HARSHIV PATEL

CYBERSECURITY ENGINEER & IT ADMINISTRATOR

+1 (862) 846-1916 | North Bergen, NJ | patelharshiv575@gmail.com | LinkedIn | GitHub | Portfolio

SUMMARY

Cybersecurity Engineer with 8+ years of experience in **cybersecurity risk assessments, SOAR (Security Orchestration, Automation, and Response) customization, and secure software development**. Proficient in **Palo Alto XSOAR, Splunk,** and **Python-based security automation**. Strong expertise in integrating SIEM tools, developing **RESTful APIs,** and **automating SOC processes**. Hands-on experience with DevSecOps, threat modeling, and incident response. Adept at enhancing security postures, reducing response times, and ensuring compliance with **industry standards (IEC 62443, OWASP, PCI DSS, HIPAA, GDPR).**

WORK EXPERIENCE

Cybersecurity Engineer & IT Administrator – AV Hospitality LLC, NJ, USA **August 2022 - Present**

- Administered IT infrastructure, managing 5+ servers and networks with 99.9% uptime.
- **Conducted cybersecurity risk assessments** for IT infrastructure, identifying and mitigating potential vulnerabilities.
- Ensured **compliance with IEC 62443** for securing industrial control systems (ICS) and connected electromechanical devices.
- Developed and implemented **cybersecurity policies**, reducing security incidents by **20%** through **firewall configuration, IAM policies, and security monitoring**.
- Designed and deployed automated security solutions using **PowerShell and Python**, increasing efficiency.
- Developed **secure RESTful APIs** and **implemented encryption mechanisms** to protect sensitive data.
- **Conducted penetration testing** and vulnerability assessments on company infrastructure to identify security weaknesses.
- Optimized **SIEM and threat detection** using Splunk, Wireshark, and other forensic tools to enhance **incident response**.
- Led **Splunk SIEM** deployment and onboarding of new data sources, improving threat detection efficiency.
- Provided technical support and security configurations, resolving 95% of IT issues within 24 hours.

Secure Full Stack Developer – Developer Squad (developersquad.in), India (Remote) **January 2017 – August 2022**

- Led the **development of secure applications** by integrating security best practices into the **SDLC**.
- Integrated **SOAR and SIEM** solutions to enhance real-time threat monitoring and response.
- Developed **custom XSOAR playbooks** for automated threat response and incident handling.
- Spearheaded **DevSecOps initiatives**, integrating **SAST/DAST scanners**, and secure coding best practices.
- Implemented secure coding practices using **Python, Django, and Flask** to develop security tools.
- Conducted **threat modeling** and **penetration testing** to enhance application security.
- Created **RESTful APIs** for security automation, ensuring seamless data exchange across SOC tools.
- Developed **IAM policies and role-based access control (RBAC)** to protect sensitive data.
- Enhanced system security using **SIEM tools (Splunk, Azure Sentinel)** for log analysis and anomaly detection.
- Conducted secure code reviews, penetration testing, and vulnerability assessments.
- Conducted **secure code reviews** for **web and mobile applications**, ensuring compliance with **OWASP Top 10**.
- Enhanced resource utilization by 20% through the implementation of robust database architectures and improved system performance by resolving critical code errors and optimizing storage solutions.

CORE COMPETENCIES

Cybersecurity Risk Assessments | Industrial Cybersecurity (IEC 62443, NIST, ISO 27001) | Secure Software Engineering | Threat Modeling & Security Architecture | Penetration Testing & Vulnerability Assessment | Secure SDLC | RESTful APIs & Microservices | DevSecOps & CI/CD Security | Cloud Security (AWS, Azure) | Agile Development (Scrum, Kanban) |SQL & NoSQL Databases |Unix Shell Scripting | Power Shell Scripting | IAM & Role-Based Access Control (RBAC) | SIEM & Security Monitoring (Splunk, Wireshark) | Application Vulnerability Assessment | Secure Code Reviews for Web and Mobile Applications | Application Security (SAST, DAST, OWASP, Secure Code Reviews) | Network Security (Firewalls, TCP/IP, OSI Model, Intrusion Detection Systems) | **SOAR Customization** (Palo Alto XSOAR, Python-based Automation)

TECHNICAL SKILLS

Programming & Automation: .NET, React.js, JavaScript, Node.js, TypeScript, C, C++, Java, Python
Cloud & DevOps: Azure Functions, Azure Queues, AWS, Firebase
API & Integration: REST APIs, GraphQL, OAuth, Azure Graph API, Snyk
Databases: MongoDB, MySQL, PostgreSQL, NoSQL
Security & Compliance: OWASP, SAST, DAST, Secure SDLC, IAM, Wireshark, Splunk, HIPAA, GDPR, PCI DSS
CI/CD & Workflow Automation: Azure DevOps, GitHub Actions, Jenkins, Docker, Kubernetes
Dashboards & Reporting: Power BI, Grafana, React.js, Vue.js, UML Diagram, System Modeling

EDUCATION

Pace University, Seidenberg School of Computer Science and Information Systems **New York, United States**
Master in Cybersecurity August 2022 – May 2024

Gujarat Technological University **Gujarat, India**
Bachelor of Computer Engineering June 2016 – August 2020

KEY CYBERSECURITY PROJECTS

SOAR Customization & Automation – AV Hospitality LLC, NJ, USA (2024)

- Developed custom XSOAR playbooks to automate security event triage and response.
- Integrated SOAR with Splunk SIEM to automate log correlation and threat hunting.
- Created RESTful APIs for secure integration between SOC tools, reducing response time by 50%.

Threat Detection & SIEM Implementation, AV Hospitality LLC, NJ, USA

- Deployed Splunk and Azure Sentinel for real-time log analysis and anomaly detection.
- Created custom security alerts to identify potential cyber threats and unauthorized access attempts.

Secure API Gateway Development, Developer Squad, India

- Designed and implemented a secure API gateway for a financial services client, ensuring end-to-end encryption and authentication (OAuth, JWT).
- Integrated SAST/DAST security scans to detect and mitigate vulnerabilities in APIs.

ADDITIONAL TRAINING & CERTIFICATIONS

GOOGLE CYBERSECURITY PROFESSIONAL CERTIFICATE

Application Security: OWASP, SAST/DAST Tools, Penetration Testing, SIEM & SOAR Tools, SAST and SAC tools
Programming Languages: .NET, JavaScript, Java, ReactJS, AngularJS, VueJS, Python, PHP