ARIN SUKHWAL

Bengaluru, Karnataka,
+91-8114461447
mrarinsukhwal@gmail.com

EXPERIENCE

April 2024 – Present · **SECPOD TECHNOLOGIES.**

Bengaluru, India
SecOps Engineer

- Developed and automated IR alerts using REST APIs to enhance incident response efficiency.
- Deployed, configured, and monitored SOC tools including SIEM, SOAR, Network Monitoring, and EDR, ensuring optimal system security and performance.
- Identified critical vulnerabilities in production environments and products, driving timely remediation efforts.
- Conducted penetration testing for web applications, thick-client (agent-side) platforms, and network infrastructures.
- Managed monthly vulnerability assessments, including impact analysis and patching for enhanced security posture.
- Performed vendor risk assessments for secure product onboarding.
- Monitored and analyzed alerts from external and internal network activities, ensuring rapid response to threats.
- Conducted open-source application risk assessments with thorough triage and mitigation processes.
- Led the onboarding, configuration, and management of the Security Awareness Simulation Tool to enhance organizational awareness.
- Deployed and managed on-premises password management systems for secure credential storage.
- Designed and maintained APM dashboards and managed alert systems for performance monitoring.
- Developed and enforced security policies and best practices, increasing overall organizational security maturity.
- Assisted with SOC2 and GDPR controls, including their implementation and alignment with organizational policies.
- Worked on the deployment and configuration of Microsoft Intune and Conditional Access policies, ensuring secure access and device management.

Skills: Vulnerability Management · Incident Handling & Triage · Threat Detection and Alert Tuning · SOAR · SIEM · DLP · EDR · AI Security · Firewall & VPN Management · Risk Assessment.

March 2023 – April 2024 · **REAL TIME DATA SERVICES.**

Gurugram, India
IT Security Engineer

- Participating in daily SOC activities, Incident Investigation and Incident response.
- Email security with Proofpoint (Reported malicious mails,releasing quarantined mails).
- Assisted in preparing policies and procedures for organization and establishing a central change management system.
- Effectively monitored CrowdStrike EDR platform to identify and respond to potential cyber threats.
- Implemented Vulnerability Management tool Qualys for Internal servers as well as for MSSP clients.
- Responsible for VAPT/WAPT in infrastructure as well as quarterly VA of the entire Business Unit (Ace Cloud Hosting).
- Utilizing KnowBe4 for enhanced security awareness training.
- Tools used daily are CrowdStrike, Nessus, Elastic SIEM, Proofpoint, Qualys, OpenSearch.
- Part of In-House SIEM product Research and Development
- Monitored and tracked SIEM logs throughout the day to monitor traffic and potential threats on the network.
- Tested software/services for vulnerabilities to approve or reject for use within the company/clients.

- Coordinated with third-party security information and event management (SIEM) providers to maintain protection and predict threats.
- Worked with teams to develop company-wide information assurance, security standards and procedures.

Skills: Intrusion Detection Systems (IDS) · Infrastructure Security · Identity and Access Management (IAM) · Web Application Firewalls (WAF) · Log Auditing.

Jul 2022 - Oct 2022 · 3 months **VIEH-GROUP.**
Delhi, India
Cyber Intern

- Worked as an Intern in Domain of Web Application Penetration Testing.
- Group Coordinator of 11 Interns.
- Organized Webinar/Offline Seminar on Cyber-awareness.
- Team Leader for Internship Project.
- Created Project on '**Image Encryption Using AES**" With 2 Team Members.

Skills: WAPT · Burp Suite · Project Management · Team Leadership · OWASP.

May 2022 · 1-month **EKAGA-GROUP,**
Delhi, India
Network Intern

- Training was on an IPMPLS Defense Project wherein the GPON network was being configured by our team.

Skills: Network Operations · DHCP/DNS Hardening · TCP/IP · Routers · Firewall Configuration.

EDUCATION

2020-2023 **K.R. MANGALAM UNIVERSITY** Gurugram, Haryana
Bachelor of Science (Hons.) - Cybersecurity

Relevant Subjects: Cryptography · Computer Networks · Linux Environment Lab · Cyber Law · Digital Forensics · Network Security & Stenography · Python · BASH/PS Scripting ·MATLAB.

Academic Activities:

- Ali-Baba Low Code Competition (Submission Qualifies)
- "Mobilize Your Technical Ideas" Organized by CSI. (**P2P Cloud Mining**).
- Designed the Eco-Friendly Electric Car Logo for a contest.
- Member of the **Investment Club**.

PROJECTS:

Internal Threat Simulation Platform

- Led design of internal simulation platform to test detection capability IR using Atomic Red Team & APT Simulator.
- Included tests for phishing, PUP's, DNS anomalies. Integrated Defender logs with SIEM for fine tuning.

Keylogger created for activity monitoring and self-analysis

- Utilize the Cryptography library to encrypt files.
- Maintains a log of forbidden words and keystrokes.
- Capitalize on what the management is doing.
- Serves as a method of parental control.

QR Sticker Based Service to Report Facility issue On the Campus.

- Maintain the campus budget while keeping track of the restoration process.
- Internal and external technicians are filtered for repairs.
- Location of the problematic equipment.

CERTIFICATION:

SAP Cybersecurity Engineering (The Forage) – Certification Number: N/A
Introduction to Cyber Security (FutureSkills Prime) - Certification Number: N/A

OTHER:

- Languages: English (fluent), Hindi (fluent), Marwari (Native).
- Volunteering 10 hours/month at Black Girls Hack. (2022-Present).