Bala Donthamsetti

Senior Cyber Security Engineer | Application Security | Vulnerability Management | Incident Response
London, United Kingdom | +44 7442583226 | bala.cyber5598@outlook.com | LinkedIn: linkedin.com/in/dbalamurali

Professional Summary

• Cyber security professional with 5+ years of experience across SOC operations, incident response, vulnerability management and application security. OSCP-certified and hands-on in driving remediation with engineering and infrastructure teams, improving scan coverage and meeting SLAs (Cyber Essentials 14-day, PCI ASV). Experienced with Microsoft Sentinel/Defender, Splunk, Tenable.io, Burp Suite and Checkmarx, with strong network security fundamentals (firewalls, router ACLs, packet analysis) and governance exposure (ISO 27001, PCI DSS).

Core Skills

• Application Security: OWASP Top 10, web/API testing, authn/authz & access control, session management, remediation guidance and fix validation
• Vulnerability Management: Tenable.io/Nessus operations, asset tagging & coverage, scan scheduling, SLA reporting, exception handling (recast/accepted), Cyber Essentials / CE+ and PCI ASV
• Incident Response & SOC: alert triage, investigation, containment and reporting; evidence collection and stakeholder communication
• Security Tooling: Burp Suite, Checkmarx, Metasploit, Nmap, Wireshark, OpenVAS; Microsoft Defender and Sentinel; Splunk and Grafana
• Network Security: firewall rule management (Palo Alto/FortiGate/Checkpoint), router ACL implementation, TCP/IP fundamentals and packet analysis
• Automation: PowerShell (compliance evidence/account validation), Python (basic automation and scripting)

Professional Experience

• Senior Information Security Engineer | Markerstudy Group
• United Kingdom | Oct 2023 - Present
• Lead web application security testing across internal and external applications using Burp Suite; provide clear reproduction steps, business impact and remediation guidance.
• Partner with developers to remediate findings and validate fixes through re-testing; maintain a strong security posture with no outstanding Critical/High/Medium web application vulnerabilities after remediation cycles.
• Conduct source code review using Checkmarx; triage false positives and prioritise findings based on exploitability and business impact.
• Own the vulnerability lifecycle in Tenable.io: asset tagging, scan coverage checks, scan scheduling/operations, remediation tracking and SLA reporting (including Cyber Essentials 14-day requirements).
• Act as incident responder (day-to-day): triage tickets, investigate alerts, collect evidence and coordinate containment/remediation with technology teams.
• Delivered DMARC implementation end-to-end with the cloud team to strengthen email authentication and reduce spoofing risk.
• Support security controls (Cisco Umbrella, iboss) and compliance activities including PCI account validation (PowerShell evidence) and quarterly PCI ASV scans in Tenable.
• Security Researcher | HackerOne (Bug Bounty)
• Remote | Jun 2022 - Oct 2023
• Performed independent security research across web and API targets, focusing on OWASP Top 10 categories (authentication/session, access control, injection, XSS, SSRF and misconfigurations).
• Used Burp Suite (Proxy, Repeater, Intruder) and lightweight Python/Bash scripts to validate and reproduce vulnerabilities.
• Produced high-quality reports with step-by-step reproduction, impact analysis and remediation guidance; collaborated with program teams for validation and re-testing.
• Triaged duplicates and false positives and mapped findings to OWASP/CWE to support consistent risk communication.

• Security Analyst (SOC, Vulnerability Management and Application Security) | Pi Data Centres Pvt Ltd
• India | Jun 2019 - Jan 2022
• SOC Analyst (2019-2020): monitored and triaged alerts using Splunk and Grafana; supported incident investigations, escalation and reporting.
• Supported datacentre security operations by implementing router ACLs and firewall rules; validated change outcomes and maintained configuration documentation.
• Vulnerability Management (2020-2021): ran Tenable/Nessus scans, raised vulnerabilities to infrastructure teams for patching, tracked remediation progress and maintained SLAs (including Cyber Essentials Plus).
• Performed vulnerability assessments and penetration testing for web applications and network devices using Burp Suite, Nmap and Metasploit; documented findings and confirmed remediation via re-testing.
• Supported Active Directory security testing activities (enumeration, privilege escalation and misconfiguration review) as part of internal testing.
• Contributed to ISO 27001/27002 compliance by supporting policies/standards, project risk assessments and evidence preparation for audits.

Education

• MSc Cyber Security | Swansea University

Certifications

• Offensive Security Certified Professional (OSCP)
• Certified Ethical Hacker (CEH)

Keywords

• Application Security, Vulnerability Management, Incident Response, SOC, SIEM, EDR, Microsoft Sentinel, Microsoft Defender, Splunk, Tenable.io, Nessus, Burp Suite, Checkmarx, OWASP Top 10, SAST, DAST, Threat Hunting, DMARC, PCI DSS, Cyber Essentials, ISO 27001, Firewall Rules, Router ACLs, Nmap, Wireshark, Metasploit