ALBIN JOHN SEBASTIAN

Scarborough | 6478659446 | albin@johnsafe.tech | LinkedIn | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity professional with over 3 years of experience in monitoring security systems, penetration testing, vulnerability assessment and threat hunting. CompTIA Security+ and Google Cybersecurity certified. I bring expertise in SIEM, malware analysis, exploit development and zero trust architecture. Proven track record in securing systems, mitigating risks and ensuring compliance with industry standards(NIST 2.0). Eager to apply my technical skills to strengthen cybersecurity defenses and collaborate with cross-functional teams eager to strengthen cybersecurity defenses.

TOOLS

BRUTEFORCE: BurpSuite, Metasploit, msfvenom, Hydra, John The Ripper, Armitage.
RECONNAISSANCE: nmap, gobuster, SQLmap, Maltego, spiderfoot, tcpdump, aircrack-ng.
NETWORK ANALYSIS: Wireshark, Suricata, tcpdump, netcat, packet analysis, IDS/IPS.
SIEM: Splunk, Wazuh
CONTAINERIZATION: Docker
EDR and UEM: Kaspersky EDR for Small Business, Microsoft Intune incorporated with MS Defender EDR.

SKILLS

TECHNICAL: Python, C, MySQL, bash, Powershell, Linux/Windows systems, Active Directory.
OFFENSIVE TECHNOLOGY: Pen-testing, exploit development, vulnerability assessment, malware analysis, OSINT.
SECURITY FRAMEWORKS: NIST 2.0, MITRE ATT&CK, OWASP Top 10, incident response playbooks.
NETWORKING & PROTOCOLS: TCP/IP, OSI model, VPN, IDS/IPS, routing protocols.
ADDITIONAL: Incident triage, security monitoring, remediation strategies, security audits

EXPERIENCE

CONCENTRIX
Technical Support Analyst (Cybersecurity) - L2 **November 2024 – May 2025**

- Configured firewalls on macOS for end-users and business devices, implementing packet/network filtering to block threats and secure client devices and networks.
- Handled macOS security issues like VPN setup and antivirus scans using Malwarebytes, resolving support tickets to maintain compliance with security standards and keep end-devices safe.
- Provided support for macOS security issues, including data encryption(Filevault), malware analysis.
- Took over escalated cases from L1 support, demonstrating expertise in guiding solutions to ensure compliance and security; followed K-base procedures and made follow-up calls to clients.

Technical Support Analyst (Cybersecurity) - L1 **May 2024 – November 2024**

- Mitigated phishing and social engineering attacks by analyzing threats; educated users on malicious links and reducing account compromises through cybersecurity awareness training.
- Hardened iOS endpoint security via vulnerability troubleshooting and OS patching to implement latest security updates on end devices.
- Provided incident response for credential theft by recovering accounts and enforcing MFA/password resets followed by training clients on identifying phishing scams and the need for creating strong passwords.
- Identified and escalated severe vulnerabilities to engineering teams to speed up fixes and ensure compliance with organizational security policies.

—---

OFFENSO
Cyber Security Intern **October 2020 – October 2021**
Project: SIEM integration using Wazuh for Data Governance.

- Built a SIEM monitoring system with Wazuh and Docker, deployed in the Linode cloud, implemented real-time threat detection and incident response protocols.
- Monitored security events across multiple environments, reducing data integrity risks by 30% utilizing automated response suggestions from Wazuh and threat analysis techniques.
- Performed vulnerability scans and penetration tests using Burp Suite (SQL injection and XSS) to detect Web API vulnerabilities utilizing Repeater and Intruder, escalated severe incidents to senior analysts.

- Drafted vulnerability reports outlining identified vulnerabilities, exploitation techniques and provided actionable recommendations to mitigate risks.

—--

ARVIN TECHNOLOGIES

Security Analyst **August 2019 – June 2020**

- Incorporated Microsoft Intune to secure endpoints by configuring policies to protect remote access, ensured compliance with NIST standards.
- Managed endpoint security with MS Intune to implement remote wipes, password policies and antivirus scans using Microsoft Defender EDR to secure the corporate environment from attacks.
- Monitored security event logs for network and endpoints with Splunk, identifying potential threats to strengthen organizational defenses.
- Helped in incident response by investigating breaches and working to contain them quickly to reduce downtime.
- Conducted risk assessments and audits to make sure endpoint systems followed security policies and procedures with NIST standards.

Junior Security Analyst **December 2017 – August 2019**

- Conducted penetration testing, payload generation and post-exploitation analysis on wireless devices using Metasploit framework and aircrack-ng to analyze the security gaps.
- Utilized Wireshark and tcpdump to continuously monitor and ensure encrypted data trasnsfer resulting in minimizing wireless attacks and unauthorized access risks.
- Authenticated and authorized systems with automated tools to protect against unauthorized access and remote code injection.
- Escalated complex incidents to senior analysts providing detailed findings to implement aligning with industry standards.

PROJECTS

URL - https://johnsafe.tech/#working

- **DIY SIEM Environment**: SIEM solution using open-source tools for threat detection and incident response.
- **Remotely Control Any Devices Using Armitage**: for advanced penetration testing, simulating real-world attacks.
- **Create your own Server using CasaOS**: Configure a server with security best practices for efficient management.

EDUCATION

Postgraduate in IT Network Security - Conestoga College **2022 – 2023**

Bachelor's Degree in Computer Science - Mangalam College of Engineering **2013 – 2017**

CERTIFICATIONS

- CompTIA Security+ - Credly
- Google Cybersecurity Certificate - Coursera
- Practical Bug Bounty Hunting for Hackers and Pentesters - EC Council.
- SOC Member - LetsDefend
- Burp Suite Certified Practitioner - PortSwigger(in progress)