(720) 722-9759
reece@reecewatkins.tech
https://reecewatkins.tech
/reece-watkins-816017101
Aurora, CO 80015

Reece Watkins

Profile

Cybersecurity Engineer and Army Cyber Officer with over a decade of experience securing enterprise, tactical, OT/SCADA, and intergovernmental networks. Adept in DevSecOps, cloud-native infrastructure, red team operations, and vulnerability management. Proven leader across civilian and military domains, integrating security into CI/CD pipelines, developing automation, detection, penetration assessment tooling, and guiding cloud/Kubernetes security baselines. Manages dispersed cyber teams and delivers advanced threat emulation, incident response, and secure infrastructure at global scale. Brings a rare blend of technical depth, compliance leadership, and mission-oriented communication to align stakeholders to achieve success. Some of my critical assessment questions can help frame a team for success:

How do we sync development velocity with security depth?	How susceptible to exploit are our vulnerabilities in the infrastructure and applications?	What's our strategy to detect / emulate threats in serverless and containerized workloads?	What skills will our next breach require us to have mastered?	What tribal knowledge are we failing to document and scale?	How can we keep our capabilities current and ever evolving?

Professional and Business History

BITSystems (CACI) – Cyber Security Engineer
October 2020 – Present

- Develop, deploy, and maintain secure network and system architectures across multi-network AWS fabrics and domains enabling shift-left vulnerability identification.
- Conducted advanced threat modeling and security assessments across product and cloud containerized infrastructure to identify toxic combinations.
- Authored System Security Plans and change management documentation to support FedRAMP, RMF, and ATO packages, accrediting over 35 ATOs.
- Secure globally dispersed software development teams, managing AI interdiction through secure model training environments and training data sanitization.

BITSystems (CACI) – DevSecOps Software Engineer
September 2018 – October 2020

- Architected, matured, and deployed multi-cloud environments for large enterprise while coordinating between cross-functional teams achieving contract objectives.
- Maintained automated code-quality tools (SAST, DAST, SCA) across developer workflows, shifting security left within the SSDLC.
- Created and implemented robust cloud security stacks, inclusive of both cloud-native and third-party tooling to safeguard critical assets.

US ARMY – Commander – Task Force Cyber (CPT-174 & DCO-E)
July 2014 – Present

- Command five distributed cyber teams conducting highly tailored cyber operations
- Lead red team and incident response for OT/ICS, internal and external Business Units, and intergovernmental networks from start to finish.
- Execute Joint Combined Cyber Operations with EUCOM, CENTCOM, SOCOM, CYBERCOM throughout the areas of operations through tailored Cyber Packages.
- Spearhead secure robotics, RF engineering, and software R&D for digital force protection and close access operations.

SABIO Systems – Development Team Engineer
February 2016 – January 2018

- Led SharePoint modernization through AWS-hosted stack and custom tooling.
- Conducted statewide incident response and cyber validation exercises with Colorado OIT, State and local governments, Military, and Federal agencies.
- Delivered full-stack RESTful applications and data infrastructure for support to Domestic Operations and emergency management.

Skills / Knowledge

- **Assessments:** FedRAMP, ITL, Vulnerability, Threat
- **Cloud/Infra:** AWS, EKS, RKE2, Docker, Kubernetes, Terraform, Helm, Argo, CloudFormation
- **Security Tooling:** Nessus, Suricata, ELK, Splunk, OWASP ZAP, Grype, Fortify, Black Duck, Cribil
- **Secure Automation:** GitLab CI, Jenkins, Ansible, Chef, Puppet, Packer,
- **Programming:** Python, Shell, PowerShell, C/C++
- **Monitoring:** Prometheus, Grafana
- **Vulnerability Testing:** Burp Suite, Kali, Nmap, John, Wireshark, Metasploit, Aircrack, SQLi, Netcat
- **Frameworks:** CIS, CSA, NIST, ISO, PCI
- **Leadership:** Distributed team leadership, Program ownership, Training & mentorship

Certifications

- ISC2 - CISSP
- SANS - GCIH
- SANS - GSEC
- CISCO - CCNA
- CompTia - CYSA+
- CompTia - SEC+
- CompTia - NET+
- In process: OSCP, CPTS, and GXPN

Education

- B.S. in Computer Information and Systems, emphasis in development, from Missouri Valley College, 2014
- US Army Cyber Center of Excellence (CCoE)

Relevant Project Experience

Enterprise Detection-as-Code Platform (Cloud & K8s)

Built a modular detection-as-code platform that ingests AWS signals and enterprise telemetry (Carbon Black, Trellix, Patrol Agent, Flexera) plus scanners (Nessus, Grype) into Elastic, Prometheus, and Grafana. Fully versioned with GitLab CI for automated testing, rollout, and rollback. Forked open-source code to create an IC-authorized container monitoring capability and extended visibility to Kubernetes clusters running on RKE2.

Secure Personal CI/CD Blog Site (https://reecewatkins.tech)

Containerized and stored in EKS, deployed via private GitLab Pages behind Cloudflare, enforcing build-time scanning with threshold-based rejection and pre-production functionality tests. This codified "shift-left" guardrails that block vulnerable or misconfigured builds before release demonstrating practical policy-as-code integration that maps cleanly to product and production infrastructure security.

Digital Force Protection Toolkit (Threat-Informed Engineering)

Forked an Arduino ESP32 camera project (C/C++) to add Ethernet-only operation, reducing EMS signature while preserving mission functionality. Provisioned GL.iNet routers with open-source firmware for pre-built connectivity and local signal reporting. This work applied adversary-aware constraints and secure-by-default design under operational conditions, reinforcing threat emulation and low-noise telemetry patterns you can reuse in cloud/edge scenarios.

Proxmox Cloud/Container Cyber Range (Open Source)

Built a multi-VLAN homelab via Proxmox (plus a small ESXi dev cluster) to practice adversary emulation and defense. Orchestrated RKE2 with Rancher and GitOps via Argo/Terraform; centralized auth with Keycloak and Vault; ingress via NGINX. Telemetry through Security Onion, Kibana, Prometheus/InfluxDB/Grafana and remote access with WireGuard. Emulated ATT&CK TTPs (Kali/Metasploit) and Caldera.