RORY GARSHOL

Senior Cybersecurity Engineer / Cloud Security Engineer
rgarshol@gmail.com • linkedin.com/in/rory-garshol • (925) 250-4994

EXECUTIVE SUMMARY

Senior Cybersecurity Engineer with 20+ years of experience designing, building, and operating security systems across on-prem, hybrid, and cloud environments. Career spans foundational infrastructure and network security, large-scale cloud migration to Azure and AWS using infrastructure-as-code, and modern cloud security engineering embedded directly into CI/CD and platform workflows. Experienced owning vulnerability management programs, privileged access controls, security automation, incident response, and human-risk reduction initiatives, with a consistent focus on translating security signals into actionable outcomes for engineering teams and leadership. Owned the full lifecycle, availability, tuning, and escalation of enterprise security platforms supporting detection, vulnerability management, and incident response in production environments.

BEST WESTERN HOTELS & RESORTS — Senior Cybersecurity Engineer (2022–Present)

Vulnerability Management & Risk Reporting

- Designed and operated an end-to-end vulnerability management program spanning cloud infrastructure, container platforms, and infrastructure-as-code. Implemented and integrated Tenable Nessus, Aqua Security, Snyk, and AWS Security Hub, automating aggregation, normalization, prioritization, and validation of CVE findings across environments, informed by ongoing review of threat intelligence and vulnerability disclosures.
- Built reporting and notification workflows that translated raw scanner output into actionable, team-specific remediation guidance for product and platform teams, shifting vulnerability remediation from ad-hoc security requests to planned engineering work with clear ownership, tracking, and closure of risk.
- Leveraged automation and scripting to post-process vulnerability data, correlate findings across tools, and support consistent reporting and alerting used during operational reviews and incident response.
- Maintained technical documentation for vulnerability workflows, platform configurations, and reporting outputs to support audits, onboarding, and operational continuity.

Privileged Access & Identity Controls

- Implemented and operated Privileged Access Management (PAM) controls across AWS and Azure, including least-privilege role design, controlled privilege elevation, secrets management, and break-glass access to support secure operations and incident response.

CI/CD & DevSecOps Security

- Embedded preventative and detective security controls directly into CI/CD pipelines by integrating static analysis, container scanning, infrastructure-as-code validation, and scripted policy enforcement at build and deploy time.
- Tuned enforcement thresholds and workflows to block genuinely risky changes while minimizing false positives, allowing engineering teams to remediate issues early without slowing delivery velocity or introducing unnecessary friction.

- Participated in secure code reviews and design discussions with engineering teams, identifying security risks, validating remediation approaches, and ensuring application changes aligned with secure-by-design principles.

Cloud Security Guardrails & Automation

- Built and maintained Terraform-based security guardrails and standardized modules to enforce secure-by-default cloud deployments across AWS and Azure.
- Encoded security requirements such as identity boundaries, network controls, logging, and encryption into reusable infrastructure patterns, reducing configuration drift and ensuring consistent security posture across environments.

Incident Response, Detection & Automation

- Operated SIEM-driven detection and incident response workflows, investigating alerts using security telemetry from logs, events, and detections across cloud, network, and application environments.
- Built Python-based automation to process, enrich, and route security alerts, reducing noisy or duplicate events and surfacing high-confidence signals into existing security and platform operational workflows for investigation and response.
- Automated alert enrichment to add context such as asset ownership, environment, and severity, enabling faster triage and more consistent handoffs during active incidents and on-call rotations.
- Provided escalation support for complex security incidents, including platform-level troubleshooting, alert logic refinement, and post-incident control improvements.
- Fed lessons learned from incidents back into detection logic, alert automation, and preventative controls to continuously improve signal quality and response effectiveness.
- Played a key role in the migration of SIEM infrastructure from Splunk Enterprise to Splunk Cloud, supporting the transition of ingestion pipelines, detection logic, alerting workflows, and operational processes to a cloud-managed platform.
- Partnered with engineering and operations teams to validate data integrity, performance, and alert fidelity during the migration, ensuring continuity of detection and incident response capabilities throughout the transition.
- Tuned detections and alerting post-migration to account for differences in data flow, latency, and platform behavior between Splunk Enterprise and Splunk Cloud, reducing noise and preserving actionable security signals.

Compliance & Regulatory Support

- Supported PCI DSS compliance by designing, operating, and evidencing technical security controls across cloud infrastructure, identity systems, vulnerability management, logging, and incident response workflows.
- Partnered with audit, risk, and engineering teams to provide technical evidence, explain control implementation, and remediate audit findings through durable security and platform improvements.

CIRIUS GROUP, INC. — Cybersecurity Architect / IT Manager / Lead Consultant (2005–2022)

Cloud Migration & Infrastructure Transformation

- Led the migration of enterprise infrastructure from on-prem environments to Azure and AWS, designing cloud landing zones and deployment patterns using Terraform.
- Codified network, identity, and security baselines as infrastructure-as-code, balancing rapid cloud adoption with consistent controls across environments and teams.
- Developed and maintained Terraform modules and supporting scripts to standardize deployments, manage environment differences, and automate repeatable infrastructure changes during migration and ongoing operations.

Network Security & Perimeter Architecture

- Designed, deployed, and operated Palo Alto Networks firewalls as the primary perimeter and segmentation control for enterprise and healthcare environments.
- Defined security zones, routing, NAT, and policy structures to support legacy systems, cloud-connected workloads, and hybrid traffic flows.
- Managed firewall rule lifecycle, logging, and monitoring, ensuring changes were reviewed, traceable, and aligned with security and compliance requirements.

Security Engineering & Operational Ownership

- Served as the primary owner of enterprise security engineering and operations, spanning infrastructure security, network controls, identity systems, and monitoring.
- Built operational processes around change management, incident response, and system hardening that supported mission-critical and regulated workloads.
- Ensured security controls were grounded in how systems were actually built, deployed, and operated, rather than theoretical policy models.

Microsoft Identity, Endpoint & Platform Management

- Owned and administered enterprise Microsoft identity and endpoint platforms, including Active Directory, Windows Server, Office 365, and Intune, supporting authentication, authorization, device management, and secure access across the organization.
- Designed and maintained Active Directory architectures, including domain structure, Group Policy, service accounts, and identity integrations with enterprise applications and security controls.
- Led the transition from on-prem Microsoft services to Office 365, implementing identity integration, access controls, and security configurations to support secure collaboration and email services.
- Implemented and managed Intune for endpoint management and policy enforcement, integrating device compliance, configuration baselines, and security requirements into broader identity and access workflows.
- Investigated and resolved security and operational issues spanning user authentication, endpoint behavior, and platform configuration by analyzing interactions across software, operating systems, and underlying infrastructure.

- Managed and secured enterprise endpoints and servers using Intune and Active Directory, enforcing device configuration, compliance, patching standards, and integrating endpoint security telemetry into centralized logging and incident response workflows.

Security Awareness & Human Risk Reduction

- Designed and operated enterprise security awareness initiatives, including phishing simulation campaigns, to measure organizational susceptibility to social engineering and reduce credential-based attack risk.
- Analyzed phishing simulation results alongside real-world incident trends to identify high-risk behaviors, tailoring training and awareness efforts to address observed weaknesses rather than generic compliance checklists.
- Integrated human-risk insights into broader security strategy, reinforcing technical controls with user education to reduce the likelihood and impact of social engineering attacks.

Platform Reliability & Risk Reduction

- Led security hardening and modernization efforts across core platforms, reducing system outages by 78% and achieving sustained 99.999% uptime for critical systems.
- Balanced security controls with reliability and performance requirements, ensuring protective measures improved — rather than degraded — system stability.

Compliance & Audit Enablement

- Designed and operated security controls supporting HIPAA, HITRUST, and SOC 2 requirements across infrastructure, identity, network security, logging, and incident response.
- Supported internal and external audits by producing technical evidence, explaining control operation, and implementing remediation actions to address audit findings in regulated healthcare and enterprise environments.

Leadership & Advisory Role

- Acted as a trusted technical and security advisor to executive leadership and enterprise customers, translating infrastructure and security risk into clear operational and business terms.
- Mentored engineers and consultants across infrastructure and security disciplines, establishing durable practices that scaled beyond individual contributors.

EDUCATION

Bachelor of Science in Computer Science — Holy Names University

CERTIFICATIONS

GIAC Certified Incident Handler (GCIH)
GIAC Public Cloud Security (GPCS)
GIAC Cloud Security Automation (GCSA)
CompTIA Security+