Kushagra Choudhary

linkedin.com/in/kushagrachoudhary · github.com/pinpwn · pinpwn@pwnprone.com
pwnprone.com · +91 9971633731

PROFILE

Cybersecurity engineer and product owner with 13 years of hands-on security practice, beginning with self-directed offensive research and evolving into designing and shipping enterprise-grade detection systems at scale. Over 8 years as a core engineering member at a cybersecurity startup, I have worked across the full technical spectrum: from kernel-level systems programming to distributed data architecture, and from automated threat-hunting pipelines to an AI-driven correlation engine stitching alerts into complete attack-cycle narratives. A results-oriented leader with a proven track record of driving measurable performance gains and representing organizational interests in national policy and commercial forums.

EXPERIENCE

AttackFence TechLabs **Gurugram, HR**

Principal Engineer & Product Lead *Apr 2022 – Present*

- Architected an incident correlation engine using **graph-based threat detection leveraging Markov models**, tightly mapped to MITRE ATT&CK, stitching alerts across third-party EDR, NDR, and SIEM into complete attack-cycle narratives with actor attribution and next-step TTP prediction.
- **Architect and product owner** of an **OT security** threat detection platform built on MITRE ATT&CK for ICS and MITRE D3FEND, defining architecture, research roadmap, and GTM for an emerging segment.
- Owned the full product lifecycle: **vision, sprint planning, team hiring, and daily execution**, reporting directly to the CTO and **managing stakeholder alignment** at the executive level.
- Contributed to AttackFence **NDR** development; Led IR engagements for Fortune 500 and publicly listed entities and **supported commercial outcomes** through presales and solution architecture; **speaker at national and international cybersecurity conferences**; consulted in state-level policy dialogues.

Senior Software Development Engineer *Jul 2021 – Apr 2022*

- Led development of a proprietary **agentless endpoint threat detection platform** built for high-throughput environments with minimal performance overhead and footprint.
- Drove a company-wide database modernization: evaluated Cassandra, MongoDB, CouchDB, and Parquet against production requirements; outcome: **87% reduction in storage, 300% improvement in search latency.**
- Deployed an internal Threat Intelligence platform, selecting and **customising open-source tooling** to consolidate external feeds into actionable detection intelligence.

ACPL Systems Pvt. Ltd. **Gurugram, HR**

Software Development Engineer *Jul 2019 – Jul 2021*

- Reduced **MTTD from 30 to 12 minutes (60%)** via automated agentless threat hunting in Windows environments and GPO-driven telemetry pipelines across Active Directory.
- Migrated stack from MySQL to Apache Cassandra, achieving a **42% query performance gain** and **32% execution speed improvement**.

Consultant - Cybersecurity Software Engineer *Jun 2018 – Jul 2019*

- Built a unified integration layer across NGFW, IPS, SIEM, and load balancers (Palo Alto, Check Point, McAfee, F5); automated threat response policies, **improving team productivity by 60%**.
- Mentored new engineers in **VAPT and Red Teaming**, accelerating onboarding and raising team capability.
- Built a host-based **firewall for Linux kernel v2.6.32.69** as a Loadable Kernel Module (LKM), working directly with the sk_buff network stack.

· AttackFence TechLabs operates as the product R&D sister concern of ACPL Systems.

RESEARCH & PROJECTS

AttackAxis (github.com/pinpwn/attackaxis)

- An adversarial simulation engine based on MITRE ATT&CK that generates realistic security telemetry for SOC training and detection validation.

JetFolio (github.com/pinpwn/jetfolio)

- An LLM-powered stock portfolio manager that tracks personalized investment themes and dynamic risk exposure relative to prevalent global conditions.

SKILLS

Languages: Python · C/C++ · Assembly · PowerShell · Bash
Threat Detection: MITRE ATT&CK · D3FEND · ATT&CK for ICS · Behavioral & Anomaly Detection · Heuristic Detection · YARA · Sigma Rules · Detection Engineering · Threat Modelling · STIX/TAXII · Threat Intelligence · Incident Response · IEC 62443
Security Tools: Wazuh · OSSEC · Suricata · Sysmon · Kali Suite · Windows AD/GPO · ICS/OT Protocols · SIEM · SOAR · EDR · NDR · XDR · LLM Security · VAPT
Architecture: Event-Driven Design · Microservice Architecture · Kernel/Userspace · REST API · gRPC · Graph Analytics · Zero Trust
Data & Streaming: Apache Kafka · Spark · Vector · MQTT · ZeroMQ
Storage: Apache Cassandra · Parquet · DuckDB · Memgraph · MongoDB
Platforms & Infra: Azure · AWS · Docker · GitHub Actions
Observability: Grafana · Kibana · Logstash · Elasticsearch · PowerBI · Superset

EDUCATION

SRM University **Sonepat, Haryana**
Bachelors in Computer Science *2019*

CERTIFICATES

Leadership skills **IIM Ahmedabad, 2024**
OSINT **Basel Institute on Governance, 2024**
Malware Analysis **IBM, 2024**