

Liz Ude, Cyber Security/Information Security

07577957991, elizabeth.ude@outlook.com

Summary

I am a passionate and motivated Cybersecurity Analyst with hands-on experience in identifying and addressing threats to IT systems and networks. With a solid understanding of security operations and threat analysis, I am constantly learning and applying new skills to help protect critical information assets. I have experience conducting assessments of threats and vulnerabilities, and I'm focused on recommending practical mitigation strategies. I'm eager to continue growing within a collaborative team, where I can bring my adaptability, enthusiasm, and problem-solving mindset to strengthen overall security efforts.

Work Experience

Apr 2024 - Present	Security Operation Center Analyst, Cloud Connectiv	Remote
	Managed and triaged security incidents, ensuring timely resolutions in alignment with SLAs, which improved incident response times and minimized security risks.	
	Assisted clients during onboarding, conducting assessments to provide tailored recommendations, resulting in enhanced user experiences and smoother transitions to secure environments.	
	Conducted proactive threat hunting using SIEM tools to identify anomalous activities, strengthening overall security posture by detecting and mitigating potential breaches early.	
	Developed and maintained a knowledge base of troubleshooting guides and best practices, improving operational efficiency and response times across security and support teams.	
	Tailored security recommendations based on assessments, aligning client needs with best practices and strengthening security measures to meet organizational requirements.	
Nov 2023 - Mar 2024	Cyber Security Technician, Firebrand Training (Contract)	Remote
	Developed expertise in cloud security by monitoring and securing IaaS, PaaS, and SaaS platforms, including Azure AD, Microsoft 365, and Azure Security, ensuring robust protection of cloud-based environments.	
	Managed virtual deployments in Azure, overseeing IAM and Security groups across various environments, enhancing security controls and streamlining access management.	
	Implemented industry-standard security frameworks (ISO 27001, NIST CSF, GDPR, PCI DSS, HIPAA), elevating compliance and ensuring alignment with organizational security policies.	
	Applied NIST and ISO 27001 frameworks to design and enforce security policies, leading to improved compliance and strengthened operational security for diverse environments.	
	Configured and managed security tools such as firewalls, antivirus software, and IDS/IPS systems, demonstrating a high proficiency in threat prevention and mitigation strategies.	
	Enhanced cloud security posture by applying best practices and monitoring techniques, ensuring adherence to regulatory standards and reducing security risks across platforms.	
Jul 2022 - Jul 2023	Cyber Security Associate, Grant Thornton	London
	Optimized threat detection in Microsoft Sentinel, leading to a 20% increase in identified security incidents and a 15% reduction in false positives, enhancing the SOC team's threat detection and response efficiency.	
	Reduced mean time to detect threats by 30% through real-time log analysis on platforms such as Carbon Black and Microsoft Sentinel, improving the overall incident response process.	
	Implemented Azure AD security controls in collaboration with cross-functional teams, ensuring a secure and compliant IT infrastructure for cloud-based assets.	
	Investigated and contained security incidents using KQL queries in Microsoft Sentinel, preventing unauthorized access and data exfiltration through immediate remediation actions.	
	Enhanced network security measures by resolving malware infiltration issues, conducting thorough analyses, and delivering tailored security recommendations.	
	Presented actionable insights to stakeholders by translating complex security reports, fostering organization-wide understanding of security issues and compliance measures.	

Nov 2021 - Jul 2022	IT Support/Customer Service Specialist, Odondo	Remote
	Led multi-channel customer support (phone, email, chat), efficiently resolving technical issues and ensuring high levels of customer satisfaction across various touchpoints.	
	Implemented a self-service knowledge base, reducing IT support queries and empowering users to troubleshoot common issues independently, improving operational efficiency.	
	Developed a customer feedback system, driving a 10% increase in positive reviews and enhancing service quality through continuous improvement efforts based on user insights.	
	Facilitated smooth process transitions by leading training sessions for new system implementations, minimizing user resistance and ensuring seamless adoption of new technologies.	
	Resolved hardware and software issues through hands-on troubleshooting, routine maintenance, and security configurations, maintaining system integrity and functionality.	
	Demonstrated strong communication skills by effectively documenting and simplifying technical information, enabling both technical and non-technical stakeholders to understand key issues and solutions.	
Jul 2019 - Sep 2019	Cyber Intern, SRM Corporate Intelligence, Crisis management and Cyber security	London
	Assisted in penetration testing, identifying critical vulnerabilities and recommending security enhancements that significantly improved system defenses.	
	Leveraged Splunk for security monitoring, increasing incident detection accuracy and response effectiveness through comprehensive threat analysis and real-time data insights.	
	Contributed to the development and audit of Information Security policies, SOPs, and standards, ensuring compliance and improving security governance across business units.	
	Executed phishing simulation campaigns, increasing user awareness and reducing the organization's susceptibility to phishing attacks, strengthening overall cybersecurity culture.	

Education

Sep 2018 - Jun 2020	Cyberpsychology , Nottingham Trent University (MSc)
	Computer Forensics
	Psychology of Cyberspace and Online Behaviors
	Applied Psychology of Digital Technologies
Sep 2014 - Jun 2018	Telecommunications and Computer Network Engineering, London South Bank University (BEng)
	Computer Systems and Networks
	Network Security Engineering
	Digital Techniques

Certifications

Sep 2023	CompTIA Security+, CompTIA
Nov 2023	CertNexus, CertNexus
Jan 2024	BCS CISMP - Certificate in Information Security Management Principles, BCS, The Chartered Institute for IT
Apr 2024	Microsoft Security, Compliance, and Identity Fundamentals, Microsoft

Skills

Endpoint Detection and Response	Experienced	Microsoft Azure	Experienced
SIEM	Experienced	Security Operations	Experienced
Research	Expert	Teamwork	Expert
Threat Intelligence	Experienced	IDS/IPS	Experienced
Linux	Experienced	TCP/IP Networking	Experienced
Cyber Security Engineer	Beginner	Malware analysis	Beginner
Network Forensics	Beginner	Penetration Testing	Experienced
Threat Detection	Experienced	Data Loss Prevention	Beginner
Python	Beginner		