Luca Iannino

Cybersecurity Analyst

Andover, MA 01810
(781) 632-0894
lu.iannino@gmail.com
www.linkedin.com/in/lucaitechnology
portfolio: lucaitech.github.io

Strengthening Security Posture through Proactive Threat Detection, Incident Response, and SIEM Optimization

Proactive Cybersecurity Analyst with strong IT and enterprise security expertise across finance, healthcare, and biopharma. Skilled in vulnerability management, threat monitoring, incident response, and access controls. Experienced in securing systems, streamlining workflows, and enforcing compliance to reduce risk. Collaborative and growth-driven, with a strategic approach to cybersecurity as a driver of trust and resilience.

CORE COMPETENCIES

Cyber Operations | Identity and Access Management (IAM) Multi-Factor Authentication (MFA) | Knowledge Management Security Perimeter Tools | Security Incident Management Security Operations Center (SOC) Management | Endpoint Security | Malware Analysis | IT Operations | Security Monitoring | IP Threat Investigation | Windows System Administration | Web Application Architecture | Content Filtering | Threat Detection | Vulnerability Scanning | Firewall Log Investigation | Intrusion Detection | Security Metrics and Reporting | Security Infrastructure Management | Compliance (SOC 2, NIST, ISO 27001)

PROFESSIONAL EXPERIENCE

Eliassen Group/Loomis Sayles – Boston, MA | Nov 2023 – Present

Security Analyst

Perform security analysis, vulnerability scanning, and incident response to improve defenses and support enterprise risk mitigation.

- Detect and analyze potential threats using Falcon CrowdStrike and SIEM platform management, ensuring timely incident handling.
- Develop and refine security workflows and procedures to increase operational efficiency and maintain compliance standards.
- Lead cybersecurity training for end users and assess third-party software, improving organizational security and compliance.
- Enhanced IRP maturity by benchmarking against best practices, identifying key gaps, and presenting strategic fixes to the CISO.
- Strengthened security posture by identifying and remediating 150+ vulnerabilities through targeted Rapid7 scans and remediation efforts.
- Achieved SOC 2 readiness by closing compliance gaps, standardizing audit documentation, and aligning controls with NIST standards.
- Reduced phishing incidents by 40% through data-driven awareness campaigns and interactive cybersecurity workshops for 100+ staff.
- Reduced risk exposure by validating 50+ vendor applications for security and compliance before production deployment.

Sevita Health – Boston, MA | Jan 2022 – Nov 2023

IT Help Desk Technician

Provided IT support and security monitoring for a large enterprise with more than 45,000 end users as well as multiple departments.

- Ensured incident resolution by escalating issues to management and on-call teams, minimizing system downtime and disruptions.
- Secured enterprise systems by resetting AD passwords, managing server and mailbox permissions using DataPrivilege and Varonis Advantage.
- Strengthened data security by managing access controls and permissions for 500+ user accounts through Active Directory and Varonis.
- Prevented unauthorized access by deploying MFA via PINGID and SMS for 400+ users, significantly enhancing overall cyber defense posture.
- Delivered 95% customer satisfaction by efficiently resolving 200+ weekly support tickets and maintaining high service responsiveness.

Ocular Therapeutix – Bedford, MA | Jul 2019 – Dec 2021

IT Deskside Analyst

Delivered technical support and handled the user onboarding /offboarding for a 3-person IT team in a BioPharma setting.

- Preserved data integrity by automating Office 365 mailbox backups for departing employees via Veeam, ensuring compliance.
- Strengthened support efficiency by mentoring technicians in troubleshooting, maintenance, and documentation creation.
- Reduced credential-based attack incidents by implementing and enforcing Duo 2FA for secure remote access across all endpoints.
- Enhanced security by managing 300+ user accounts, enforcing strict IAM policies, and revoking credentials to prevent threats.
- Enhanced security by managing 300+ user accounts, enforcing strict IAM policies, and revoking credentials to prevent threats.
- Blocked 25% of threats before reaching end users by optimizing Mimecast phishing and malware filters for threat mitigation.

EDUCATION & PROFESSIONAL DEVELOPMENT

Bachelor's Degree, Salem State University
Associate's Degree, Bunker Hill Community College
Certifications: CompTIA Security+ | Google Cybersecurity Specialization, Google | EDX /IBM Cybersecurity Compliance and Framework | ISACA CISA (In Progress)

TECHNICAL SKILLS

CrowdStrike | Splunk | Rapid7 | Wiz | Varonis | Mimecast | Active Directory | Azure | Microsoft Office Suite (Word, Excel, PowerPoint)