www.linkedin.com/in/zkalathiya
220 W Bell Rd, Phoenix, AZ - 85023

Zulin Kalathiya

571-508-8672
zkalathiya@hawk.iit.edu

EDUCATION

Illinois Institute of Technology, Master in **Cyber Forensics and Security** | GPA – 3.7/4 May 20
(Courses – *Vulnerability Analysis, Database Security, Cyber Forensics, operating system security, System Security)*
Veltech University, Bachelor of Technology in **Computer Science and Engineering** | CGPA – 3.6/4 May 18
(Courses – *Data Networks, Operating system, Object Programming, Database Management, Compiler Design)*

EXPERIENCE

Security Analyst, Early Warning Services, Phoenix, Arizona May 19 – Present

- Support internal static (**SAST**) and dynamic (**DAST**) analysis, including web applications, web services, and cloud-hosted application assessments using Fortify, Checkmarx, Veracode, black duck, and dependency-check.
- Perform timely **vulnerability scanning** on engineering infrastructure using a nexpose scanner and report the respective team with the mitigation.
- Have experience in **Security Assessment** for the product using techniques SQL Injection, XSS, Broken Authentication, etc.
- Work with architecture teams to ensure that all applications and implementations are in line with security policy and are in compliance with the required **frameworks** (ISO, PCI, OWASP, NIST 800-53, etc.)
- Lead the product line dashboard maintenance project for the entire security department to improve the visibility of about **~95%.**
- Triage software vulnerability and work together with software development teams to fix security bugs.
- Document all procedures within the security department.
- Conducts **threat modeling** activities for all applications and products in assigned verticals.
- Experience in managing **CDN Cloudflare** for Early Warning Services.
- Identify vulnerabilities, active exploits, and advanced cyber threats to help the business rigorously protect and strengthen the security posture using **Security Scorecard**.
- Advises and approves of changes and architectures for assigned areas from a security perspective.
- Perform Security Information and Event Management (SIEM) using **Splunk** by creating various personalized dashboards for active response and log analysis.
- Support weekly JIRA review meetings to identify and manage tickets based on the risk rating.
- Conduct and develop Early Warning' **Security awareness** training for IT and the business.
- Wrote python scripts to **fetch customized** data, data are encrypted end-to-end, at rest, and in transit with AES 256. Also customized HTTP header to fetch data that are not part of a documented API.
- Support Product Pen testing – Internal and External assessment process
- Manage **bug bounty** program and triage the findings and fix it by collaborating with different teams.

Cybersecurity Intern, **STQC,** Hyderabad, India May 17 - Mar 18

- Conducted vulnerability analysis with programs such as Nessus, Zen map, and Wireshark. Searched for suspect traffic, network topologies, and open/closed ports.
- Manage critical cybersecurity events in a central ticketing system from the time the event is detected through the alerting process
- Given the solution and coordinate with the end customer team to fix the vulnerability found in their environment.
- Provided customer support for installation, deployment, and configuration.
- Assist with the creation of written supervisory procedures, newsletters, and other documentation related to cybersecurity.

CERTIFICATION

- CompTIA **Security+**
- Certified Ethical Hacker (**CEH**)
- eLearn Security **WAPT**

TECHNICAL SKILLS

- **Programming / Scripting:** Python, Bash
- **Security Tools**: Nmap, Metasploit, Burp Proxy, Nmap
- **Security Testing Tools**: Checkmarx, Fortify, Veracode, Black duck, OWASP Top 10
- **Vulnerability Assessment**: Nessus, Nexpose, OpenVAS, Nikto
- **AWS** – Cloud Computing
- **Monitoring/Packet Capture**: Wireshark, tcpdump
- **Protocol**: TCP/IP, SSO, HTTP
- **Firewall**: Linux Firewall, ModSecurity(WAF)
- CASB (Cloud Access Security Broker)
- **Project Management Tool**: Jira, ServiceNow
- **Framework**: NIST, PCI DSS