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 detection, log analysis, and cyber defense within dynamic environments. Skilled in triaging security events, performing root cause analysis, and documenting detailed investigation reports. Proficient in Microsoft Sentinel, Power BI, and Qualys, with working knowledge of NIST and ISO frameworks to support scalable incident response operations. Known for collaborating with cross functional teams and adapting quickly in high-pressure, 24/7 operational settings.

SKILLS | TECHNOLOGIES | QUALIFICATIONS

Security Tools and Technical Skills: MS Sentinel, MS Defender, Microsoft Azure, Microsoft Intune, Microsoft Office, QRadar, Splunk, Sentinel, Active Directory, Wireshark, DNS, Firewalls, XDR, MFA, EDR, IAM, Nmap, Qualys, Cisco Defense Orchestrator, Meraki, Trivy, CVE, CVSS, Qualys Container Security, Docker, Kubernetes, Security Risk Assessment, Risk Reduction, Technology Architecture, Malware Analysis, Cyber Defense, Application Security, Software Development Life Cycle, Lead Development, Code Review, Source Analysis, Access Control, Security Protocols, IT Security, Security Architecture, GRC, Penetration, Data Analysis, Report Writing , Documentation, Cloud Computing, Security Automation, Syslog administration, Incident Investigation, IDS/IPS, Virtual Desktop, Networking Protocol, Risk Assessment, Cloud Security, Vulnerability Assessment, Vulnerability Management, Process Review, Incident Handling, Security Monitoring, Threat Intelligence, IT Compliance, Freshdesk, Endpoint Security

Cybersecurity Incident Response: Root Cause Analysis, Gap Analysis, Vendor Management, Log Analysis, Threat Detection, Security Testing, DevOps, Research, Network Traffic Analysis, Network Security, Network Administration, Control Testing, Data Extraction, Data Classification, Patch Management, OSI, Management, Server Administration, Remediation, Security Audits, Infrastructure Security, Information Science, Computer Engineering, IR, Third Party Risk Management, Intrusion Detection, Business Process, Business Continuity, Compliance Support, Reporting, Awareness Simulations, Data Security, CI/CD, L1/L2, Reporting, Security Controls Deployment, Internal Audits, DDoS Mitigation, Data Loss
Protection (DLP), MDR, Disaster Recovery, Data Governance, Principle of least privilege, Privacy Policies Regulations, Compliance Management

Framework, Standards and Procedures: NIST, ITIL, MITRE, ISO, SOC 2, HIPAA, GDPR, FFIEC, OWASP, ISO, PCI DSS, HITRUST, TCP/IP, Policy Writing, Windows, Linux/Unix, Mac, AWS, GCP, SharePoint, Management Experience, Identity Access Management, SOPs

Scripting/ Computer Programming Languages: Python, Bash, SQL, Java, Scripting, KQL, C#, JavaScript, Powershell

Security Compliance & Auditing: Regulatory Compliance, Monitoring, SSL, HTTPS, LDAP, COBIT, System Administration, Confidentiality Maintenance, Bitlocker, Microsoft Excel, Visio, Word, OneNote, PowerPoint, Outlook, Project Management, IT Audit

PROFESSIONAL EXPERIENCE

Cyber Security Analyst | HIAS 11/2023 – 3/2025

- Conducted comprehensive vulnerability assessments of applications and containerized environments using Qualys, Nessus, and Trivy, identifying runtime misconfigurations and security gaps in Docker workloads. Streamlined remediation workflows and drove a 30% improvement in SOC team efficiency through targeted automation, internal communications, and structured escalation processes.
- **Developed and maintained cybersecurity playbooks and SOPs (Standard Operating Procedure) for various sectors including utilities, incorporating incident timelines and escalation procedures reducing incidents by 47%.** Conducted threat hunting and engineered security solutions, mitigating 50+ threats, enhancing defenses, and providing recommendations for future security improvements.
- Tracked and analyzed over **1,000** cyber incident logs monthly, performing incident tracking, and correlating data from various sources for identification of **root causes, vulnerabilities, and failed defenses, reducing response times by 25%.** Built a **threat dashboard** to **visualize key indicators** and trends. Managed external SOC communication for high and critical alerts, ensuring executive-level management and stakeholders received timely updates to support informed decision-making.
- **Collaborated** with cross-functional teams, stakeholders, and external partners during **escalated incidents** and emergencies, leading crisis management, ensuring **rapid response** and **business continuity**. **Led investigations**, generating reports and executive summaries quarterly.
- **Managed** Physical and Global Security efforts by **monitoring social media threats**, including **doxing and impersonation**. Investigated incidents, coordinated remediations, and bridged gaps between teams to strengthen internal communication, response timelines, and

organizational risk posture in alignment with the Information Security Management System (ISMS).

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 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 Systems and Assurance** | Pace University |
SANS (Blue Team: Security Operation & Analysis) | Digital Transformation Google Cloud, 08/23 | CompTIA Sec+(Expected June2025)