Sathishkumar Anamalamudi
E-mail: Anamalamudi.sathishkumar@gmail.com
Phone no: (475)655-6223.
LinkedIn: www.linkedin.com/in/sathishkumaraamalamudi-cybersecurity
Location: CT, United States,06605.

SUMMARY:

- Cyber Security & AI Specialist with around 4+ years of expertise in AI-driven security, offensive & defensive security, and advanced threat intelligence.
- Expertise in AI-driven security automation, advanced threat intelligence, and next-generation cybersecurity strategies for proactive threat mitigation.
- Proven ability to engineer self-healing cybersecurity infrastructures using SOAR, XDR, and AI-powered SIEM solutions (Splunk, ArcSight, Cortex XDR).
- Extensive hands-on experience in penetration testing, ethical hacking, red teaming, and adversary emulation to assess and strengthen enterprise security postures.
- Strong background in network security, vulnerability management, and offensive/defensive threat analysis, ensuring comprehensive cyber risk assessment.
- Proficient in machine learning and deep learning techniques for automated anomaly detection, behavioral analytics, and predictive cyber risk modeling.
- Expertise in developing AI-driven deception technologies to mislead, detect, and neutralize advanced cyber adversaries.
- Skilled in cloud security (AWS, Azure, GCP), implementing zero-trust architectures, multi-cloud workload protection, and security monitoring.
- Experience in cyber warfare, threat hunting, and malware reverse engineering, leveraging AI-powered threat intelligence platforms.
- Developed and deployed AI-enhanced intrusion detection and prevention systems (IDS/IPS) and next-gen SIEM integrations for real-time threat monitoring.
- Designed offensive and defensive cybersecurity AI frameworks to proactively counter emerging attack vectors and mitigate zero-day vulnerabilities.
- Hands-on experience with cryptographic security solutions, including post-quantum cryptography, blockchain security, and secure data lakes.
- Led high-profile incident response operations, ensuring rapid detection, containment, and mitigation of advanced persistent threats (APT).
- Developed and enforced security policies aligned with NIST, ISO 27001, and GDPR, ensuring regulatory compliance and cyber resilience.
- Implemented AI-powered endpoint detection and response (EDR) systems to enhance protection against evolving cyber threats.
- Integrated security-as-code methodologies into CI/CD pipelines, ensuring DevSecOps best practices for continuous security enforcement.
- Strong expertise in cloud-native security architectures, container security (Docker, Kubernetes), and AI-driven workload protection strategies.
- Designed and automated intelligent threat modeling techniques to enhance proactive cyber defense strategies and SOC automation.
- Conducted extensive security audits, risk assessments, and penetration testing to identify vulnerabilities and strengthen enterprise defenses.
- Engineered automated response playbooks, integrating AI-based decision-making to improve real-time security incident response.
- Developed and implemented fraud detection systems leveraging cybersecurity analytics, protecting organizations from financial cybercrime.
- Collaborates with AI/ML engineers, cloud security architects, and enterprise IT teams to build cutting-edge autonomous security solutions.
- Strong analytical skills, problem-solving, writing, and communication skills.
- Working in a 24x7 security operation center.

Technical Skills:

Cybersecurity & Threat Intelligence:

- **SIEM:** Splunk, ArcSight, Sentinel, QRadar
- **SOAR:** XSOAR, Phantom
- **IDS/IPS:** Snort, Zeek, Suricata
- **Frameworks:** MITRE ATT&CK, NIST, ISO 27001, CIS Controls
- **Threat Intelligence:** MISP, ThreatConnect, Recorded Future

AI & Security Automation:

- **AI-driven Security:** Machine Learning for Threat Detection, AI-powered SOAR, Behavioral Analytics
- **Tools:** Python, TensorFlow, PyTorch, Splunk Machine Learning Toolkit, ELK Stack

Cloud & Zero Trust:

- **Multi-Cloud Security:** AWS, Azure, GCP
- Zero Trust Architecture (ZTA), CSPM, Kubernetes Security, Cloud Workload Protection

Offensive & Defensive Security:

- **Penetration Testing & Red Teaming:** Kali Linux, Metasploit, Cobalt Strike, Atomic Red Team
- **Malware Analysis:** IDA Pro, Ghidra, YARA, Volatility
- **Secure Coding:** SAST/DAST (SonarQube, Checkmarx, OWASP ZAP)

DevSecOps & Infrastructure Security:

- **Infrastructure as Code:** Terraform, Ansible, CloudFormation
- **CI/CD & Security-as-Code:** GitHub Actions, Jenkins, Policy-as-Code (OPA, Sentinel)
    - **Soft Skills:** Communication, up-skill, teamwork, Problem-Solving, Pressure Handling, critical thinking, and leadership.

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.
- 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) and evaluate enterprise security resilience.
- Developed AI-enhanced cyber deception technologies to mislead, detect, and counteract cyber adversaries before they reach critical systems.
- Implemented AI-driven behavior analytics models to detect insider threats and identify deviations from normal user activity.

- Led real-time security operations, utilizing AI-driven security analytics to identify, investigate, and respond to security incidents instantly.
- Developed and integrated AI-powered penetration testing tools to conduct automated vulnerability assessments and exploit detection.
- Engineered AI-enhanced malware analysis platforms to reverse-engineer and neutralize complex cyber threats.
- Implemented blockchain security frameworks and post-quantum cryptographic models to future-proof cryptographic infrastructures.
- Designed secure containerized workloads (Kubernetes, Docker) with AI-driven runtime threat detection and mitigation.
- Developed and enforced security frameworks aligned with NIST, ISO 27001, and advanced cyber warfare strategies to enhance organizational resilience.
- Orchestrated large-scale cybersecurity AI frameworks for next-gen offensive and defensive security operations.
- Utilized AI-powered SIEM integrations to enhance next-gen threat intelligence platforms and streamline event correlation.
- Collaborated with AI/ML engineers and cloud security architects to drive autonomous threat detection and mitigation strategies.
- Stayed ahead of global cybersecurity trends, continuously evolving security methodologies, and AI-driven security advancements to counter emerging cyber threats.

University of Bridgeport:

SOC Analyst(JAN 2023 to DEC 2023):

- 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 :

Cyber Security Analyst(April 2021 - SEPT 2022):

- Monitored 500+ security alerts daily using SIEM tools (Splunk, QRadar) and Microsoft Defender.
- Responsible for incident response work including analyzing security events, identifying false positives vs. real threats, identifying host involvement, comparing scan results, analyzing Splunk logs & prioritizing incidents/events.
- Utilized advanced threat detection tools and techniques to identify and investigate security incidents, reducing incident response time by 20%.
- Participate in deploying and managing Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) to achieve a zero-trust architecture and principles, ensuring secure access to network resources and mitigating potential risks.
- Support the configuration, optimization, and modification of Zscaler policies, including access control, URL filtering, and threat prevention.

- Support the configuration, optimization, and modification of Zscaler Private Service Edges, App Connectors, Client Connectors, logging, and other related Zscaler components and functionality.
- Monitor and troubleshoot Zscaler performance issues using advanced diagnostic tools included but not limited to ZDX.
- 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.
- Working on application security like SAT and DAST, SQL injection technologies.
- Working on software development life cycle, including coding standards, code reviews, source control management, build processes, testing, and operations.
- Communicate alerts to users regarding intrusions and compromises to their mailboxes and assist with implementing countermeasures or mitigating controls.
- Stay updated with cybersecurity threats, vulnerabilities, and attack techniques. Analyze threat intelligence feeds and reports to identify potential risks and indicators of compromise.
- Analyze and triage security alerts to determine their severity and validity. Investigate alerts to identify potential security incidents or anomalies.
- Follow established incident response procedures and workflows to address security incidents. Coordinate with other teams such as IT operations, network engineering, and management to respond effectively to incidents.
- Configure and tune security tools and technologies to enhance detection capabilities and reduce false positives. Document incident details, investigation findings, and response actions in incident reports and case management systems.
- Generate end-of-shift Report for documentation and knowledge transfer to subsequent analysis on duty.

Q Spiders Global:

SOC Analyst(MARCH 2020 - MARCH 2021):

- Working in a 24x7 security operation center.
- Continuous monitoring and interpretation of threats using IDS and SIEM.
- Assisted senior analysts in monitoring and analyzing security events and incidents.
- Investigate malicious phishing emails, domains, and IPS using open-source tools and recommend proper blocking-based analysis.
- 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.
- Research new and evolving threats and vulnerabilities with the potential to impact the monitoring environment.

Certification:

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

Education:

- Master's in computer science at the University of Bridgeport. **December-2023**
- Bachelors in Electronics and communication Engineering at Anna University. **December 2020**