RUSSELL BARTSON
Portland, OR | www.linkedin.com/in/Rbartson

SENIOR SECURITY ENGINEER

Application Security | Security Automation | AI-Assisted Security Engineering

SUMMARY

Senior Security Engineer and Technical Lead with 20+ years of experience across enterprise security, infrastructure architecture, cloud environments, endpoint protection, and security operations. Proven track record of building security capabilities from the ground up, partnering with engineering teams, and translating complex security requirements into scalable, practical controls.

CORE COMPETENCIES

- **Application Security:** Application security reviews, security architecture, vulnerability assessment support, secure design principles, threat modeling (STRIDE), remediation collaboration
- **Secure Development Workflows:** Terraform reviews, GitLab merge requests, CI/CD security scanning, security finding assessment
- **Programming & Code Analysis:** Python, Bash, Terraform
- **Security Automation:** CI/CD security scanning, infrastructure-as-code controls, workflow automation, telemetry monitoring, tool integration
- **AI-Assisted Security:** Application of AI systems and LLM/agent tooling to security workflows and automation
- **Security Architecture:** Threat and exposure reduction, network segmentation, secure configuration baselines, Zero Trust principles
- **Technical Leadership:** Security program ownership, architectural standards, cross-functional collaboration, SOPs, runbooks

KEY ACHIEVEMENTS

- **Established Security Programs:** Built enterprise endpoint and network security capabilities aligned with NIST SP 800-53 and the Secure Controls Framework, including tooling, configuration baselines, telemetry, and operational processes.
- **Path Traversal Remediation:** Investigated a Snyk-reported path traversal vulnerability in Caldera, used AI-assisted coding to develop a remediation, reviewed the resulting code, and reran the scan to confirm the finding was resolved.
- **Advanced Security Automation:** Designed infrastructure-as-code driven web application firewall (WAF) patterns and developed automated monitoring to improve control visibility and operational reliability.
- **Applied AI to Security Workflows:** Integrated AI systems and agents into professional security workflows to automate and accelerate security outcomes.
- **Enabled Secure Infrastructure Modernization:** Delivered network security improvements, secure connectivity architecture, and security control enhancements across enterprise environments.

PROFESSIONAL EXPERIENCE

Quanata

Senior Security Engineer | December 2022 – Present

Lead engineer for enterprise network and endpoint security programs, responsible for security architecture, tooling, control implementation, telemetry integration, and operational security improvements.

Security Engineering & Architecture

- Built and matured enterprise security capabilities from the ground up, aligning security architecture and controls with NIST SP 800-53 and the Secure Controls Framework (SCF).
- Defined secure configuration baselines across macOS, Linux, and network infrastructure to ensure consistency and reduce exposure.
- Designed infrastructure-as-code driven web application firewall (WAF) patterns to strengthen perimeter protection.
- Partnered with Engineering, IT, and Compliance to implement secure configurations, address technical risks, and align security practices across boundaries.
- Conducted application security reviews and automated scanning activities using OWASP Top 10 standards, bridging infrastructure and security engineering discipline.

Security Tooling & Automation

- Integrated endpoint and network security telemetry into Splunk, supporting log normalization, correlation rule tuning, and security operational dashboards.
- Implemented automated monitoring of telemetry data-source health to ensure visibility into logging integrity and coverage.
- Administered CrowdStrike EDR, Jamf, and Kolide endpoint security controls, optimizing policy enforcement, detection coverage, and device posture.
- Applied AI systems and Wiz CSPM security scanning to workflows, streamlining cloud risk identification and vulnerability management.

Technical Leadership & Incident Response

- Owned technical direction and operational development for endpoint and network security domains.
- Established security workflows, RACI models, SOPs, and runbooks to standardize operations and clarify ownership.
- Responded to escalated security detections and incidents, coordinating investigation, remediation, and root-cause analysis with cross-functional teams.
- Supported SOC 2 assessments by mapping technical evidence to control requirements and strengthening compliance documentation.

Quanata / BlueOwl

Senior Systems Engineer | May 2021 – December 2022

Senior infrastructure engineer responsible for network security architecture, identity integrations, infrastructure reliability, and secure connectivity.

- Managed enterprise network security and infrastructure technologies, including firewalls, switches, routers, Wi-Fi, DNS, and ISP services.
- Modernized network infrastructure and security baselines to improve configuration consistency and reduce attack surfaces.

- Replaced legacy firewall platforms with next-generation Palo Alto firewalls, strengthening inspection, logging, and threat prevention.
- Designed migration solution from traditional VPN to Prisma Access SASE architecture, improving secure access and Zero Trust alignment.
- Designed and deployed secure network architecture for new Arizona office location, including connectivity, ISP integration, and access controls.
- Supported Okta-based IAM, including provisioning/deprovisioning workflows, role-based access control (RBAC), and least-privilege policies.
- Investigated escalated security and infrastructure incidents, performed root-cause analysis, and led remediation efforts.

Telestream

Senior Network Engineer | July 2019 – May 2021

Infrastructure engineer responsible for securing and modernizing AWS and on-premises environments, improving visibility, and supporting distributed operations.

- Architected AWS environments using EC2, RDS, and CloudFormation, embedding security controls into infrastructure design and provisioning.
- Designed global network and security architecture to improve monitoring, identity alignment, and service integrity.
- Led infrastructure modernization initiatives involving firewalls, storage, servers, and physical access controls.
- Supported business continuity during the Tektronix-to-Telestream merger through infrastructure integration and modernization.
- Migrated legacy ClearCase and SVN environments to Git-based workflows, improving source-control consistency and security lifecycle management.

FOUNDATIONAL INFRASTRUCTURE & SECURITY EXPERIENCE

- **DevOps / Systems Administrator** | Aspen Capital — January 2019 – July 2019
- **IT Manager** | Korbel — 2017 – 2019
- **Senior Systems Administrator** | WB Games — 2014 – 2017
- **IT Specialist** | Defense Logistics Agency — 2010 – 2014
- **Network Administrator** | VT Group — 2008 – 2010
- **IT Specialist** | U.S. Navy — 2004 – 2008

EDUCATION & CERTIFICATIONS

Bachelor of Science, Computer Information Systems — Magna Cum Laude

Certifications:

- GIAC Incident Handler (GCIH)
- GIAC Cloud Security Automation (GCSA)
- CompTIA Security+