Nevin Shine

Undergraduate Systems Security Researcher

Citizenship: German (Native Speaker) | **Phone:** +49 157 54256832
Neustädterstraße 130A, 90431 Nürnberg, Germany | Currently in India — Available On-site May 2026
Email: nevinshine05@outlook.com | GitHub: github.com/nevinshine

RESEARCH SUMMARY

Undergraduate Researcher specializing in **Linux runtime defense** and **kernel-bypass networking**. Focus on eBPF/XDP enforcement, systems security, and bridging the semantic gap in AI agent security. Architect of the **TELOS** strategy, a hybrid defense architecture integrating independent Host and Network engines. Expert in syscall interception, zero-copy datapaths, and adversarial evasion (TOCTOU). Seeking to apply research on **eBPF enforcement** and unsupervised anomaly detection at Fraunhofer AISEC.

TECHNICAL ARSENAL

- **Kernel & Systems:** eBPF/XDP, Linux `ptrace`, Seccomp, Cgroups v2, Namespaces, Ring Buffers, LSM.
- **Languages:** C (System/Driver), Python (ML/Analysis), Go (Control Plane), Rust (Working Knowledge).
- **Security Domains:** Runtime Enforcement, Kernel Exploitation, Malware Analysis (Ransomware), Network Forensics.
- **Engineering Practices:** Zero-Copy Memory Management, Kernel Debugging (GDB/kgdb), Performance Profiling.
- **Tools:** Docker, Kubernetes (DaemonSets), Git, PyTorch, Wireshark, `strace`, perf, bpftool.

RESEARCH EXPERIENCE

Sentinel Runtime (TELOS Core) Nov 2025 – Present
Lead Architect (Host-Based Runtime Defense) github.com/nevinshine/sentinel-runtime

- **Role in TELOS:** Kernel-level enforcement engine preventing unauthorized execution and file access by compromised agents.
- **Core Engine (M3.2):** Engineered a closed-loop runtime monitor for active data exfiltration detection and cross-process taint tracking.
- **Implementation:** Implemented synchronous interception via `ptrace`, featuring semantic mapping of arguments and watchdog persistence against SIGKILL; now migrating to zero-overhead **eBPF LSM**.
- **Adversarial Defense:** Mapped detection logic to MITRE ATT&CK (T1562.001), validating resilience against ransomware encryption patterns.

Hyperion XDP (TELOS Edge) Nov 2025 – Present
Lead Developer (High-Performance Network Security) github.com/nevinshine/hyperion-xdp

- **Role in TELOS:** Network-level containment engine blocking malicious traffic at the NIC before it reaches the OS stack.
- **Architecture (M4.6):** Designed a high-speed packet inspection engine using **eBPF/XDP** for $O(1)$ rejection of Layer 7 payloads.
- **Control Plane:** Implemented dynamic policy maps (`BPF_MAP_TYPE_ARRAY`) with a Go-based controller for real-time rule updates.
- **Telemetry:** Built lock-free alert pipelines using BPF ring buffers to stream threats to userspace without packet loss.

Mindscape BCI 2025
Lead Researcher (Academic Project) – Awarded Best Project, Mastermind 2025

- Developed an EEG→IoT pipeline achieving 87% accuracy in real-time signal classification.
- Demonstrated hardware–software integration for assistive technology control interfaces.

EDUCATION

Bachelor of Technology in Computer Science & Engineering Expected 2028
Amal Jyothi College of Engineering, India

- **Focus:** Operating Systems, Network Security, Data Structures, Kernel Development.

HONORS & ENGAGEMENT

- **Winner:** Mar Mathew Vattakkuzhy Award for Best Project (Mastermind 2025).
- **Challenge:** 100 Days of System Security (Documenting Kernel exploitation research).
- **Languages:** German (Native), English (Professional/Bilingual).