LARAIB SARMAD

sarmadlaraib@gmail.com | 845-793-6654 | www.linkedin.com/in/laraibsarmad | github.com/LaraibSarmad | NY, US

INCIDENT RESPONSE | IT RISK MANAGEMENT| AUDIT & GOVERNANCE

Cybersecurity professional with hands-on experience in incident response, threat detection, and vulnerability management. Improved SOC efficiency by 30% and reduced incidents by 47% through automation and structured escalation. Proficient in Microsoft Sentinel, Defender, Qualys, Azure, Intune, and Active Directory. Experienced in applying NIST, ISO 27001, and SOC 2 frameworks in high-pressure, 24/7 operational environments.

SKILLS | TECHNOLOGIES | QUALIFICATIONS

Security Tools and Technical Skills: Microsoft Sentinel, Defender (Identity, Cloud), Intune, Azure, QRadar, Splunk, Active Directory, Cisco Defense Orchestrator, Meraki, Qualys (w/ Container Security), Syslog, Freshdesk, Intrusion Detection, IT Security

Network Architecture & System Security: Firewalls, IDS/IPS, VPN, DNS, XDR, MFA, EDR, IAM, Access Control, Security Protocols, Network Security, Networking Protocols, Patch Management, Server Administration, Endpoint Security

Cloud & DevSecOps: Azure, AWS, GCP, Docker, Kubernetes, Cloud Security, SOAR, CI/CD, DevOps, OS Hardening

Cybersecurity Operations & IR: Threat Detection, Incident Investigation, Root Cause Analysis, Gap Analysis, Vulnerability Assessment & Management, Log Analysis, Data Classification, Threat Intelligence, Incident Handling, DDoS Mitigation

Governance, Risk & Compliance: NIST, ISO 27001, SOC 2, HIPAA, GDPR, PCI DSS, HITRUST, MITRE ATT&CK, ITIL, Third-Party Risk, Compliance Management, Security Controls Deployment, Internal Audits, Regulatory Reporting

Security Testing & Assessment: Penetration Testing, Malware Analysis, Application Security, Code Review, Security Audits, Security Testing, Business Continuity Planning, Risk Reduction, Control Testing, Data Governance, System Architecture

Programming, Scripting & OS: Python, PowerShell, Bash, SQL, KQL | Microsoft Windows, Mobile Devices OS

Productivity & Documentation: Microsoft Office Application (Word, Excel, PowerPoint, Outlook, OneNote), Visio, SharePoint, Project Management Tools, Policy Writing, SOP Development, Management Information Systems, Manage Documentation,

PROFESSIONAL EXPERIENCE

Cyber Security Analyst | HIAS (Hebrew Immigration Aid Society) 11/2023 – 3/2025

- Investigated and triaged **1,000+ monthly security events**, leveraging log analysis, threat intelligence, and SIEM tools to identify root causes, contain threats, and deliver actionable insights via custom-built dashboards.
- Developed and maintained incident response playbooks and SOPs aligned with **ISO/IEC 27001**, reducing security incidents by **47%** through pre-defined timelines and escalation paths.
- Performed in-depth vulnerability assessments using **Qualys**, focusing on Docker and endpoint misconfigurations; automated remediation processes and improved SOC (Security Operations Center) efficiency by **30%** through documented escalation workflows.
- Delivered frontline response during global security incidents, ensuring timely containment, coordinating remediation across departments, and providing clear incident summaries for leadership.
- Managed social media threat investigations (doxing, impersonation) and implemented proactive security monitoring strategies to

support a **risk-based ISMS** approach, reducing exposure to reputational attacks.

- Collaborated with **legal, IT, and global safety teams** to assess **vendor risk,** respond to security questionnaires, and ensure data handling met compliance expectations.

IT Support Consultant | Pace University 08/2022 -05/2023

- **Implemented vulnerability scanning on different Operating Systems (OS)** using **Malwarebytes, VMware,** and **other EDR solutions**, reducing security incidents and improving **incident response time** by 20%.
- Spearheaded **risk mitigation strategies** to enhance data integrity, reducing breaches by 20% and optimizing **incident management** strategies.

Information Security Program Assistant | Pace University 01/2022 – 05/2022

- **Executed ethical hacking simulations, digital forensics initiatives and tabletop exercises with social engineering techniques** like phishing and pretexting to identify vulnerabilities in human behavior.
- **Led daily cybersecurity exercises to gain** leverage in refining incident response procedures, contributing to a **20% overall reduction in risk.**

EDUCATION & SECURITY CERTIFICATION

Bachelor of Science in Information Technology | Computer Science | Concentration: **Information Security & System Assurance** | Minor: Criminal Justice (Law) | Pace University | **SANS (Blue Team: Security Operation & Analysis) | Digital Transformation Google Cloud, 08/23 | CompTIA Sec+(Expected June2025)**