HARSHA CHANDRASEKARAN

Cybersecurity Professional | Vulnerability Management | SOC | Application Security | Security Automation

harshachandru1996@gmail.com

https://www.linkedin.com/in/harsha-cs-128507109/

+91 8680838518

Profile Summary:

Cybersecurity Professional with 8 years of experience in Vulnerability Management, Application Security (DevSecOps), SOC Operations, SIEM Monitoring, and GRC Compliance across Banking, Telecom, Healthcare, and Enterprise environments. Strong expertise in enterprise vulnerability assessments using Tenable Nessus, Qualys, CheckMarx SAST/SCA, OWASP Dependency Check, and driving remediation aligned with CVE, CVSS, CIS Benchmarks, PCI DSS, and ISO 27001 standards.
Hands-on experience with Microsoft Defender, Azure Sentinel, Proofpoint, CrowdStrike, Arbor DDoS, and threat hunting with KQL queries. Proven ability in risk register management, GRC policy exception handling, audit evidence preparation, PCI DSS QSA coordination, and ISO 27001 ISMS support. Recognized for developing scan templates, onboarding assets from CMDB, reducing MTTR for critical vulnerabilities, and ensuring audit readiness through structured security processes.

CORE COMPETENCIES:

Vulnerability Management • CIS Benchmark • Tenable Nessus • Checkmarx SAST/SCA • CVE/CVSS • PCI DSS • ISO 27001 • Risk Register • MITRE ATT&CK Framework• SIEM Monitoring • Azure Sentinel •Secure SDLC • Microsoft Defender • Vulnerability Remediation Lifecycle •CrowdStrike • Proofpoint • Arbor DDoS • Incident Response • Threat Hunting • DevSecOps • Security Audits • Compliance Reporting • OWASP Dependency Check • Security Automation • KQL Queries • NIST Cybersecurity Framework (CSF) • UAE Information Assurance (IA) • Patch Management • CMDB Reconciliation

TOOLS & TECHNOLOGIES

Vulnerability & AppSec: Tenable Nessus, Checkmarx SAST, Checkmarx SCA, OWASP Dependency Check, Rapid 7
SIEM & SOC: MS Azure Sentinel, Microsoft Defender 365, CrowdStrike, Proofpoint
DDoS & Network Security: Arbor AED
Compliance: PCI DSS, ISO 27001, CIS Benchmark, Risk Register, Exception Register, GDPR, DSAR,DPIA,GRC.
Cloud & Platforms: Azure, O365 Security, Jira, Servicenow.

PROFESSIONAL EXPERIENCE

Ingram Micro Pvt. Ltd

Jan 2021 – Present

- Conduct enterprise-wide vulnerability assessments using Tenable Nessus and Checkmarx, aligned to CIS Benchmarks, PCI DSS, and ISO 27001.
- Drive complete vulnerability remediation lifecycle based on CVE, CVSS scoring, and business impact.
- Design and maintain scan templates, onboard assets from CMDB, and ensure scan coverage for in-scope systems.
- Evaluate policy exception requests, maintain exception register, and recommend compensating controls.
- Supported IT compliance programs aligned with ISO 27001, PCI DSS, NIST CSF and CIS Benchmarks.
- Perform **SAST/SCA analysis** to support secure **SDLC practices in DevSecOps** while leading cybersecurity project coordination, stakeholder communication, and compliance reporting.
- Analyze threats using Microsoft Defender, Azure Sentinel, ArcSight, and support incident response.

- Respond alerts related to DDoS, SQL Injection, XSS, Malware (QBot) and assist in containment and Supported policy exception handling and compensating control evaluation.

Tata Communications Pvt. Ltd

Jun 2018 – Jan 2021

- Provided 24/7 SOC monitoring using **SIEM tools (Microsoft Azure Sentinel, Rapid 7)**.
- Assisted in policy review and compliance documentation for information security standards.
- Monitored email and endpoint threats using **Proofpoint, Microsoft Defender, CrowdStrike**.
- Developed and tuned correlation rules and active lists to reduce false positives and enhance threat detection.
- Worked on **Arbor AED** for DDoS monitoring and protection group automation for banking clients, Configured and managed SmartConnectors for log collection and normalization.
- Supported SOC team with incident investigation using ArcSight dashboards and event analysis, Maintained risk register, exception register and remediation tracking for security findings.
- Assisted clients in recovering from security incidents and maintaining SLA compliance. Performed control validation for access management, vulnerability management, and log monitoring.
- Led the end-to-end implementation and deployment of **Microsoft Sentinel** for a banking client within the Azure environment, integrating multiple log sources to establish centralized security monitoring, advanced threat detection, and regulatory compliance visibility.

KEY PROJECTS

Vulnerability Management & Compliance Program:

- Implemented vulnerability management program aligned with **PCI DSS, CIS Benchmark, ISO 27001**, **Patching**.
- Reduced critical vulnerability backlog through structured remediation tracking and stakeholder engagement.
- Worked on PCI DSS to initiate scans for the Payment and credit card assets and supported for QSA audit processes.
    - **Application Security Testing & DevSecOps:**
- Conducted **SAST/SCA** scans using Checkmarx and OWASP tools.
- Prioritized vulnerabilities using CVSS and business impact.
- Enabled secure SDLC practices with DevOps and application teams.

CERTIFICATIONS

- CEH – Certified Ethical Hacker (EC Council) • CCNA – Cisco Certified Network Associate • CompTIA CySA+ – Cybersecurity Analyst • Microsoft SC-200 – Security Operations Analyst • Arbor Certified Specialist – DDoS Protection • EC-Council Certified Application Security (DevSecOps)

• *SUCCESS STORIES IN CYBERSECURITY OPERATIONS:*

- Reduced MTTR for Application Security Vulnerabilities in DevSecOps and Automated Arbor AED protection groups for banking clients to mitigate DDoS risks.
- Spotlight Award – Ingram Micro for handling the incidents in SOC
- Recognized for SLA excellence in SOC.
- Enabled Audit Readiness for PCI DSS and ISO 27001 Assessments

EDUCATION

Bachelor of Engineering in Electronics and Communication Engineering (ECE), Sri Krishna College of Technology, Coimbatore (2014–2018) — CGPA: 7.8/10