerability remediation, stringent BYOD guidelines, fortifying data integrity, and mitigating cyber risks.
- Deployed and administered endpoint security solutions, and ensured all company devices were equipped with Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), and other essential security tools.
- Created easy-to-follow documents for end users as well as other IT personnel, (SOPs).
- Utilized security tools such as Proofpoint and Mimecast to investigate email-based threats, mitigate phishing attacks, and augment overall threat detection capabilities.

IT INTERN – NETWORKING, HELPDESK

Kehr Technologies **August 2022 – October 2022**

- Analyzed network security issues, identified root causes, and devised effective solutions to mitigate risks and enhance the overall security posture of the network infrastructure.
- Managed critical DNS infrastructure, and performed meticulous record updates, renewals, and configurations to maintain a seamless internet presence and optimize performance.
- Enabled secure VPN access, empowered remote workforce connectivity while maintaining strict security measures, encryption protocols, and safeguarding organizational data.

EDUCATION & CERTIFICATIONS

COLLIN COLLEGE, FRISCO, TX

Bachelor of Applied Technology in Cybersecurity | December 2023

Associates of Applied Science in Information Systems Cybersecurity | May 2022
GPA: 3.7/4.0

Cisco Certified Network Associate (CCNA)
CompTIA CySA+ | CompTIA Security+
CompTIA Network+ | CompTIA A+
(ISC)² Certified in Cybersecurity
AI Solutions on Cisco Infrastructure Essentials (DCAIE)
CWT - Certified Wireless Technician
Microsoft Office Specialist Certifications

SELECTED COMPETENCIES

- Technical Support and Help Desk Management
- Security Monitoring and Incident Response
- Route/Switch Protocols
- Firewall Configuration and Management
- Secure VPN Deployment
- SIEM Integration & Threat Intelligence
- Data Security and Privacy Compliance
- Remote Support and Diagnostics
- Security Protocols and Data Protection
- Project Management and Task Prioritization
- Security Awareness & Phishing Defense
- Communication & Interpersonal Skills
- Hardware and Software Integration

TECHNICAL SKILLS

Network Administration: Network deployment and segmentation, Routing & Switching, TCP/IP Networking, BGP, OSPF, STP, Software, Hardware, and Network Troubleshooting
Cybersecurity Tools: Proofpoint, Mimecast, Bitsight, InfoSec IQ, M365/Entra/Azure/MS Defender, SentinelOne, Huntress, Cisco Umbrella, Blackpoint, Fortinet and Zyxel Firewalls, Qualys, Tenable, Adlumin MDR, Wazuh SIEM, KnowBe4, DFIR-IRIS
System Administration: Track-it ticketing, Jira ticketing, NinjaOne, ADManager Plus, ADAudit Plus, PowerShell, Python, Active Directory, Hyena, Atera, Splashtop remote monitoring, MobaXterm, Advanced IP Scanner, NordVPN, NordLayer, Cisco Meraki, Meraki Systems Manager, Intune MDM, ITOP Ticketing
Vulnerability Assessment: Nessus, Google Dorking, Wireshark, Nmap, Zenmap, CIS, NIST, Greenbone Security Assistant
Productivity & Collaboration Tools: Password managers, Microsoft applications, Google Workspace