Rayman Thandi

E: thandi.rayman@gmail.com | P: (916) 247-1836 | L:Linkedin Profile | W: Website Portfolio

Professional Statement

A passionate cybersecurity analyst with a strong computer science background and hands-on experience supporting SOC-style alert triage, root cause analysis and issue resolution under tight SLAs.

Education

Bachelor of Science in Computer Science | California State University, Sacramento | Sacramento, CA

Technical Skills

Security Operations & Analysis: Alert triage • Incident lifecycle management • SLA management • Escalation support

Log review and correlation • False positive identification • MITRE ATT&CK technique mapping

Threat Detection & Investigation: Phishing analysis (headers, URLs, attachments) • Malware and endpoint triage • Indicator of Compromise (IoC) analysis • Root cause analysis • Timeline reconstruction

Security Tooling: SIEM & log platforms: Splunk, ELK, Wazuh • **Network & forensic tools:** Wireshark, Autopsy, Volatility and emerging AI supported security tools • **Threat intelligence**: AlienVault OTX

Scripting & Data Handling: Python (log parsing, detection logic, automation), Bash, PowerShell • SQL • REST APIs

Systems & Networking Fundamentals: Linux (Ubuntu, Kali) • Windows Server • TCP/IP, DNS, HTTP/S, SSL/TLS • Active Directory (users, groups, basic GPO concepts)

Cloud & Development Environment: AWS EC2 (basic deployment) • Docker • Virtualization (VirtualBox / Hypervisor) • Git/GitHub • Jira • VS Code • Microsoft 365 • LLMs • Generative AI

Certifications (Active)

- **CompTIA Security+ |** Credential ID: c098ec1678aa458f85e721371b2622e7
- **Blue Team Level One |** Security Blue Team | Credential ID: 462018443
- **Google Cybersecurity Professional Certificate |** Coursera | Credential ID: YKCNEDGVGEQJ

Projects

Honeypot Threat Monitoring Project — Splunk • Cowrie • Ubuntu • SSH | June 2024

- Deployment and configuration of SSH/Telnet honeypot **capturing hundreds of authentication attempts**, generating a dataset of real-world attacker interaction for analysis.
- Analysis of logs to identify suspicious behavior patterns, extract indicators of compromise, and assess attacker techniques.
- Analysis activities in Splunk to correlate events, reduce noise, and distinguish automated scanning from targeted behavior.
- Mapping activity behavior in MITRE ATT&CK techniques to contextualize findings and record analytical conclusions.
- Record findings and investigative limitations in written reports aligned with SOC-style case documentation for auditing.
- More details → Portfolio

Log Analyzer & Alerting System — Python • Flask • Cybersecurity Analytics | May–June 2025

- Develop Python-based log analysis application to process thousands of structured log entries to simulate Tier 1 alert review and detection workflows.
- Implement logic to flag authentication anomalies, repeated failures, and suspicious IP activity, emphasizing signal over noise.
- Apply correlation techniques across events to identify patterns indicative of brute-force/ abuse scenarios.
- Integrate external threat intelligence sources to enrich indicators and support investigative context.
- Design system to demonstrate alerts generation, review and interpretation in SOC-style workflow.
- More details → Portfolio

Virtual Labs | Blue Team Labs Online | Profile | April 2024 - November 2025

- Performed several guided SOC-style investigations spanning phishing, malware execution, endpoint compromise, and network intrusion scenarios.
- Performed alert triage, evidence review, IoC extraction, and timeline reconstruction using structured investigative workflows.
- Analyzed logs, artifacts, and packet data to determine root cause, scope, and potential impact of simulated incidents.
- Documentation of findings with clear summaries, assumptions, and recommended response actions aligned with Tier 1 SOC expectations.

Experience

Alexa Developer | City of Sacramento | August 2022 - May 2023

- Support production applications and backend services by monitoring system behavior, logs, and API workflows, identifying anomalies and service disruptions and issue resolutions.
- Investigate authentication, data flow, and integration issues across REST APIs, Salesforce CRM, and ESRI GIS platforms using structured troubleshooting methodologies.
- Perform root-cause analysis on incidents involving failed transactions, access issues, and system errors, escalating findings with clear impact assessments.
- Document incidents, resolutions, and remediation steps in a ticket-based workflow, aligning with SOC-style case documentation and escalation practices.
- Collaborate in an Agile environment, participating in issue triage, prioritization, issue resolution and post-incident reviews to improve system reliability.

Computer Science Tutor — CSU Sacramento | Feb 2022 - May 2025

- Mentor students through structured problem-solving workflows to diagnose unknown system and application issues in Python, Unix/Linux, and database-backed programs.
- Analyze program output, error messages, and logs to identify root causes, validate hypotheses, and confirm corrective actions.
- Perform troubleshooting logic errors, misconfigurations, and runtime failures, reinforcing investigative techniques foundational to technical incident triage.
- Communicate technical findings clearly and concisely to non-technical audiences, strengthening documentation and escalation-ready communication skills.