KISHOREKUMAR BATHINI SANKARAN

Fresno, CA 559-360-9718 hksankaran@gmail.com linkedin/kishorekumarbs/ Portfolio Website

SECURITY ENGINEER

SUMMARY

- Experience in **Detection Engineering**, analyzing **host, network, and cloud logs** to build high-fidelity detection rules aligned with **attacker TTPs** (**MITRE ATT&CK Framework**).
- Proficient with security tools and platforms including **SIEM** (Wazuh, ELK), **IDS/IPS** (**Suricata**), **Network Analysis** (**Wireshark**), **Endpoint Monitoring** (Osquery), and **Vulnerability Assessment** tools (**Burp Suite**).
- Skilled in **Python** scripting for **security automation**, developing **SOAR** playbooks (conceptual), building **logging pipelines**, and integrating security tools via APIs.
- Hands-on experience performing **TTP-based Threat Modeling**, **Incident Response** simulations, and security reviews across diverse environments including **Linux**, **Windows**, and **AWS Cloud**.

SKILLS

Security Operations & Engineering: SIEM (Wazuh, ELK, Splunk), Log Analysis (Host/Network/Cloud), TTP Detection.
Security Tools: Kali, Burp Suite, OWASP ZAP, Wireshark, Nmap, Metasploit, ModSecurity, Suricata, Snort, Zeek.
Threat Modeling & Vuln Mgmt: MITRE ATT&CK Framework, Adversary Emulation, Vuln Assessment, Threat Hunting.
Application & Web Security: OWASP Top 10, Web App Pentesting, API Security Concepts, SAST/DAST Principles, WAF.
Development & Automation: Python, PowerShell, Bash, YAML, SOAR Playbooks, Sigma Rules, YARA, Secure Coding.
Infrastructure & Cloud Security: Windows/Linux Security, TCP/IP, Cloud (AWS/Azure Security), Endpoint Sec.
Languages: Java, Python, SQL, C++, JavaScript, GO, PHP

WORK EXPERIENCE

Security Analyst | *Employer's Outsourcing, Fresno, California* **Feb 2025 – Mar 2025**

- Designed and implemented **TTP-based detection rules** aligned with MITRE ATT&CK framework, reducing false positives by **68%** while increasing true positive detection rates by **41%** across production and corporate environments.
- Engineered automated response workflows for **high-volume alerts**, implementing custom SOAR playbooks that resolved **87%** of false positives without human intervention and provided rich context for remaining alerts.
- Built custom **logging pipelines** for critical applications, normalizing heterogeneous data sources to enable threat identification across **15TB** of daily logs with reduced latency from 45 minutes to **under 3 minutes**.

Penetration Testing Intern & Security Instructor | *California State University, Fresno* **Sep 2024 – Nov 2024**

- Led **threat hunting operations** using SIEM tools to proactively search for indicators of compromise, developing **17 new detection rules** that identified previously undetected lateral movement attempts.
- Implemented a comprehensive **Network Detection and Response (NDR)** system using **Suricata** and **Zeek**, creating custom rules that identified **C2 traffic** and reduced malicious network activity by **76%**.
- Performed **attack testing automation** to validate detection coverage, simulating common adversary TTPs to measure detection efficacy and identifying blind spots in existing security controls.
- Enhanced **endpoint visibility** by optimizing EDR configurations and building robust log collection mechanisms, increasing the detection window for advanced persistent threats from 24 hours to **45 days**.

Security Research Assistant | *California State University, Fresno* **Nov 2022 - Dec 2023**

- Analyzed **operating system internals** (**Windows, Linux**) focusing on **memory structures** and **file system interactions** to understand malware persistence and evasion techniques.
- Utilized **user-mode debugging tools** (GDB, WinDbg) to perform basic **reverse engineering** on executable samples, identifying key functionalities and potential vulnerabilities.
- Investigated common **exploitation techniques** (e.g., buffer overflows, ROP basics) by analyzing proof-of-concept code and recreating scenarios in controlled lab environments.
- Researched **kernel-mode security mechanisms** and potential bypass techniques across different OS platforms, contributing to studies on rootkit detection methodologies.

Software Engineer Intern | *Cognizant Technology Solutions, Chennai, India* **Feb 2022 – Jul 2022**

- Implemented comprehensive **security logging** throughout enterprise applications using **ELK Stack**, increasing visibility into authentication events and data access patterns for 7,000+ user accounts.
- Developed **automated vulnerability scanning** pipelines integrated with CI/CD workflows, identifying and remediating **43 critical** security issues before production deployment.
- Created **threat model documentation** for key applications, mapping potential attack vectors and implementing appropriate detection controls at critical junctures in application workflows.
- Engineered custom **Python scripts** to analyze network traffic patterns and identify anomalous behavior, reducing false positive alerts by **47%** while maintaining detection efficacy.

EDUCATION

California State University, Fresno **Dec 2024**
Master of Science - Computer Science *Fresno, California, USA*

Anna University **May 2022**
Bachelor's of Engineering - Computer Science and Engineering *Chennai, TamilNadu, India*

PROJECTS

Threat Detection & Response Platform | *Advanced Security Implementation* **Mar 2025**

- Architected a comprehensive **threat detection system** using **Wazuh SIEM** and **ELK Stack**, implementing correlation rules for detecting multi-stage attacks across network and endpoint telemetry.
- Developed **custom Sigma rules** for detecting emerging threats, successfully identifying **living-off-the-land techniques** and **fileless malware** with minimal false positives.
- Created **automated response workflows** using Python and SOAR integration, reducing incident response time from hours to **minutes** for common attack patterns and providing rich context for analyst investigation.

Advanced Network Threat Analysis Framework | *Security Research Project* **Feb 2025**

- Built a comprehensive **network security monitoring** solution combining **Suricata IDS/IPS** with **Zeek** network security monitor to provide deep visibility into network traffic patterns.
- Implemented **machine learning algorithms** to detect anomalous network behavior, identifying previously unknown C2 communications with **93%** accuracy while maintaining a false positive rate below **0.5%.**
- Developed a **threat intelligence integration** framework that automatically consumed IOCs from multiple sources and generated appropriate detection rules for **Suricata** and **SIEM** platforms.

Scalable Threat Detection Pipeline | *Python, ELK Stack, Suricata, Osquery, AWS CloudTrail* **Dec 2024**

- Engineered a **log aggregation and analysis pipeline** using Logstash to parse and normalize events from diverse sources: **Suricata** (**network traffic**), **Osquery** (**host endpoints - Linux/Windows**), and **AWS CloudTrail**.
- Developed **custom detection rules** in Elasticsearch Query DSL and Kibana, aligning with **MITRE ATT&CK TTPs** such as Persistence (T1547) and Credential Access (T1110) for improved threat visibility.
- Created Kibana dashboards for real-time monitoring, alert triage, and visualizing attack patterns across correlated **host** and **network event data**, simulating analysis on **large datasets**.
- Leveraged **Python** scripting to automate the periodic ingestion of custom threat intelligence feeds (IoCs) into Elasticsearch, enhancing detection rule context.
- Designed the pipeline with scalability in mind, utilizing Elasticsearch indexing strategies and Logstash filtering to handle anticipated increases in log volume efficiently.

Automated Incident Response Playbook for Phishing | *Python, VirusTotal API* **Aug 2024**

- Developed a proof-of-concept **Security Orchestration, Automation, and Response (SOAR)** playbook using **Python** to automate the triage and initial response to reported phishing emails.
- Implemented automated extraction of indicators (URLs, IPs, file hashes, sender domains) from email headers and body using regular expressions and parsing libraries.
- Integrated external threat intelligence via **VirusTotal API** using **Python** to automatically enrich extracted indicators with reputation data, reducing manual lookup time by an estimated 90%.
- Designed conditional logic within the playbook to categorize alerts based on enrichment results (e.g., known malicious, suspicious, benign) and trigger subsequent actions like simulated endpoint isolation or user notification.
- Documented the workflow, including decision points and potential integration points with **SIEM** systems, demonstrating an understanding of building complex automations for incident response.

Wireshark Traffic Analysis | *Cyber Security Exercise* **Feb 2024**

- Utilized Wireshark for comprehensive in-depth analysis of network traffic, meticulously dissecting protocols including **SSH, Telnet**, and **HTTP.**
- Collaborated on developing and implementing incident response strategies, ensuring swift resolution of security incidents while minimizing operational impact.
- Detected and successfully mitigated various security threats including malware activity and unauthorized access attempts, substantially enhancing overall system defense.