Sunita Sharma
Cypress, CA | (714) 616-8520
sunitanigam@yahoo.com | LinkedIn | GitHub Portfolio

Cybersecurity Analyst | SOAR Tester | Blue Team Practitioner

Dedicated Cybersecurity QA Analyst with 15+ years of professional experience in secure software validation, threat detection, and alert triage. Specializing in SIEM/EDR monitoring, security automation, and Blue Team support through rigorous QA practices. Hands-on experience in threat detection lab simulations, real-time log monitoring, and SOAR platform testing. Certified Scrum Master with a proven track record in Agile teams.

Core Competencies

- **Security Monitoring & Detection**: SIEM (Wazuh, Splunk, QRadar), EDR (CrowdStrike, Suricata), MITRE ATT&CK, Security Alerts Triage
- **SOAR Testing**: Workflow testing, Playbook validation, API/EDR integration verification
- **Log & Threat Analysis**: Windows/Linux logs, Sysmon, Wireshark, Suricata, Zeek, IOC extraction
- **QA & Automation**: Selenium, Cypress, Postman, Cucumber, TestNG, Python (alert parsing), Git, Jenkins
- **API & Security Validation**: Input validation, abuse case design, REST/SOAP testing
- **Cloud & Infrastructure**: AWS (basic), OS/Cloud Hardening (CIS/NIST), Docker, Consul, Kibana
- **Collaboration & Agile**: JIRA, Confluence, Story Grooming, Sprint Planning, Scrum (CSM/SAFe)

Professional Experience

Trustwave Holdings Inc – Remote *Jul 2019 – May 2023*

Senior QA Engineer (Cybersecurity/EDR Focus)

- Validated SOAR playbooks and automated response integrations with EDR tools like CrowdStrike and Cortex XDR
- Designed and executed API validation frameworks for microservices in CI/CD pipelines
- Triaged SIEM alerts from QRadar and contributed to incident containment
- Developed reusable test cases for vulnerability validation and patch verification
- Led automation of negative test scenarios to simulate privilege escalation and broken authentication

- Participated in threat modeling sessions and log validation of simulated security incidents

Serenity Dojo – Remote (Contract) *Jun 2023 – Jun 2024*

Security Automation Test Engineer

- Built secure automation frameworks for API/UI testing using Playwright and Cypress
- Executed abuse case testing aligned with OWASP and SOC response workflows
- Implemented Python scripts for log parsing, alert validation, and mock threat injection
- Collaborated with IR teams to test detection coverage and alert logic

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

QA Engineer

- Performed validation of secure web filtering and endpoint access policies
- Automated API test scripts and backend validations for network security platforms
- Partnered with QA and SOC teams to test malware detection logic in threat intelligence workflows

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

QA Engineer

- Delivered end-to-end testing for secure network appliances and policy enforcement tools
- Conducted cross-platform regression, exploratory, and UAT testing for critical releases

---

Featured Project

30-Day SOC Analyst Challenge

Hands-on Security Lab Series (2025)
GitHub: SOC-Hands-On-Challenge

- Completed 30 Blue Team labs simulating real-world SOC scenarios
- Performed live detection of brute force, malware, phishing, and C2 traffic
- Used Splunk, Wazuh, and Suricata to triage alerts and validate detection rules
- Documented every lab with detailed SOPs, screenshots, indicators, and response strategies

---

Education & Certifications

M.S. (Botany), Rani Durgavati Vishwavidyalaya, India
Certificate in Software Quality Assurance, Portnov Computer School, CA

- Certified ScrumMaster (CSM), Scrum Alliance (Valid through Nov 2025)
- SAFe 6 Agilist, Scaled Agile Inc (Valid through May 2025)
- Python for Cybersecurity, Udemy (Completed Feb 2025)
- *In Progress*: CompTIA Security+ (Expected Aug 2025)

Volunteering & Leadership *Feb 2024 – Present*

CrowdDoing – Remote (Volunteer Scrum Master)

- Mentored QA volunteers in secure defect triage, detection mapping, and agile QA planning
- Integrated security-focused use case reviews and incident validation workflows into sprints

---

✅ *Resume tailored for Security Analyst, SOAR Validation, or Security QA positions*

References and sample security projects available upon request.