Divya A

Email: meenu.adb@gmail.com | **Phone:** +1(903) 933-9309 | **LinkedIn Profile:** www.linkedin.com/in/divya-reddy-meenu

Desirous of working in an organization which provides adequate opportunity for career development and to learn to utilize my knowledge and contribute to the success of organization by my sincere efforts

Technical Highlights

- SIEM (Security Information and Event Management): Experienced in monitoring security events and incidents in real-time using Wazuh (Open source), AlienVault & Splunk. Vulnerability Management: Experienced in planning and conducting end to end vulnerability scans and assessments using Rapid7 and Tenable Nessus, Web App scanners - OWASP ZAP, and Burp Suite.
- Skilled in investigating end to end forensic analysis to gather evidence and applied the MITRE attack framework to understand the tactics, techniques, and procedures (TTPs) used in the attack. Endpoint Detection and Response (EDR/XDR): Experience in monitoring, investigating and analyzing security alerts generated by Sophos, SentinelOne and CoSoSys Endpoint Protector.
- Data loss prevention: Implement data loss prevention strategies using CoSoSys Endpoint. Protector tools to safeguard sensitive data across endpoints and cloud environments, ensure compliance with industry regulations and minimize data breach risks.
- Information Security Standards: Trained in information security frameworks like NIST Cybersecurity Framework, PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act) and GDPR.
- Cloud Technologies: Experienced in Amazon Web Service - Audited access token misuse, EC2 security groups, network ACLs, database configurations and addressed security concerns on AWS accounts using the Scout Suite cloud security auditing tool
- Phishing Campaign Oversight: Monitor alerts related to internal phishing campaigns, ensure that activities were intentional and assessing impact on the organization security posture. Legitimate Email Verification: Analyse, monitor and confirm authenticity of emails from internal departments, such as those from HR team, to prevent false positives in email filtering systems.
- Spam and Phishing Mitigation: Addressed instances where spam emails were not intercepted despite existing blocklist configurations. Coordinated with Darktrace support to enhance filtering rules and improve detection rates. Microsoft Defender Office 365: Analyzed security alerts related to risky users, sign-ins and detections, ensure that no significant threats were present.
- Investigated suspicious URL accesses detected by AlienVault OTX pulses, to identify potential threats and initiate appropriate responses. Raised and managed support tickets with security vendors, including Darktrace, to address issues like spam emails bypassing blocklists. Provided detailed information and collaborated with support teams to implement effective solutions.
- Ensured seamless transition between shifts by documenting ongoing investigations and tasks, such as assigning next shift. Regularly monitored cloud security alerts, confirm the absence of threats and maintaining the integrity of cloud resources. Collaborated with cross-functional teams to review and refine security policies, enhance the organization's security posture.
- Participated in ongoing training to stay updated on the latest cybersecurity threats and mitigation strategies, applying this knowledge to protect the organization effectively. KnowBe4 Phishing Simulations: Executed phishing simulation campaigns to assess organizational awareness. Provide post-campaign reports and recommended security awareness training improvements.
- Educated employees on best security practices, identifying social engineering tactics, and reinforcing compliance with security policies. Completed learning in Office 365 Security and CISM, reinforcing in enterprise security management and governance.

Certification: CEH v12 - Certified 2023 - ECC1236890745 | CompTIA Security+ SY0-601 - Certified 2021 | ISO 27001:2013 ISMS - Certified 2022 - IN/17615/192225 | AWS Certified Solutions Architect - Associate Certified 2024 | Azure AZ-900 - Certified-2025

Experience

Cyber Security Analyst | Since Jul 2024 | Client: Reiter Affiliated Companies, Oxnard, CA | Environments: EDR/XDR, Network ACLs, IDS/IPS, AlienVault, IOCs, TTPs, Windows, Linux, OSX, SentinalOne, Phishing emails darktrace, Threat hunting, AD and Cisco umbrella

- Leveraged AlienVault USM to centralize security event monitoring, correlating events from multiple sources for comprehensive threat visibility. Implemented security policies in Cisco Umbrella to enhance DNS-layer protection, restrict access to malicious domains, and enforce web filtering controls. Optimized security settings to prevent malware, phishing, and unauthorized access.
- Entra ID Conditional Access Management: Configured Conditional Access policies in Microsoft Entra ID (formerly Azure AD) to enforce adaptive authentication, limit access based on device compliance and risk level, and enhance identity security posture. Applied Zero Trust principles to strengthen user access controls. Report on cybersecurity risks, controls, and compliance metrics.

- Develop, implement, and maintain cybersecurity policies, standards, and procedures in alignment with industry frameworks and regulatory requirements. Conduct risk assessments, security control evaluations, and gap analyses to identify and mitigate risks. Work with key cross-functional teams to ensure security controls are embedded in business processes and IT operations.
- SentinelOne Administration: Managed SentinelOne EDR solutions, including responding to alerts. Collaborated with the IT team to verify applications and adjust security policies accordingly. Darktrace Email Protection: Utilized Darktrace's AI-driven email security solutions to detect and block sophisticated email threats, including spam and phishing attempts targeting users

Sr Cybersecurity Analyst | Nov 2018 - July 2024 | Employer : PurpleTalk |Client: XcubeLABS, McKinney, TX (Offshore - Hyderabad) | Project clients: UHG, DreamWorks Animation, General Electronics (GE), Hasbro, Fanatics, CBS, Mann Hummel, Atari | Environments: Vulnerability Management, AWS, EDR/XDR, XQL Queries, AWS EC2, Network ACLs, IDS/IPS, Sophos Firewall, IOCs, TTPs, Windows, Linux, OSX, SIEM, Jira, ISMS, Phishing, SSDLC, DLP, Threat hunting.

- Led the configuration and optimization of various firewall solutions Sophos and Intrusion Detection/Prevention Systems (IDS/IPS) to safeguard the organization's network infrastructure. Deployed advanced security rulesets and actively monitored alerts, reducing network intrusions by 40%. Follow documented incident response procedures to resolve key threats efficiently.
- Collaborated closely with clients like UHG, DreamWorks Animation, GE, Hasbro and Atari to design and deploy advanced threat detection and response strategies, resulting in a 50% reduction in security incidents. Demonstrate foresight in recognizing potential or existing security issues, vulnerabilities, and threats and work with cross-functional teams to implement remediation
- Led vulnerability assessment and remediation efforts for critical infrastructure at clients like Panini/fanatics, CBS, GE, and Mann Hummel, utilizing tools like Rapid7 and Tenable Nessus to identify and mitigate high-risk vulnerabilities, safeguarding sensitive data and maintaining operational integrity. Plan, analyze and confirm the severity of security incidents based on available data.
- Collaborate with technical experts to develop and implement remediation plans. Track and monitor corrective actions, ensuring stakeholders are informed and engaged. Participate in crisis management, including artifact collection, risk analysis, and first-level threat assessments. Provide technical expertise for projects, tool evaluations, risk analysis assistance, and technical audits.
- Propose and develop new detection scenarios, automation tools, or enhancements to improve productivity. Conduct team knowledge-sharing sessions by presenting in-depth technical topics. Planning and design of corporate security architecture. Recommend additional security solutions or enhancements to current security solutions to improve overall enterprise security
- Perform the deployment, integration, and initial configuration of all new security solutions and any enhancements to existing security solutions following standard best operating procedures generically and the enterprise's security documents specifically. Regularly participate in the creation of corporate security documents (policies, standards, baselines, guidelines, and procedures)
- Implemented Antivirus, Endpoint Security, and XDR solutions for comprehensive threat detection and response capabilities. Actively monitored cyber threat landscapes and gathered intelligence to anticipate and mitigate emerging threats. Utilized threat intelligence feeds and SIEM platforms (Splunk, Wazuh) to analyze network traffic and proactively detect potential risks.
- Conduct audits on access token misuse, EC2 security groups, database configurations on AWS accounts using Scout Suite cloud security auditing tool, recommend strategic upgrades and configuration changes to mitigate vulnerabilities. Enhance security monitoring through real-time data activity monitoring using Wazuh tools, identify unusual activities around sensitive data.
- Analyse, monitor and reduced cyber-attack incidents by 65% by identifying potential threats through detailed analysis and correlation of events across IDS/IPS and Sophos Firewall platforms. Utilized investigative tools, techniques, and procedures with an in-depth understanding of security threats, applying defined runbooks to take decisive actions on incoming signals.

Cybersecurity analyst-Gmail | May 2017 - Aug 2018 |Employer: Wipro | Client: Google , Hyderabad

- Led proactive monitoring and rapid response to incoming security alerts, ensuring prompt resolution and effective mitigation of potential threats. Investigated and neutralized Gmail-Inbound threats, including phishing and spam emails targeting Google, successfully blocking 95% of malicious attempts using the Phish Rails tool, significantly enhancing organizational security.
- Plan and design of the corporate Business Continuity Plan and Disaster Recovery Plan. Maintain up-to-date baselines for the secure configuration and operations of all in-place devices, whether they are under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.). Tune security events and correlation from applicable security products and sources
- Perform network traffic analysis, host behavior analysis, kill chain, windows event analysis, etc. to protect company assets. Produce a monthly security operations dashboard with KPI's (incidents, metrics, security threats, intelligence, etc.).

Documented findings and response actions meticulously in ticketing system (Internal Nuff tool), improve incident response efficiency by 30%.

- Collaborated closely with the anti-phishing operations team in California, ensuring seamless operations in Hyderabad and maintaining high-quality review standards, resulting in a 60% improvement in operational efficiency. Compiled Monthly Business Review Reports, leading to a improvement loop and a 15% increase in operational effectiveness for upcoming periods.

Anti-Phishing Ops -Cybersecurity analyst | Aug 2014 -April 2017 | Employer: GlobalLogic Pvt LTD | Client: Google, Hyderabad

- Conduct daily system log monitoring with efficiency, leading to a 20% increase in threat detection accuracy. Neutralize phishing email threats to fortify security measures, resulting in a 30% reduction in successful phishing attempts. Swiftly respond to security incidents in accordance with detailed alert response protocol, achieving a 40% decrease in incident response time.
- Analyse, monitor and maintain vigilant monitoring for indications of attacks, intrusions or unauthorized activities, safeguarding the integrity of our network with a 95% success rate in threat identification. Successfully eradicated numerous phishing domains targeting reputable organizations, enhancing their digital security posture and reduce potential breaches by 50%.
- Implemented blacklisting measures for 1000 phishing domains, reducing risk of potential security breaches by 70%. Resolved escalated issues from global Google offices and efficient resolutions with a 90% satisfaction rate. Transitioned to a specialized role in Gmail-Inbound Ops, dedicate 100% effort to combating phishing threats and achieving a 100% focus on threat mitigation.

Education: Bachelor of technology in Computer science | RRS College of engineering | Hyderabad | 2014

Divya A