Sathishkumar Anamalamudi

CT, United States,06605.
475-655-6223 Anamalamudi.sathishkumar@gmail.com www.linkedin.com/in/sathishkumaraamalamudi-cybersecurity

SUMMARY

Cyber Security Engineer with extensive experience in AI-driven security solutions and advanced threat intelligence. Proven track record in engineering self-healing cybersecurity infrastructures using SOAR, XDR, and AI-powered SIEM solutions. Successfully led high-profile incident response operations and developed AI-enhanced intrusion detection systems. Aims to leverage expertise in AI and cybersecurity to enhance proactive threat mitigation and security resilience.

Technical Skills

- **Cybersecurity & Threat Intelligence**: SIEM, SOAR, IDS/IPS, Frameworks, Threat Intelligence
- **AI & Security Automation**: Al-driven Security, Tools
- **Cloud & Zero Trust**: Multi-Cloud Security, Zero Trust Architecture (ZTA), CSPM, Kubernetes Security, Cloud Workload Protection
- **Offensive & Defensive Security**: Penetration Testing & Red Teaming, Malware Analysis, Secure Coding
- **DevSecOps & Infrastructure Security**: Infrastructure as Code, CI/CD & Security-as-Code, Soft Skills

EXPERIENCE

Shelton Dental Group **Jan 2024 - Present**

Cyber Security Engineer

- Designed and implemented AI-driven threat detection and response systems, leveraging deep learning for advanced anomaly detection
- Engineered self-healing cybersecurity infrastructures using SOAR, XDR, and AI-powered SIEM (Splunk, ArcSight, Cortex XDR) to automate threat mitigation
- Developed autonomous AI-powered security automation using Python, integrating with next-gen security orchestration platforms to enhance threat response efficiency
- Led the development of predictive cyber risk models utilizing machine learning algorithms to preemptively identify and neutralize security threats.
- Integrated AI-enhanced IDS/IPS solutions to detect and prevent sophisticated cyber threats in real-time
- Designed and implemented zero-trust security architectures in multi-cloud environments (AWS, Azure, GCP) to enforce least-privilege access and AI-driven workload protection
- Built and maintained AI-powered adversary emulation techniques to simulate advanced persistent threats (APT), enhancing enterprise security resilience by identifying potential vulnerabilities
- Developed AI-enhanced cyber deception technologies to mislead, detect, and counteract cyber adversaries, improving the protection of critical systems
- Implemented AI-driven behavior analytics models to detect insider threats and identify deviations from normal user activity, strengthening internal security measures
- Led real-time security operations, utilizing AI-driven security analytics to identify, investigate, and respond to security incidents instantly, ensuring rapid threat mitigation
- Developed and integrated AI-powered penetration testing tools to conduct automated vulnerability assessments and exploit detection, improving the efficiency and accuracy of security audits
- Engineered AI-enhanced malware analysis platforms to reverse-engineer and neutralize complex cyber threats, reducing the time to identify and mitigate potential risks
- Implemented blockchain security frameworks and post-quantum cryptographic models to enhance cryptographic infrastructures, ensuring long-term data protection against emerging threats
- Designed secure containerized workloads using Kubernetes and Docker with AI-driven runtime threat detection and mitigation, increasing system reliability and security
- Developed and enforced security frameworks aligned with NIST and ISO 27001 standards to enhance organizational resilience, improving the company's defense against cyber threats
- Orchestrated large-scale cybersecurity AI frameworks, improving security operations by enhancing both offensive and defensive strategies
- Utilized AI-powered SIEM integrations to enhance threat intelligence platforms, resulting in more efficient event correlation and quicker threat response
- Collaborated with AI/ML engineers and cloud security architects to develop autonomous threat detection strategies, leading to faster mitigation of security threats
- Monitored global cybersecurity trends and evolved security methodologies and AI-driven advancements to counter emerging cyber threats

University of Bridgeport **Jan 2023 - Dec 2023**

SOC Analyst

- Developed and enforced zero-trust security architectures, ensuring strict access controls, network segmentation, and continuous authentication.

- Led cybersecurity incident response operations, including threat containment, forensic analysis, and mitigation of security breaches.
- Implemented network security controls, including IDS/IPS, firewalls, and endpoint protection, to safeguard against evolving cyber threats.
- Conducted security audits and risk assessments to evaluate vulnerabilities in cloud and on-premises environments, ensuring compliance with NIST and ISO 27001.
- Designed endpoint security frameworks, deploying EDR solutions, and enforcing policy-based controls to protect against malware and unauthorized access.
- Implemented cryptographic security solutions, including encryption protocols, SSL/TLS configurations, and PKI management for data protection.
- Developed automated security compliance reporting frameworks to track security incidents, access controls, and regulatory adherence.
- Conducted vulnerability assessments and penetration testing on enterprise applications and networks to identify security weaknesses and remediation plans.
- Established robust identity and access management (IAM) policies, enforcing least privilege principles and multi-factor authentication (MFA) for critical assets.

Tata Consultancy Services **Apr 2021 - Sep 2022**

Cyber Security Analyst

- Monitored 500+ security alerts daily using SIEM tools (Splunk, QRadar) and Microsoft Defender.
- Conducted incident response work by analyzing security events, identifying false positives vs. real threats, determining host involvement, comparing scan results, analyzing Splunk logs, and prioritizing incidents/events, leading to improved threat management
- Utilized advanced threat detection tools and techniques to identify and investigate security incidents, reducing incident response time by 20%.
- Deployed and managed Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) to implement zero-trust architecture, ensuring secure access to network resources and mitigating potential risks
- Configured, optimized, and modified Zscaler policies, including access control, URL filtering, and threat prevention, to enhance network security and policy effectiveness
- Supported the configuration, optimization, and modification of Zscaler components, enhancing system efficiency and security
- Monitored and troubleshot Zscaler performance issues using advanced diagnostic tools like ZDX, improving system reliability
- Conducted forensic analysis of incidents, reducing false positives by 20%.
- Collaborated with cross-functional teams to develop effective incident response workflows.
- Managed DLP incidents and resolved 300+ security tickets daily, enhancing response efficiency.
- Worked on application security using SAT and DAST, and addressed SQL injection vulnerabilities, enhancing the security posture of applications
- Contributed to the software development life cycle by implementing coding standards, conducting code reviews, and managing source control, which improved code quality and development efficiency
- Communicated alerts to users about intrusions and mailbox compromises, and assisted in implementing countermeasures, reducing the risk of data breaches
- Stayed updated with cybersecurity threats and analyzed threat intelligence feeds to identify potential risks, which helped in proactively mitigating security threats
- Analyzed and triaged security alerts to determine their severity and validity, leading to the identification and resolution of potential security incidents
- Followed established incident response procedures and workflows to address security incidents, coordinating with IT operations, network engineering, and management to ensure effective incident resolution
- Configured and tuned security tools and technologies, such as SOAR platforms, to enhance detection capabilities and reduce false positives, which improved incident response efficiency. Documented incident details, investigation findings, and response actions in incident reports and case management systems, ensuring comprehensive records for future reference
- Generated end-of-shift reports for documentation and knowledge transfer, ensuring seamless transition and continuity for subsequent analysts on duty

Q Spiders Global **Mar 2020 - Mar 2021**

SOC Analyst

- Worked in a 24x7 security operation center, ensuring continuous protection and rapid response to threats
- Monitored and interpreted threats using IDS and SIEM, enhancing threat detection capabilities
- Assisted senior analysts in monitoring and analyzing security events and incidents.
- Investigated malicious phishing emails, domains, and IPs using open-source tools, recommending effective blocking strategies to enhance security
- Responded to security alerts and performed initial triage to determine the severity and validity of incidents.
- Documented incident details, actions taken, and recommendations for future improvement.
- Contributed to developing and documenting standard operating procedures (SOPs) for incident response and threat detection.
- Researched new and evolving threats and vulnerabilities that could impact the monitoring environment, leading to enhanced threat detection capabilities

Certification

- **CompTIA**: CompTIA Security+ Certification.
- **Testout**: Certified Ethical Hacker (CEH) Certification.
- **Qualys**: Vulnerability Detection and Response Certification(VMDR) by Qualys-certified specialist.
- **CISA**: 210W-07 ICS Cybersecurity Vulnerabilities training by CISA.
- **ISC2**: ISC2-CC-Certified in cybersecurity.
- **Splunk**: Intro to Splunk from Splunk.
- **Linkdin**: Build A HIPAA Compliance Program LinkedIn.

Education

University of Bridgeport **Dec 2023**
Master's, computer science

Anna University **Dec 2020**
Bachelors, Electronics and communication Engineering