***SUNITA SHARMA***  
Cypress, CA | (714) 616-8520  
[LinkedIn](https://www.linkedin.com/in/sunitanigam-sharma) | [GitHub](https://github.com/suneetasharma) | sunitanigam@yahoo.com

**SUMMARY**  
Cybersecurity QA Engineer & Blue Team Practitioner with 3+ years of experience validating secure infrastructure, performing threat analysis, and building security test automation. Proficient in monitoring IAM, firewall rules, encryption, and cloud hardening against NIST/CIS standards.

Adept at integrating SAST/DAST scans into CI/CD, validating APIs, and simulating threat scenarios using MITRE ATT&CK. Recently completed a 30-day SOC Challenge, applying hands-on blue team skills across threat detection, malware analysis, and EDR tools (Splunk, Suricata, Wazuh).

**TECHNICAL SKILLS**

* **Security Monitoring & EDR:** Wazuh, Suricata, CrowdStrike (conceptual), Firewall Analysis, SIEM (Splunk, QRadar), EDR alert triage
* **Threat Detection & IR:** Sysmon, Log analysis (Linux/Windows), MITRE ATT&CK, Cyber Kill Chain, IOC extraction
* **Secure SDLC & QA:** SAST, DAST, SCA, OWASP Top 10, API Abuse Testing, Cucumber, Selenium, Postman
* **CI/CD & Automation:** Git, GitHub, Jenkins, Python, Bash, Cypress, Playwright, Serenity BDD
* **Network & Protocols:** Wireshark, Nmap, DHCP, LDAP, SMTP, HTTP, SSL/TLS
* **Cloud & Compliance:** AWS, OS/Cloud Hardening (CIS/NIST), Risk Management
* **Collaboration & Agile:** Jira, Confluence, Scrum ceremonies, Sprint planning, Story grooming

**PROFESSIONAL DEVELOPMENT PROJECT (FREELANCE)**  
**SOC Hands-On Challenge (2024–2025)**  
GitHub Repo: [SOC-Hands-On-Challenge](https://github.com/suneetasharma/SOC-Hands-On-Challenge)

* Completed 30 structured labs simulating real-world Blue Team scenarios: -
* Log correlation and alert triage from Windows Event Logs, Sysmon, UFW
* Network packet inspection using Wireshark, Zeek, TCP/UDP analysis
* Threat detection using Suricata IDS and Wazuh agent alerting
* Malware and phishing incident analysis with IOC extraction
* SSH brute-force attack detection and alert customization
* File Integrity Monitoring (FIM) and memory acquisition (AVML)
* Splunk dashboards for DNS, HTTP, and SSH anomaly detection
* Documented step-by-step investigations with evidence and mitigation actions

**PROFESSIONAL EXPERIENCE**

**Serenity Dojo – Remote Jun 2023 – Jun 2024**  
*Agile Automation Test Engineer*

* Developed secure test suites with Playwright and Cypress for REST API and UI regression Built BDD scripts to test business and security rule compliance via Cucumber + RestAssured
* Integrated test pipelines in GitHub CI/CD workflows with built-in security scanning
* Simulated abuse cases and tested authentication failures, injections, and insecure redirects

**Trustwave Holdings Inc. - Remote Jul 2019 – May 2023**  
*Senior Test Engineer*

* Led infrastructure and cloud security validation across CrowdStrike, Carbon Black, Cortex XDR
* Verified firewall, IAM, and encryption settings against CIS/NIST security benchmarks
* Integrated SAST/DAST tools into CI/CD pipelines for continuous security validation
* Supported SOC triage and remediation by analyzing QRadar and Cybereason alerts
* Authored secure QA workflows for SOAR playbooks and remediation validation

**M86 Security (Acquired by Trustwave) – Irvine, CA Mar 2012 – Jun 2019**  
*QA Engineer*

* Validated SOAR platform security: API abuse prevention, threat intelligence workflows
* Automated Postman-based security tests for vulnerability detection and remediation
* Ensured adherence to secure development practices for microservice-based platforms

**Marshal8e6 – Orange, CA** Dec 2007 – Feb 2012  
*QA Engineer*

* Conducted QA for enterprise filtering products, endpoint policy enforcement
* Automated test scripts to detect weak configurations and bypasses
* Partnered with SOC and threat teams to validate malware detection scenarios

**EDUCATION & CERTIFICATIONS**

* Certificate in Software Quality Assurance – Portnov Computer School, CA
* MS Botany & BS Education – Rani Durgavati University, India
* Certified ScrumMaster (CSM), PMI-ACP, SAFe Agilist
* CompTIA Security+ (in progress – target Oct 2025)
* Splunk Fundamentals 1 (in progress)

**SECURITY RESEARCH & INTERESTS**

* Completed bootcamps: Threat Intelligence, Malware Analysis, Blue Team Labs
* Hands-on with Wazuh, Splunk, AVML, CyberChef, OSSIM
* Interests: Threat Hunting, Memory Forensics, Security QA Automation

**Portfolio:** [suneetasharma.github.io](https://suneetasharma.github.io)  
**GitHub:** [github.com/suneetasharma](https://github.com/suneetasharma)  
**LinkedIn:** [linkedin.com/in/sunitanigam-sharma](https://linkedin.com/in/sunitanigam-sharma)