Divye Kalra

Livermore, CA | divyekalra3@gmail.com | +1 4438006625 | LinkedIn | Github | Website

Education

Johns Hopkins University — **Baltimore, USA**
M.S. Cybersecurity — *Aug 2024 – Dec 2025*

Birla Institute of Technology and Science (BITS) Pilani — **Hyderabad, India**
B.E. Electrical and Electronics; M.Sc. Mathematics (Double Major) — *Aug 2019 – Jun 2024*

Technical Skills

- **Languages & Core Technologies:** Python, C, C++, Java, Rust, SQL, Bash, HTML/CSS, AWS, GCP, Docker, Kubernetes, OpenStack, Linux, FastAPI, Django, Burp Suite, Wireshark, Ghidra, Git, GitHub, MySQL, PostgreSQL, Prometheus, Grafana, Loki, Tempo, Proxmox, Jira, Ollama, Terraform
- **Security:** Application Security, Secure SDLC, Threat Modeling, SIEM, Incident Response, Logging and Monitoring, Threat Intelligence, IAM/RBAC/MFA/SSO, Endpoint Security, Zero Trust Architecture, Risk Management and Compliance, MITRE ATT&CK, ISO 27001, CIS, HIPAA, PCI-DSS

Experience

Wildlife for All — Information Security Engineer — Feb 2026 – Present

Bringing formal security oversight to a nonprofit's SaaS stack — auditing the platforms staff rely on daily against CIS benchmarks and enforcing access controls to eliminate misconfigurations and shrink the organization's attack surface.

- Reduced misconfigurations by **30%** across Google Workspace, Slack, and GiveButter by auditing against CIS benchmarks and eliminating unused OAuth connectors and dormant automation workflows.
- Cut the organization's attack surface by **40%** by enforcing least-privilege access, RBAC, SSO, MFA, and API key rotation across all platforms, triaging findings by severity to close the highest-risk gaps first.

JHU Applied Physics Laboratory — Information Security Engineer — Jan 2025 – Dec 2025

- Designed and implemented the first complete SCMS (Secure Credential Management System) reference — a 6-service system comprising a 3-tier certificate authority hierarchy, vehicles broadcasting digitally-signed messages, and roadside server with **15+** real-time misbehavior checks — enabling end-to-end research on Connected and Automated Vehicle (CAV) authentication and misbehavior detection.
- Mitigated replay attacks and location spoofing in V2X networks via a privacy-preserving pseudonym certificate revocation pipeline using cryptographic linkage values; integrated C-V2X into an open-source security platform to accelerate CRL delivery, reducing communication latency by **20%**.

IITB Trust Lab — Applied Cryptography Engineer — Jan 2024 – Jun 2024

- Reduced encryption overhead by **30%** while delivering the first open-source Rust implementation of CASE — a scheme that hides message content, sender, and receiver identity — by limiting operations to fixed-size keys via a hybrid symmetric/asymmetric construction.
- Achieved **15%** faster anonymous signature verification by eliminating redundant scalar multiplications and batching hash computations across the three-step path: commitment decryption, signature check, and consistency verification.
- Cut intern ramp-up time by **40%** by building onboarding documentation that mapped each formal security definition from the paper directly to its corresponding code module.

Cyber Security Hub, Macquarie University — Confidential Computing Engineer — Jul 2023 – Dec 2023

- Built a privacy-preserving record matching system using Trusted Execution Environments (TEEs) and differential privacy (DP) - achieving **0.45s** latency on 30K records and **∼16s** on 1M records.
- Reduced side-channel information leakage by **30–50%** through distributed enclave partitioning, validated on datasets (size: 30K – 1M records); produced the first algorithm combining TEEs, multi-party computation, and DP for record matching

Projects

- **Production-Style Homelab Infrastructure**
  Fully self-hosted home infrastructure — deploying **10+** services across Proxmox VMs and containers including TrueNAS, Pi-hole, OPNsense, and Prometheus/Grafana/Uptime Kuma monitoring — with Tailscale VPN for remote LAN access without port-forwarding and select workloads on AWS, eliminating all cloud storage subscriptions.
- **LLM-Powered Security Code Review Assistant**
  Detected **25+** vulnerability classes across **8+** languages with **95%** accuracy by building a two-phase SAST pipeline — regex pattern matching to surface candidates, GPT to validate exploitability in context and generate a secure fix — with every finding mapped to OWASP, CWE, and MITRE ATT&CK with CVSS scores, exposed via CLI and FastAPI web UI.
- **AI-Driven Security Operations Center (SOC)**
  Reduced false positives by **70%** and mean time to detect (MTTD) by **60%** while processing **1000+** events/sec at **95%** accuracy — by building a SOC (Security Operations Center) dashboard with ML based anomaly detection, a Claude natural language query interface replacing manual log query syntax, and an incident correlator mapping alerts by shared IP, user, and attack pattern to MITRE ATT&CK kill chains.
- **Kubernetes Security (Policies, Runtime, and Exploitation)**
  Executed full Kubernetes attack chains — Server-Side Request Forgery (SSRF) to steal a mounted service account token and enumerate cluster secrets, misconfigured RBAC to exfiltrate secrets via pod volume mount, and a privileged container escape to gain access to the underlying nodes — then hardened each attack path using Kyverno admission policies aligned to CIS benchmarks and validated detection coverage with Cilium Tetragon kernel-level eBPF telemetry.

Certifications and Achievements

- Hack The Box Certified Penetration Testing Specialist (HTB CPTS) - Ongoing
- AWS Certified Cloud Practitioner (AWS CCP)
- CompTIA Security+