

MANIPRAMODH M

Cyber Security Analyst

CONTACT

Phone:

+91 9740417903

Email:

Pramodh122000@gmail.com

LinkedIn:

<https://www.linkedin.com/in/mani-pramodh-097b4020b>

EDUCATION

Bachelor of Technology (ECE),

Reva University, Bangalore

TOOLS AND TECHNOLOGIES

- IBM- Q-Radar
- Azure Sentinel
- CrowdStrike
- Proofpoint
- Darktrace
- Taegis XDR
- ServiceNow, Jira
- Confluence
- SOC Radar
- Imperva
- Sky High, Defender

SKILLS

- Incident Response and Management
- Threat Hunting and Analysis
- SIEM and Security Tools Proficiency
- Malware and Log Analysis
- Documentation and Reporting
- OWASP top 10

LANGUAGES

ENGLISH
KANNADA
TELUGU
HINDI

ACHIEVEMENTS

Team Excellence Award, 2023

OBJECTIVE

Dedicated SOC Engineer with 2+ years of hands-on experience in threat detection, incident response, and SIEM management. Seeking to leverage my expertise in cybersecurity tools and proactive threat mitigation to enhance security operations and safeguard critical assets in a dynamic environment.

EXPERIENCE

Happiest Minds Technology, Bangalore

SOC ANALYST | AUG 2022 – Present

- Monitored and analyzed security events using IBM Qradar and Microsoft Sentinel SIEM, escalating incidents and responding to potential threats.
- Investigated logs and events from proxy, firewall, EDR, O365, and Windows platforms within the SIEM and XDR environment.
- Utilized Falcon CrowdStrike EDR and Bitdefender GravityZone for real-time malware analysis, threat mitigation, root cause analysis, and comprehensive endpoint protection.
- Conducted in-depth traffic analysis with Darktrace NDR, monitoring AI-based cyber threats and Antigena model breaches via the Darktrace dashboard.
- Managed email security with Proofpoint, analyzing phishing and spam threats, and leveraging open-source intelligence for threat assessment.
- Performed daily health checks and troubleshooting for event collectors and non-reporting devices, ensuring system integrity.
- Created SOPs, summary reports, and documentation for Security Operations Center (SOC) activities, along with weekly and monthly security reports.
- Updating List including those for latest threat IOCs for early and fast detection with IOC sweeping in the environment.
- Led incident triage calls, resolving pending incidents and ensuring adherence to resolution timelines.
- Monitored and analyzed alert traffic for AWS, Azure, and GitHub to improve security and ensure compliance
- Stayed current with the latest security threats, vulnerabilities, and best practices, applying knowledge of the Cyber Kill Chain, MITRE ATT&CK, and NIST frameworks to enhance incident response.
- Good Knowledge of OSI reference Models, TCP/IP, NAT, PAT, DHCP, DNS, and Networking Devices.
- Proficient in utilizing tools such as Wireshark, VirusTotal.com, IPvoid.com, Any. Run, MXToolbox.com, Nessus, and Nmap to analyze and mitigate security threats.

CERTIFICATIONS

XDR Certified Analyst Exam – 2022 [from SecureWorks](#)

SOC Excellence Program [from Ant Walk](#)

SC-200: Microsoft Security Operations Analyst, [Udemy](#)

Learn Python & Ethical Hacking from Scratch, [Udemy](#)

The CrowdStrike Certified Falcon Responder ([CCFR](#))