SUSHIN K

Senior Cloud Security Software Engineer

sushink70@gmail.com | +91 9074958879 | GitHub | LinkedIn | LeetCode | Hackthebox

PROFESSIONAL SUMMARY

Senior Cloud Security Software Engineer with **7+ years** building security platforms and Kubernetes infrastructure across AWS, Azure, and GCP. Expert in Linux security, zero-trust architecture, network security, container security, eBPF threat detection, and systems programming (**Rust, Go, C/C++**).

CORE SKILLS

Languages: Go, Rust, Python, TypeScript, C/C++
Core CS Concepts: Data Structures and Algorithms, OOPs concepts, Distributed systems, Concurrency patterns, CAP theorem, Event-driven architecture, Microservices patterns, Zero-trust architecture
Cloud & Platforms: AWS, Azure, GCP, Kubernetes (EKS, GKE, AKS), RHEL, Crossplane, Terraform
Containers & Observability: containerd, Docker, Helm, Prometheus, Grafana, OpenTelemetry, Pixie
Kernel & Low-Level: eBPF, XDP, AppArmor, SELinux, BPF CO-RE, libbpf, bpftrace
Security & Compliance: Falco, MITRE ATT&CK, SPIRE/SPIFFE, cert-manager, Tetragon, Harbor, Kyverno
Networking & Mesh: BGP, NATS, mTLS, gRPC, CNI, Cilium, Calico, VXLAN, Gateway API
Runtime & Execution: wasmcloud, Cloud Hypervisor, QEMU/KVM, Podman, Confidential Computing
Libraries & SDKs: kube-rs, AWS SDK (Boto3, aws-sdk-go), GCP Client Libraries, Tokio, hyper, tonic (gRPC)
Database & Data Infrastructure: PostgreSQL, pgaudit, MongoDB RBAC, Vitess, Redis, Apache Cassandra
Security Practices: Secret rotation, Zero-trust networking, Defense in depth, Secure SDLC
DevSecOps: GitHub Actions, GitLab CI, Jenkins, Argo (CD/Workflows/Rollouts/Events)

PROFESSIONAL EXPERIENCE

Information Security Consultant I – P3

Lumen Technologies — Bengaluru, India | Oct 2023 – Present | Promoted from P2 → P3 level

• Architected and maintained Network Protection Services using GRE tunnels, IPsec VPN, BGP route filtering, and preventing 1,200+ DDoS attacks and blocking 98.7% of malicious traffic (15TB+ filtered monthly), achieving 99.8% uptime SLA and 98% customer satisfaction across 300+ enterprise clients.
• Architected security automation framework using Python/Go with SOLID principles, applying design patterns (singleton for config, factory for parsers, observer for alerts), achieving 95% code coverage, maintaining < O(n log n) complexity for critical security operations.

Information Security Software Engineer – P2

Lumen Technologies — Bengaluru, India | Dec 2020 – Oct 2023

• Deployed DDoS mitigation using Arbor Networks TMS based traffic baselines, mitigating 15 volumetric attacks (peak 20Gbps), blocking 1.3M malicious connections daily, reducing false positives by 62%, and protecting $40K+ revenue-generating services.
• Automated network security verification using Python scripts and Juniper/Nokia router CLIs, scanning 500+ network devices, identifying and remediating misconfigurations, reducing attack surface by 45% and achieving zero security audit findings.
• Secured API infrastructure by implementing OAuth2/JWT authentication, rate limiting, GraphQL query depth limiting (max 5 levels), and WebSocket connection validation, reducing credential stuffing attacks.

Networking Engineer – Python Network Automation

Tejas Networks — Bengaluru, India | Jan 2019 – Dec 2020

• Architected network security automation framework using Python, policy templates, and Benchmark validation, enforcing 150+ security controls (SELinux policies, firewall rules, SSH hardening) across 200+ RHEL servers, reducing deployment time from 6 hours to 54 minutes (85% reduction), eliminating 100% of human configuration errors, and achieving 100% compliance in 12 consecutive security audits.
• Investigated 47 security incidents using tcpdump, Wireshark, audited logs, strace, and identifying root

causes (kernel vulnerabilities, privilege escalation attempts, network intrusions), implementing preventive controls (kernel patches, SELinux policies, iptables rules), reducing incident recurrence by 91% and MTTR (Mean Time To Resolve) by 68% (from 4.2 hours to 1.3 hours).
• Conducted security testing of optical network devices using custom Python test harness, and protocol conformance testing (SNMP, SSH, TLS), identifying 23 security defects (buffer overflows, authentication bypasses, weak crypto), reproducing 100% in isolated lab environments, accelerating bug resolution by 55%, and preventing 8 potential bugs from reaching production networks.

OPEN-SOURCE CONTRIBUTIONS

bpfman **(**Rust**)** https://github.com/sushink70/bpfman An eBPF Manager for Linux and Kubernetes.
bpftrace **(**C/CPP**)** https://github.com/sushink70/bpftrace High-level tracing language for Linux.
MemErase (Rust/C++ secure memory wiping tool) implements standard 7-pass wipe erasure benchmarked at 2.1GB/s throughput on NVMe SSDs. https://github.com/sushink70/memErase
Conjure (Python) https://github.com/sushink70/conjure Python code visualizer Conjure is a production-ready CLI tool for Python code execution step-by-step.
Cilium (Go) https://github.com/sushink70/cilium eBPF-based Networking, Security, and Observability.
bcc (C) https://github.com/iovisor/bcc Tools for BPF-based Linux IO analysis, networking, monitoring.
libbpf (C) https://github.com/libbpf/libbpf Automated upstream mirror for libbpf stand-alone build.

PROJECTS

Network Audit Tool (Python, Django, SQL, Linux) – Automated auditing, configuration analysis, and compliance reporting. https://github.com/sushink70/wyvern-netaudit-pro
Network Automation System (Python, RHEL, Proxmox) – Automated for optical and Linux systems.
NgrokAlive (Python, ngrok, Linux) - ngrok keep alive script. https://github.com/sushink70/ngrokAlive

EDUCATION

Bachelor of Engineering (Electronics & Communication Engineering) Anna University, Chennai - 2016
XIIth - Computer Science - Kerala State Examination Board, Kerala - 2012

COURSES AND CERTIFICATIONS

EC Council: Certified Ethical Hacker (CEH v11) – Bengaluru
Networkers Home: CCNA, CCNP R&S and Security – Bengaluru
Emertxe: Certified Embedded Professional, Specialized in Advanced Embedded C, Linux Device Drivers, Kernel Development, Network programming, Data Structures and Algorithms – Bengaluru

ACHIEVEMENTS

• Promoted from P2 → P3 for outstanding technical performance.
• Developed Python automation framework using Django, reducing configuration workload by 75%.
• Built log aggregation pipeline using Go with concurrent programming (goroutines, channels), implementing B-tree indexing and bloom filters, processing 2TB+ logs daily, reducing storage by 67% through compression algorithms, enabling <50ms security query response across distributed clusters.
• Architected zero-trust network segmentation using Cilium network policies, Istio mTLS, OPA admission control, blocking non-compliant pod deployments, reducing blast radius by 70% (red team verified), and achieving 99.2% threat detection across Kubernetes nodes.
• Build custom eBPF programs using bpf/libbpf for packet filtering at kernel level, bypassing iptables overhead. Implement connection tracking and rate limiting. Integrate with Cilium for visualization and policy management, benchmark against traditional kube-proxy (expect 30-40% latency reduction).
• Build OpenTelemetry Collector + Prometheus + Grafana + Loki + Tempo stack capturing security events from K3s. Collect audit logs, Falco alerts, network flows (eBPF), and API server events into unified dashboards. Created custom Grafana panels showing MITRE ATT&CK technique detection.

Sushin K