Sunny Dilipkumar Shah

San Jose, California, United States sunnydilipkumar.shah@gmail.com +1(669)-2939156 in/sunnydilipkumarshah sunnyshah.tech/

Summary

Most alerts are noise. I find the ones that aren't. Across SOC and detection engineering, I've triaged 150–200 alerts daily and built detections at scale for 4B+ users at Meta, cutting false positives by 60%. Now I build AI-powered systems that don't just flag threats but reason about them, triage autonomously, and get sharper over time.

Experience

Meta Menlo Park, CA

Security Engineer Intern *May 2025 - August 2025*

- Deployed SQL-based detections across billion-row datasets using TTP-based threat modeling, cutting false positives by 60% and compute costs by 95%.
- Engineered scalable SOAR automation workflows, reducing alert triage time by 40% and MTTR by 25%, enabling faster IR at platform scale.
- Closed detection gaps in data exfiltration and data misuse by engineering correlation logic that strengthened defense-in-depth controls across Meta's 4B+ user surface.
- Partnered with IR teams on high-fidelity alert investigations; authored standardized incident response playbooks that streamlined SOC triage workflows.

Demmisto Technologies Ahmedabad, India

Cyber Security Analyst *January 2024 - May 2024*

- Owned end-to-end investigation workflows for 150–200 daily alerts, triaging, escalating, and tracking incidents through resolution, cutting response time by 30%.
- Engineered high-fidelity SIEM correlation rules using SPL and KQL, reducing false positives by 25% and accelerating alert triage velocity.
- Led organization-wide phishing simulations to surface exposure gaps and harden email security controls.
- Applied MITRE ATT&CK and D3FEND frameworks to standardize incident classification and reporting, maintaining 95%+ SLA compliance.

Aditech Infotech Ahmedabad, India

Security Engineer *August 2022 - December 2023*

- Triaged 40–60 daily alerts across 500+ endpoints using Splunk and Suricata, detecting phishing, lateral movement, and unauthorized access attempts.
- Reduced false positives by 35% through systematic detection tuning, correlation rule refinement, and IDS/IPS optimization.
- Conducted host, network, and cloud forensics and root cause analysis on incidents; tracked and prioritized remediation to achieve a 25% MTTR reduction.
- Executed containment actions via firewall policy updates and access control changes, reducing breach dwell time.

Project

Agentic AI Threat Correlation Engine

- Built an agentic AI pipeline for automated threat correlation, cutting incident response time by 40% and boosting detection accuracy.
- Integrated LLMs for real-time alert summarization, delivering concise, actionable triage insights directly to analysts.
- Achieved 90% false positive reduction via behavior-based analytics and optimized SIEM/SOAR rule logic.
- Developed a Python-based threat intelligence enrichment engine, aggregating multi-source IOC data for deeper contextual reporting.

Education

M.S., Computer Engineering San Jose, CA

San Jose State University *May 2026*

B.E., Computer Engineering Ahmedabad, India

Gujarat Technological University *May 2024*

Certifications

CompTIA Security+, GCIH

Skills

Languages: Python, PowerShell, SQL, Bash, Regex

IR & SecOps: Incident Response Lifecycle, Threat Investigation, Proactive Threat Hunting, Behavioural Analysis, Insider Threat Detection, Phishing Simulation, Vulnerability Management, Playbook Automation

Frameworks: MITRE ATT&CK, D3FEND, NIST, OWASP, Threat Intelligence

SIEM / EDR / Tools: Splunk, Microsoft Sentinel, CrowdStrike Falcon, SentinelOne, Wiz (CSPM), FortiGate, FortiAnalyzer, Suricata IDS/IPS, Wireshark, MISP, Tenable, Qualys, OSINT, Sandbox

Cloud & Networking: AWS (CloudTrail, VPC Flow Logs, Core Services), TCP/IP, Network Forensics, Log Analysis (AV, IPS, DLP, Anti-Spam)

AI & Automation: Large Language Models (LLMs), Generative AI for SecOps, Agentic AI Pipelines, SOAR Automation, Splunk Dashboards, PostgreSQL