RISHIKESH REDDY PUNTIKURA

Email: Puntikurarishikeshreddy@gmail.com | Phone: +1 (737) 895-3945 | linkedin.com/in/rishikeshreddyp

Cybersecurity Analyst

PROFESSIONAL SUMMARY:

As a Cybersecurity Analyst with 4+ years of experience in SOC operations, application security, vulnerability management, and cloud security. Skilled in detecting and responding to security incidents using SIEM tools, performing phishing and malware investigations, and securing web applications and APIs following OWASP and Secure SDLC practices. Hands-on experience with AWS and Azure security, IAM monitoring, endpoint protection, and threat hunting, with a strong focus on accurate documentation, compliance support, and continuous security improvement.

TECHNICAL SKILLS:

SIEM Monitoring | Incident Response | Threat Hunting | MITRE ATT&CK | Splunk | Microsoft Sentinel | Phishing & Malware Analysis | Vulnerability Management (Nessus, Qualys) | OWASP Top 10 | SAST & DAST | AWS & Azure Security | IAM (AWS, Azure AD) | Microsoft Defender | NIST Frameworks | Python Automation

PROFESSIONAL EXPERIENCE:

Health Plan Of San Joaquin HPSJ ||Cybersecurity Analyst|| California CA **Feb 2025 – Present**

- Monitored and analyzed security events using Splunk and Microsoft Sentinel, correlating logs from endpoints, servers, firewalls, cloud workloads, and identity systems, improving real-time threat detection accuracy by 35% and reducing mean time to detect (MTTD) by 30%.
- Performed incident triage and investigations for phishing, malware infections, credential compromise, suspicious API activity, and cloud security alerts, following IR playbooks and SLA-driven escalation procedures, resulting in 40% faster incident resolution and 25% fewer repeat incidents.
- Applied MITRE ATT&CK framework and proactive threat-hunting methodologies across SIEM data, endpoint telemetry, and cloud environments, increasing detection of advanced and stealthy attack patterns by 30% and strengthening overall SOC visibility.
- Monitored AWS GuardDuty and Azure security alerts, identifying IAM misuse, anomalous access patterns, cloud misconfigurations, and risky user behavior, contributing to a 28% reduction in cloud security risks and improved cloud security posture.
- Investigated endpoint and identity-related alerts using EDR/XDR tools (Microsoft Defender and CrowdStrike concepts) along with Azure AD / Entra ID and Active Directory logs; documented incidents, RCA, and remediation actions in ServiceNow and Jira, supporting ATO, compliance, and audits while achieving 100% audit readiness aligned with NIST RMF, NIST CSF, and NIST SP 800-53.

Kroger ||Application Security Engineer || Remote **May 2024 – Feb 2025**

- Performed application security assessments using SAST, DAST, and SCA tools (Checkmarx, Fortify, Burp Suite, OWASP Dependency-Check) across web applications and APIs, identifying and mitigating vulnerabilities and reducing overall application risk exposure by 35%.
- Conducted manual and automated vulnerability testing aligned with OWASP Top 10, validating SQL Injection, XSS, CSRF, authentication/authorization flaws, and insecure configurations, resulting in a 40% decrease in high-severity vulnerabilities prior to production releases.
- Integrated application security scanning into CI/CD pipelines using GitHub, GitLab, and Jenkins, implementing Shift-Left and Secure SDLC practices that enabled 30% earlier vulnerability detection and 25% faster remediation cycles.
- Performed API security testing and threat modeling, validating OAuth2, JWT, authentication/authorization controls, input validation, and rate limiting, and conducting STRIDE-based threat modeling, reducing API-related security risks by 28%.
- Reviewed application source code (Java, Python, JavaScript) to identify insecure coding patterns, produced risk-based vulnerability reports, and collaborated with Development, QA, and DevOps teams to track remediation, improving overall application security posture by 32%.

FIS Global || Information Security Analyst || Atlanta GA **Feb 2023 – March 2024**

- Monitored and analyzed security alerts using SIEM platforms (Splunk, IBM QRadar) by correlating logs from firewalls, servers, endpoints, Active Directory, and cloud environments, improving true-positive incident detection by 35% and reducing alert noise.
- Performed incident triage and investigations for phishing attacks, malware detections, suspicious logins, and policy violations, following SOC runbooks and SLA-based escalation procedures, resulting in 40% faster incident response times.
- Applied advanced log correlation and behavioral analysis techniques to reduce false positives, increasing alert accuracy by 30% and improving SOC operational efficiency.

- Conducted vulnerability assessments using Nessus and Qualys, validated findings, eliminated false positives, and coordinated remediation and patching with infrastructure teams, reducing critical vulnerabilities by 45%.
- Investigated endpoint, email, and identity security incidents using EDR/AV tools (Microsoft Defender concepts), email header and URL analysis, and AD/cloud IAM logs; documented incidents and remediation actions in ServiceNow and Jira, achieving 100% audit readiness and supporting continuous SOC process improvement.

Mpaul Tech IT Solutions PVT. (Internship)
Programming Developer Intern || India || **Nov 2020 – Dec 2021**

- Supported development of client-facing application features by writing and modifying code under senior developer guidance, following defined requirements, timelines, and Agile development practices.
- Developed and maintained Python scripts for data processing, automation, and backend logic, helping reduce manual effort and improve operational efficiency.
- Assisted in understanding client business requirements and translating them into basic functional and technical tasks throughout the development lifecycle.
- Supported API integrations and automation workflows, improving application reliability, data handling, and overall functionality.
- Performed debugging, basic unit testing, and issue resolution to ensure application behavior aligned with client expectations and quality standards.
- Worked with databases and SQL queries for data validation and reporting, while using Git version control to collaborate with cross-functional teams and maintain documentation.

EDUCATION:

New England College Henniker, NH
Masters in Computer and Information Systems **| GPA : 3.8/4.0** May 2023

Mahatma Gandhi University (Meghalaya) India
Bachelor of Technology in Engineering | **GPA : 8.68/10** May 2021