

Devangkumar Soni West Haven, CT +1 (203) 668 5121 devangs2611@gmail.com LinkedIn GitHub	
Summary	Cybersecurity Analyst with 3+ years of experience securing enterprise applications, cloud environments, and financial systems through Security Operations, Threat Detection, Vulnerability Management, Incident Response, DevSecOps, and Cloud Security. Hands-on expertise with Microsoft Sentinel, Splunk, Microsoft Defender XDR, DefectDojo, IAM, Azure, AWS, Python automation, and Secure SDLC. Experienced in implementing security controls aligned with NIST CSF, PCI DSS, SOC 2, and ISO 27001 while improving detection capabilities, automating security operations, and strengthening enterprise security posture. Strong collaborator with engineering, cloud, and compliance teams delivering scalable, audit-ready cybersecurity solutions.
Skills	Security Operations: Security Operations Center (SOC), Incident Response, Threat Detection, Threat Hunting, Security Monitoring, Alert Triage, Threat Intelligence, Security Investigations, Log Analysis, MITRE ATT&CK SIEM & Security Platforms: Microsoft Sentinel, Splunk Enterprise Security, Splunk, Microsoft Defender XDR, Microsoft Defender for Cloud, Microsoft Security Copilot, Kusto Query Language (KQL), SIEM Correlation Rules Application Security & DevSecOps: Secure SDLC, DevSecOps, Vulnerability Assessment & Penetration Testing (VAPT), Vulnerability Management, DefectDojo, Web Application Security, API Security Testing, SAST, DAST, Software Composition Analysis (SCA), OWASP Top 10, GitHub Advanced Security, CI/CD Security Cloud Security: Microsoft Azure Security, AWS Security, AWS Security Hub, Cloud Security Posture Management (CSPM), Secure Cloud Configuration Identity & Access Management: Identity & Access Management (IAM), Microsoft Entra ID (Azure AD), Active Directory, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Conditional Access, Privileged Access Management (PAM) Endpoint & Network Security: Endpoint Security, Microsoft Defender Antivirus, Endpoint Hardening, BitLocker, Patch Management, Windows, Linux, Firewalls, TCP/IP, DNS, VPN Security Assessment: Nessus, Qualys, Burp Suite, OWASP ZAP, Nmap, SQLMap, Metasploit Programming & Automation: Python, PowerShell, Bash Compliance & Governance: NIST Cybersecurity Framework (NIST CSF), PCI DSS, SOC 2, ISO/IEC 27001, Security Control Validation, Risk Assessment
Certifications	(ISC)² Certified in Cybersecurity (CC)
Experience	
Cybersecurity Analyst, PNC, USA	Jan 2026 – Present
- Spearheaded enterprise threat detection by engineering advanced SIEM correlation rules and analytics in Microsoft Sentinel, Splunk Enterprise Security, and Microsoft Defender XDR, to identify sophisticated banking threats across payment platforms and customer-facing applications, processing over 12,000 security events daily and reducing investigation time for more than 450 high-priority incidents annually for SOC analysts. - Orchestrated enterprise vulnerability management across cloud and on-premises environments by integrating DefectDojo, Nessus, Qualys, and automated remediation workflows into the Secure SDLC, to centralize vulnerability tracking, eliminate duplicate findings, and accelerate remediation of more than 220 critical and high-risk vulnerabilities across 150+ production applications while supporting PCI DSS, NIST CSF, and SOC 2 compliance. - Architected AI-assisted security investigation workflows using Microsoft Security Copilot, Python automation, Kusto Query Language (KQL), and threat intelligence enrichment, to automate alert correlation, contextual analysis, and incident prioritization, enabling analysts to enrich over 800 security investigations and reduce repetitive manual analysis across enterprise SOC operations. - Strengthened cloud security posture across Microsoft Azure and AWS workloads by implementing Microsoft Defender for Cloud, AWS Security Hub, Identity and Access Management (IAM), Conditional Access, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Cloud Security Posture Management (CSPM), to secure more than 300 cloud resources and 4,000 enterprise identities supporting critical financial applications. - Championed DevSecOps initiatives by integrating SAST, DAST, Software Composition Analysis (SCA), GitHub Advanced Security, Infrastructure-as-Code (IaC) security scanning, container image scanning, and DefectDojo into CI/CD pipelines, to identify security risks before production deployments and automate vulnerability tracking across 90+ repositories used by application development and DevOps teams.	
Technical Support Assistant, PixelEdge Systems, India	Jan 2023 – Jul 2024
- Resolved more than 700 Tier-1 and Tier-2 support requests involving Windows, Linux, Microsoft 365, Active Directory, VPN, endpoint devices, printers, and enterprise networking, to restore business-critical services within SLA targets while supporting over 450 end users across multiple business functions. - Administered Identity and Access Management (IAM) activities by provisioning user accounts, configuring Role-Based Access Control (RBAC), managing Microsoft Entra ID (Azure AD), performing periodic access reviews, and supporting Multi-Factor Authentication (MFA), to secure user onboarding and offboarding for more than 300 employee accounts. - Implemented endpoint security controls by deploying operating system patches, Microsoft Defender Antivirus policies, BitLocker encryption, endpoint hardening baselines, and vulnerability remediation activities, to improve endpoint compliance across approximately 550 managed Windows devices and strengthen organizational security standards. - Automated repetitive administrative and security support tasks using PowerShell, Python, and Bash scripting, to streamline user lifecycle management, system health verification, log collection, and routine operational tasks, eliminating more than 20 hours of manual effort each month for IT support engineers. - Diagnosed and resolved complex infrastructure issues involving DNS, DHCP, TCP/IP, VPN, LAN, Wi-Fi, Microsoft 365 services, and endpoint connectivity, to restore business operations with minimal downtime while coordinating escalations with infrastructure, cloud, and cybersecurity teams during critical production incidents.	
Cybersecurity Analyst, TCS, India	Sep 2021 – Dec 2022
- Executed vulnerability assessments and penetration testing across web applications, REST APIs, internal networks, and Windows/Linux environments using Burp Suite, OWASP ZAP, Nessus, Nmap, Nikto, SQLMap, and Metasploit, to identify and validate more than 150 security findings across 18 enterprise client applications, enabling development teams to prioritize remediation using CVSS risk ratings. - Performed application security validation by reproducing reported vulnerabilities, analyzing exploitability, conducting remediation verification, and eliminating false positives, to improve assessment accuracy and successfully validate remediation for over 130 resolved security findings before production releases. - Monitored security events and investigated suspicious activities using Splunk, log correlation, threat intelligence, and MITRE ATT&CK methodologies, to support SOC analysts in triaging approximately 2,500 security alerts each month involving phishing, unauthorized access, malware activity, and privilege escalation attempts. - Conducted secure application assessments by performing SAST, DAST, Software Composition Analysis (SCA), API security testing, and OWASP Top 10 validation within Secure SDLC processes, to identify software weaknesses before production deployment across multiple enterprise banking and technology projects. - Authored comprehensive vulnerability assessment reports documenting business impact, proof-of-concept evidence, CVSS scoring, remediation recommendations, compliance mapping, and executive risk summaries, delivering more than 40 technical assessment reports supporting client remediation planning and security audit readiness.	
Education	
M.S. Cybersecurity & Networks	Aug 2024 – May 2026
University of New Haven	New Haven, CT
B.Tech. Computer Science and Engineering	Jun 2019 – May 2023
Charotar University of Science and Technology	India
Projects	
SOAR-Lite for Linux — Automated Security Monitoring & Incident Response System Python, PyYAML, nftables, systemd, Linux - Engineered a Linux-based security monitoring agent achieving sub-60-second detection-to-containment for SSH brute-force attacks by ingesting auth logs, applying sliding-window correlation, generating structured incident records, and executing nftables-based blocking. - Benchmarked detection-latency versus false-positive tradeoffs across multiple policy configurations, achieving ~5–10% false-positive rate in testing; produced JSONL metrics and SHA-256 evidence bundles suitable for analyst review and incident-response documentation.	
Network Enum Tool — Network Security Assessment & CVE Correlation CLI Python, Nmap, Bash, Linux - Built a CLI network assessment tool for automated host discovery, service enumeration, SMB/NetBIOS Windows detection, and offline CVE correlation, supporting repeatable vulnerability assessment workflows. - Generated structured Markdown, JSON, and HTML reports with service-level findings, risk ratings, and audit-ready output for technical review, remediation planning, and security documentation.	