Sairam P
+91-9059271900
rampalan@aol.com

## PROFESSIONAL SUMMARY

- Security Researcher with 10+ years of experience in the Information Security domain and Cloud, with a core security background in SOC, SIEM, SOAR, and other cutting-edge technologies.
- Delivered end-to-end project management, from collecting requirements to implementation, working with cross-functional teams, including BA, Architects, and QA teams.
- Integrated API services of various tools, such as ServiceNow, Splunk, Datadog, Tanium, BMC Remedy, Atlassian JIRA, Microsoft Exchange, and Microsoft Defender, into the Swimlane Turbine System using Python.
- Provided comprehensive detection coverage for all in-the-wild threats using threat intelligence.
- Prototyped, implemented, and extended backend tools and systems to automate or improve the exploit identification, analysis, and detection process.
- Conducted exploit analysis and Advanced malware reversing.
- Developed and designed innovative cybersecurity solutions for unique and complex technologies.
- Worked on SIEM and Threat Intelligent platforms to understand customer pain points and solve problems.
- Prepared Security assessment project plans, deliverables, reporting, and recommendations.
- Managed Disaster Recovery, Backup, and Restore processes.
- Gained experience with AWS and Azure topics, tools, and concepts.
- Handled Patch Management and Software Upgrades.
- Created and managed Reporting and Analytics.
- Provided cyber security awareness workshops to employees during cyber security awareness month.
- Demonstrated team management skills, including onsite/offshore coordination, status tracking, reporting, and ownership of deliverables, with excellent analytical, problem-solving, and communication skills.

## TECHNICAL SKILLS:

| Skill Classification | Description |
|---|---|
| **Primary Skills** | VAPT, Gap Assessment, Malware Research, HTML, Java, Security Trainings |
| **Secondary Skills** | VS, Windows Terminal, CSS, HTML, Javascript |
| **Platforms** | Swimlane – Turbine, XSOAR, EDR’s, XDR’s, SIEMS, Azure Security Center, AWS Data Lake |

| | |
|---|---|
| **Methodologies** | Waterfall and Agile Methodology |
| **Version Control** | GIT, COPADO, IBM Clear case, BitBucket, GitHub |
| **Management Skills** | Estimates preparation, Coordination with business, team leads, architects, Business analysts and offshore. |
| **Domain knowledge** | Banking, RFP Bidding, Cyber Security Domain, OCSF, Turbine – TEDS |
| **Others (Hands on)** | Microsoft Visual Studio, Azure Security Central, SIEM Configurations – Rapid7, Darktrace, Dataminr, Cortex XSOAR, AWS Athena, Jump Cloud, Carbon Black, Tenable |
| **Cloud Platforms** | AWS, Azure, GCP |

## EDUCATIONAL BACKGROUND:

**Dual MASTER's in Information Assurance and Internet Architecture**, Wilmington University, Delaware, USA.

**Master's DEGREE in Electronic Networks & Computers, New Jersey Institute of Technology,** New Jersey, USA.

**Undergrad Degree in Electronics and Communication Engineering, Vignan University,** Guntur, AP, INDIA.

**Minor Degree in MBA, Vignan University, Guntur,** AP, INDIA.

## CERTIFICATIONS:

- **Certified Cyber Security Expert** – International Forensic Science
- **Certified Cyber Intelligence Investigator (CCII) –** McAfee Institute, Florida, USA.
- **CompTIA Admin+, Network+, Security+**
- **Certified Ethical Hacker (CEH)** – EC Council
- **Microsoft Azure Fundamentals (AZ-900), Security Expert (AZ-500)**
- **SOAR** – Swimlane
- **More Certifications list available on my LinkedIn Profile Page-** https://www.linkedin.com/in/sairampalabindela/

## AWARDS & RECOGNITION:

- Acknowledged as domain expert in multiples levels across several organizations – www.sairam.digital (visit).
- Organized many trainings and awareness sessions on Cyber Security at Ministry of HRD, National Security Agencies along with many Educational Institutions and Corporate offices.

Sairam P
+91-9059271900
rampalan@aol.com

## PROFESSIONAL EXPERIENCE:

| **Project #1** | **Swimlane** |
|---|---|
| Period | May 2023 to till date |
| Role | Sr. Security Solutions Engineer - Contract |
| Software's/Technologies | Swimlane – Turbine SOAR Platform, VIC's (Vendor Interaction Components), SIEM's, XDR's, EDR's |

**Description:**
Swimlane is an AI Enabled Automation for the entire Security Organization, building low-code automation with SecOps, fraud, OT Environments, cloud, compliance, audit and more. Preventing breaches and enabling continuous compliance via a low-code security automation platform that serves as the system of record. This is achieved by connecting through plugins, connectors, VIC (vendor-interaction-components), playbooks, canvas, etc.

**Responsibilities:**

- Technical team to develop connectors, Plugin's & VIC's.
- Was key member in collaboration solutions for AWS Athena and other SIEM Vendors.
- Was responsible for turbine integrating with AWS Security Lake.
- Identify stakeholders' security requirements and allocate technical resources to address them.
- Implemented lean process that led to 15% improvement in SLA performance.
- Trained existing teams to improve security awareness by training them at multiple occasions.
- Introduced code review automation tool, linting tool and unit testing as part of the connector development.
- Worked closely with PO in understanding requirements, making sprint planning, monitoring closely AR's, POV's
- Played SME role in transition external marketplace to app direct.
- Identified the gaps in internal / external marketplace and proposed various solutions by researching other SOAR competitors.
- Worked on AI Content creation and re-deployment of new marketplace with enhancements which includes coordinating with Design team and Data Engineering Teams.
- Was part of adding key features in Turbine like Correlation, Enrichment threat intelligence.
- Played key role in transition from 10.X to 11.X.

| | |
|---|---|
| **Project #2** | TSARO Labs |
| **Period** | Jan 2021 - May 2023 |
| **Role** | Security Researcher |

**Description of project:**

As a Security Researcher at TSAROLABS, your primary responsibility is to identify and analyze potential security threats to the organization's systems, networks, and applications. Your day-to-day activities involve conducting vulnerability assessments, penetration testing, and security audits to detect weaknesses and vulnerabilities. You design and implement threat models, develop and maintain security tools, and collaborate with cross-functional teams to implement remediation measures. Additionally, you stay up to date with emerging threats and technologies, providing recommendations for security enhancements and best practices to ensure the organization's security posture is robust and aligned with industry standards.

**Responsibilities:**

- Conduct vulnerability assessments and penetration testing to identify potential security threats to the organization's systems, networks, and applications.
- Design and implement threat models to anticipate and mitigate potential security risks.
- Develop and maintain security tools, scripts, and methodologies to support security testing and research.
- Collaborate with cross-functional teams to implement remediation measures and security patches.
- Stay up to date with emerging threats, technologies, and trends in the cybersecurity landscape.
- Analyze and respond to security incidents, including incident response and post-incident activities.
- Develop and maintain security documentation, including threat models, vulnerability assessments, and security testing reports.
- Provide recommendations for security enhancements and best practices to improve the organization's overall security posture.
- Collaborate with development teams to ensure secure coding practices and secure software development lifecycle (SDLC) processes.
- Present research findings and security recommendations to technical and non-technical stakeholders, including management and executive teams.

| | |
|---|---|
| **Project #3** | Ananya Technologies Inc, New Jersey. |
| **Period** | June 2015 – Nov 2020 |
| **Role** | Cloud Solution Engineer |
| **Software's/Technologies** | Security Center (ASC), Sentinel (SIEM), Active Directory (AAD), Identity and Access Management (IAM), Key Vault (AKV), Storage Security, Network Security Group (NSG), Firewall, Web Application Firewall (WAF), DDoS |

| | |
|---|---|
| | Protection, Security Center for IoT (ASC for IoT), Cloud Security Gateway (CSG), Cloud App Security (CAS), Information Protection (AIP), Advanced Threat Protection (ATP), Cloud Security Assessment and Compliance (CSAC). |

**Description of project:**
As a Cloud Security Engineer, I designed and implemented a secure cloud infrastructure for a Fortune 500 company using Azure Cloud Security Services. I leveraged Azure Security Center (ASC) to monitor and respond to security threats, and Azure Sentinel (SIEM) to detect and investigate security incidents. I also implemented Azure Identity and Access Management (IAM) to manage access and authentication, and Azure Key Vault (AKV) to secure sensitive data. Additionally, I used Azure Policy and Azure Compliance Manager to ensure compliance with regulatory requirements. The project resulted in a 99.99% uptime and a 50% reduction in security incidents.

**Responsibilities**:

- **Drive Cloud Security Initiatives**: Spearhead cloud security initiatives across the entire portfolio of cloud security services to meet client needs and ensure robust security posture.
- **Lead Cloud Security Teams**: Lead high-performing cloud security teams, fostering a culture of innovation and collaboration to drive security excellence.
- **Executive Stakeholder Engagement**: Engage with senior executive members through regular meetings to understand priorities, gather customer inputs, and align cloud security strategies with business objectives.
- **Cloud Security Assessments and Workshops**: Conduct comprehensive cloud security assessments and workshops on Microsoft O365 Security Compliance, ensuring clients are equipped to address security challenges.
- **CSP Vendor Collaboration**: Collaborate with various Cloud Service Providers (CSPs) to conduct workshops on O365 Security Compliance, promoting a culture of security awareness and best practices.
- **Data Security and Compliance**: Manage technical systems to maintain the confidentiality, integrity, and availability of data, ensuring adherence to regulatory requirements and industry standards.
- **Cloud Security Risk Management**: Demonstrate a deep understanding of current risks and threats to cloud data security, CASB infrastructure, and IT infrastructures, providing technical and managerial expertise to mitigate risks.
- **Security Gap Analysis and Improvement**: Identify gaps and areas for improvement in data security, IAM, and CASB capabilities, collaborating with engineering and product teams to drive enhancements.
- **System Audits and Vulnerability Assessments**: Perform regular and on-demand system audits and vulnerability assessments of systems, internal applications, and CASB services to identify security vulnerabilities and ensure prompt remediation.

- **Log Monitoring and Analysis**: Monitor and analyze logs from various sources (e.g., AWS, Azure, Linux, Networking, and Cloud Appliances) to detect security incidents and anomalies.
- **System Performance and Optimization**: Review periodic reports on server health, resource usage, user experience, and environmental performance to inform next steps and upgrades, ensuring optimal system performance.
- **Vulnerability Management**: Manage application and system vulnerabilities, ensuring timely identification, prioritization, and remediation to minimize security risks.
- **Change and Project Management**: Apply change and project management expertise to ensure seamless execution of security projects, minimizing disruptions to business operations.
- **Security Policy and Compliance**: Review control standards, identify exceptions, and update policies to ensure alignment with regulatory requirements and industry best practices.

| | |
|---|---|
| **Project #4** | RCI Labs – DRDO, INDIA |
| **Period** | June 2012 – MAY 2013 |
| **Role** | JUNIOR SCIENTIST Cum Research Assistant |
| **Software's/Technologies** | MATLAB, SAR (Synthetic Aperture Radar), Doppler Radar, Data Acquisition & Processing |

**Description:**

This project involved the development of an advanced air surveillance radar (AASR) for air defense applications. Utilizing MATLAB, we developed signal processing algorithms for target detection, tracking, and classification. The radar employed synthetic aperture radar (SAR) technology to provide high-resolution images of targets, enabling accurate identification and tracking. The AASR was designed to protect critical infrastructure and assets by providing early warning of potential threats and guiding defensive actions within a dome-shaped coverage area.

**Responsibilities:**

- **System Design:** Contributed to the overall system architecture, defining requirements for hardware, software, and subsystems.
- **Signal Processing:** Developed algorithms for target detection, tracking, and classification, optimizing performance in challenging environments.
- **Integration and Testing:** Coordinated the integration of various subsystems, conducted comprehensive testing, and ensured compliance with performance specifications.
- **Data Analysis:** Analyzed radar data to identify trends, anomalies, and potential improvements.
- **Documentation:** Prepared technical documentation, including system specifications, user manuals, and test reports.