Ravi Buddi

ravi@ravibuddi.com ❖ Austin, TX

EXPERIENCE

Indeed **Dec. 2018 – Present**

Sr. Infrastructure Security Engineer (Jan. 2023 – Present) *Austin, TX*

- Deployed Cloudflare WAF company-wide at the account level with managed rulesets, OWASP core rules, and custom rules; tuned to eliminate false positives and moved from monitor to full block mode without business impact.
- Built a fully automated vulnerability triage pipeline using Tines that created a custom risk score by analyzing over 1M historical vulnerabilities against EPSS/CVSS data; this eliminated manual triage and focused daily remediation on the most critical threats across 4K+ servers.
- Led security testing and prompt engineering for agentic AI applications serving 200M+ monthly visitors; developed and validated the core security prompt for an "LLM-as-Judge" architecture to block prompt injections and jailbreaks.
- Achieved and maintained PCI DSS compliance for payment applications using Qualys, coordinating quarterly remediation with development teams and delivering attested reports to auditors.
- Partnered with offensive security and IR teams on purple team exercises to build durable detections and eliminate underlying attack paths, not just patch individual symptoms.
- Led vendor evaluation and deployment of Attack Surface Management solution - defined criteria, assessed multiple vendors, mentored two junior engineers through selection and rollout.

Infrastructure Security Engineer (Apr. 2020 – Dec. 2022)

- Deployed CrowdStrike to 28 Kubernetes clusters (~3,500 nodes) using a GitOps workflow with ArgoCD, eliminating a critical visibility gap for the Incident Response team within our container environment.
- Led CIS Controls implementation for vulnerability management (Control 3) and endpoints (Control 8), successfully passing external audits by authoring documentation and defending controls to auditors.
- Migrated the on-premises Rapid7 InsightVM console to AWS without disrupting scanning operations across 15K endpoints and 4K servers.
- Owned the health and operations for core security tools (CrowdStrike, Rapid7, RunZero), automating maintenance to prevent outages and training engineering teams on response protocols.
- Mentored 5+ junior engineers on security team and contributed to the team's hiring process.

Information Security Engineer (Dec. 2018 – Mar. 2020)

- Owned the enterprise vulnerability management program (Rapid7 InsightVM) for 19K+ assets, managing a complex scanning infrastructure of both agents and credentialed network scanners and driving the remediation lifecycle.
- Automated Packetfence NAC deployment across 26 offices using Ansible (learned on the job), which standardized security controls and enabled a major version upgrade with zero downtime.
- Built the company's internal Root CA from the ground up using AWS CloudHSM, establishing a secure foundation for mTLS and internal certificate issuance.
- Deployed runZero for comprehensive asset inventory after a successful POC, providing the first complete view of all devices on the corporate network.
- Moved critical internal services behind F5 APM to support the company's zero-trust architecture, eliminating VPN requirements for secure internal access.

Secureworks **Jun. 2017 – Nov. 2018**
Advisor, IT Security (Jul. 2018 – Nov. 2018) *Atlanta, GA*
Sr. Analyst, IT Security (Jun. 2017 – Jun. 2018)

- Triaged security alerts and investigated incidents across thousands of customer environments using a custom in-house SIEM. Worked on both generalist security monitoring and more specialized advisory work after moving to a new team.
- Tuned detection rules constantly to reduce false positives and make sure we were catching real threats. Also analyzed raw logs that didn't match any existing rules and created new alerts to catch similar activity in the future.
- Delivered incident summary reports and took customer calls to walk them through security findings and coordinate remediation efforts.

TECHNICAL SKILLS

- **Languages & Automation**: Python, Golang, Terraform, Tines
- **Cloud & Infrastructure**: AWS, Kubernetes, GitOps

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP)
- AWS Certified Security – Specialty (Expires Oct. 2027)
- AWS Certified Solutions Architect – Professional (Expires Dec. 2026)
- Certified Kubernetes Security Specialist (CKS) (*Expires Aug. 2027*)
- GIAC Cloud Penetration Tester (*Expires Jun. 2028*)
- Offensive Security Wireless Professional (OSWP)

EDUCATION

Rochester Institute of Technology **May, 2017**
Masters in Computing Security *Rochester, NY*

- GPA: 4.0/4.0