Augustine Tambe

a.tambe30@gmail.com
atambe.xyz
https://www.linkedin.com/in/augustine-tambe/ https://github.com/RepTambe/RepTambe

PROFESSIONAL EXPERIENCE

ARCTIC WOLF **Jul. 2024 – Present**
Concierge Security Engineer 2 *Pleasant Grove, Utah*

- Lead point of contact for client security operations, providing tailored threat detection and response guidance.
- Performed advanced investigations into phishing, malware, and privilege escalation attempts across diverse client environments.
- Coordinated with client security teams to align detection and response procedures with their operational requirements.Conducted security posture reviews to enhance incident readiness.

Triage Security Engineer 1 **Apr. 2024 – Jul. 2025**

- Investigated security events across thousands of client environments using SIEM platforms, triaging 200+ events weekly.
- Analyzed host/network artifacts to determine threat scope, persistence mechanisms, and potential data exfiltration.
- Documented incident investigations and response actions in the internal system.
- Authored detailed investigation reports and trained analysts on detection/hunting methodologies..

Children's Miracle Network of Hospitals **Aug 2023 - Apr 2024**
Security Specialist 1 *SLC, Utah*

- Managed endpoint detection and response (EDR) and vulnerability management tools to detect and remediate threats.
- Monitored for and addressed potential data loss prevention (DLP) incidents involving PII, PCI, and PHI.

The Church of Jesus Christ of Latter-Day Saints **Aug 2022 - Jan 2023**
IT Engineer Intern *SLC, Utah*

- Supported IAM operations, establishing SSO connections with partners and managing user/group directory systems. Worked with SAML, OAuth, and Active Directory to maintain secure authentication workflows.

Projects

Home Security Lab

- Built a Proxmox-based virtualized lab with an OPNsense firewall, VLAN segmentation, and remote access. Implemented enterprise-style IDS/IPS configurations for simulated threat detection and prevention.

Splunk Attack Lab (Detection Engineering Practice)

- Deployed a Splunk Attack Range with Atomic Red Team to simulate adversary techniques (e.g., T1059.001 - PowerShell).
- Developed SPL-based detections and Integrated Splunk alerts with a SOAR workflow for automated triage and Discord notifications.

CERTIFICATIONS, SKILLS & INTERESTS

- **Certifications:** HTB CDSA, BTL1, CYSA+, Network+, Security+, AWS CCP
- **Technologies:** SPL, KQL, Splunk, Linux Docker, Python, SIEM, Incident Response, EDR, AWS.

EDUCATION

Brigham Young University **Graduation: 2023**
B S Bioinformatics