Siddharth Sharma

Security Engineer | Threat Hunting | Detection Engineering | Network Security | Cloud Security

siddharth.sharma.011235@gmail.com | +91 96672 34480 | Dehradun, India
www.linkedin.com/in/Siddharth–Sharma | github.com/ssiddharthssharma

Work Experience

Cyber Threat Hunter June 2025 – Now
CDOT (Centre for Development of Telematics), New Delhi, India

- Automated North–South traffic analysis across OpenSearch and firewall logs, processing millions of records weekly and reducing reporting time from 7 days to a few hours. Enriched IPs using CTI and AbuseIPDB with caching to minimize API overhead.
- Updated 50+ Sysmon and network-based detection rules mapped to MITRE ATT&CK, reducing false positives from 400K/day to ˜10K/day through severity normalization and behavior-based tuning.
- Conducted malware investigations on 3 high-risk binaries, uncovering 2 coordinated campaigns by correlating endpoint telemetry, firewall activity, and CTI data; generated IOC reports improving SOC triage accuracy.
- Delivered platform demonstrations to CRPF and IRCTC, training 20+ analysts and developing knowledge base content that accelerated onboarding and platform adoption.
- Built automated health-check routines for 7 production data pipelines, identifying ingestion failures and dashboard degradations early to maintain SOC reporting accuracy.
- Produced 9 weekly intelligence and SOC activity reports used by 3 cross-functional teams, improving prioritization and decision-making for internal and law enforcement stakeholders.

Professional Development Jan 2024 – May 2025
India

- Completed AWS Security–Specialty and Google Cybersecurity Professional certifications with emphasis on cloud security, IAM, threat detection, and incident response.
- Achieved Top 10% ranking on TryHackMe through hands-on labs in exploitation, privilege escalation, and adversary emulation.
- Built an on-prem Active Directory security lab to practice lateral movement, escalation paths, and Blue Team detection strategies.
- Pursuing OWASP certification to strengthen capabilities in web application security and vulnerability assessment.

Security Engineer Jan 2023 – Dec 2023
Flow Traders, New York

- Led redesign of the NY office network, deploying perimeter firewalls, relocating DMZ assets, and implementing segmentation aligned with industry standards.
- Deployed Vyos firewalling to isolate GCP and on-prem workloads; performed threat hunting using Darktrace with tuned anomaly-detection sensors.
- Served as primary on-call for NY security, collaborating with EMEA/APAC teams and improving incident response efficiency by updating Palo Alto SOAR playbooks.
- Onboarded Akeyless for secure machine identity and secrets management, enabling traders to access sensitive systems using short-lived tokens.
- Conducted tabletop breach simulations addressing device compromise, PCI/PII exposure, and crypto key leakage; delivered mitigation plans improving organizational resilience.
- Led security implementation for the new Chicago office, deploying Axis cameras, Morpho biometric readers, Galaxy alarm modules, and motion/vibration sensors.
- Tuned Tenable scanning configurations for low-latency environments, improving network performance stability.
- Strengthened Proofpoint filtering rules against emerging email threats and delivered KnowBe4 phishing simulations to improve user awareness.

Security Engineer March 2020 – Oct 2022
Nordstrom, Seattle, WA

- Managed and optimized 700+ firewalls across Palo Alto, Cisco, and Checkpoint platforms, ensuring consistent network security across enterprise and retail locations.
- Automated cloud provisioning using Terraform and implemented configuration standardization via Ansible.
- Modernized remote access by enforcing HIP checks in GlobalProtect for BYOD contractor fleets.
- Migrated store WAN from Meraki to Versa SD-WAN, enhancing PCI/PII protection and increasing bandwidth efficiency by 50%.
- Reduced VPN load by publishing applications on Zscaler, improving bandwidth utilization by 50%.
- Decreased latency on Nordstrom.com and NordstromRack.com by 10% through CDN optimization and routing refinements.
- Improved SEO performance by reducing 404/5xx errors, eliminating redirect chains, and optimizing CDN status-code handling.
- Mitigated bot traffic by onboarding endpoints to Shape and refining Fastly VCL logic.
- Automated data protection workflows with Avamar REST APIs and developed a custom network backup solution using StackStorm to replace SolarWinds.

Information Security Analyst Intern Sept 2019 – Dec 2019
GoPro, San Mateo, CA

- Monitored Palo Alto firewalls, IDS, SentinelOne, and Splunk telemetry for continuous threat detection and rapid triage.
- Conducted threat hunting and assisted with multi-team incident investigations, strengthening response workflows.
- Automated Splunk alerts and deployed honeypot sensors integrated with Splunk for attacker behavior analysis.

Security Engineer Intern May 2019 – Aug 2019
Electronic Arts, Austin, TX

- Performed penetration testing on EA game clients, identifying vulnerabilities and recommending security improvements.
- Developed a custom proxy tool to decode proprietary protocols, exposing previously unseen attack vectors.
- Documented findings in Confluence and GitLab and presented work at the CTO Intern Tech Fair.

Research Assistant Jan 2016 – Dec 2017
PEC University of Technology, Chandigarh

- Managed the Wireless Design and Communication Lab, supporting research and network infrastructure needs.
- Built GNS3 labs for CSN210, improving hands-on learning in computer networking coursework.
- Conducted WSN research for greenhouse monitoring and developed a CAN firewall prototype for embedded security.

Education

M.S., Electrical Engineering, San Jose State University Jan 2018 – Dec 2019
GPA: 3.4
Courses: Network Security, Network Programming, Machine Learning, Neural Networks

B.Tech, Electrical Engineering, Guru Nanak Dev University Sep 2011 – Jun 2015
Courses: Computer Networks, Data Structures, Algorithms

Skills

Threat Hunting & Detection: Splunk, Suricata, Zeek, Sigma, YARA, Cortex SOAR
Security Engineering: Palo Alto, Checkpoint, Cisco ASA, Zscaler ZIA/ZPA, F5, Fastly, Akamai
Cloud & Infra: AWS (IAM, VPC, Security Hub), GCP, Terraform, Docker, Kubernetes
Programming & Automation: Python, Bash, Regex, YAML, JSON
Network Security: TCP/IP, DNS, HTTP, VPN (GP/AnyConnect), SD-WAN (Versa/Meraki)
Pen Testing: Burp Suite, Metasploit, Nmap, Nessus, ZAP
Tools: Git, Jira, ServiceNow, GNS3, Wireshark

Projects

Secure Social Networking System (Python, AES-GCM, TCP Sockets)

- Built an encrypted messaging system using Python, Flask, TCP sockets, and AES-256-GCM.
- Implemented multi-threaded messaging (direct/broadcast), secure key distribution, and authenticated framing.
- Designed a message broker for routing, concurrency management, and persistent SQLite logging.

Hybrid Firewall (Kernel Module, NFQUEUE, Generic Netlink)

- Developed a hybrid firewall combining an LKM fast-path engine with a Python-based inspection layer.
- Implemented Netfilter hooks, dynamic rule tables, and SYN-flood/behavioral threat logic.
- Built a Generic Netlink interface enabling real-time rule updates for adaptive mitigation.

Cloud Honeypot Telemetry & Detection Rule Generation System (GCP, Cowrie, Cloud Run, Python)

- Designed a low-cost cloud honeypot architecture using a GCP f1-micro VM (Cowrie) and Cloud Run HTTP traps to capture real attacker traffic at ˜$0/month.
- Centralized and normalized honeypot telemetry in Cloud Logging and BigQuery, enriching events with GeoIP, ASN, AbuseIPDB scoring, and MITRE ATT&CK mappings.
- Built a Python pipeline to extract attacker behavior patterns and automatically generate Suricata, Sigma, and YARA detection rules, validating signatures against benign datasets.
- Implemented automated IOC and rule export workflows producing SOC-ready detection artifacts and a version-controlled rule repository via CI pipelines.