Abhijeet Pawar

(312) 678 - 8671 | abhidotsh@gmail.com | LinkedIn | Portfolio

SUMMARY

Proactive Cybersecurity Analyst with 3+ years of experience in **Security Operations, Threat Detection, and Incident Response** across diverse **cloud and enterprise environments**. Proven ability to triage and resolve **security incidents**, significantly enhancing defenses through expert utilization of **SIEM/SOAR platforms** (Splunk, Panther, SentinelOne)**, WAF, IDS/IPS, and DLP**. Adept at building **high-fidelity detection rules,** developing **AI-driven security solutions**, leading critical threat hunts that uncovered previously unknown threat vectors, and **automating workflows** to reduce response times and elevate overall security posture.

TECHNICAL SKILLS

Tools: Splunk, SentinelOne, Microsoft Defender EDR, Snort (IDS/IPS), Burp Suite, Tines (SOAR), Nessus, Google Admin Console, Panther SIEM, Snowflake, OWASP ZAP, Wireshark, Metasploit, Nmap, Cloudflare (WAF)
Systems and Platforms: Windows, Mac, Linux, Microsoft Office, Git, Jira, Docker, AWS, Azure, GCP
Security Frameworks: ISO 27001, NIST Framework, MITRE ATT&CK Framework, CIS Critical Security Control
Programming Languages: Python, C++, Bash, SQL, PowerShell

WORK EXPERIENCE

Security Detection and Response Engineer Intern | *Circle Internet Group – USA* MAY 2024 – DEC 2024

- Investigated **350+ security incidents** (phishing, cloud anomalies, endpoint intrusions) as on-call lead, leveraging **Panther SIEM** and **SentinelOne EDR** to identify root causes, coordinate containment, and deliver incident reports.
- Triaged and remediated **AWS cloud security** misconfigurations and anomalies including EC2 instances communicating with malicious IPs, publicly exposed S3 buckets and implemented **CloudTrail anomaly alerts.**
- Authored **25+** advanced **detection rules** for critical threats (e.g., OnePassword login anomalies, Okta admin misuse, Cloud anomalies), uncovering 8 previously unknown threat vectors and **reducing false positives by 10%**.
- Led proactive **threat-hunting** for the Polyfill **supply chain** attack, identifying **30 vulnerabilities** across 10 repositories and driving remediation efforts that averted a potential compromise.
- Secured **1,550+ Google OAuth** apps and **Chrome extensions**, blocking **80+** unauthorized **apps** and reducing the attack surface by 5% via a security approval process. Built a **risk rating** tool to automate reviews, saving **$50K** by avoiding **third-party** spend.
- Developed a Python-based "**Sigma Converter**" to automate **100+** Sigma rule conversions for Panther **SIEM**, slashing **deployment time by 50%** and expanding threat detection coverage by 15%.

Cyber Security Analyst | *Atos* JULY 2021 – JUNE 2023

- Triaged and **analyzed 25+ security alerts daily** (Splunk, Microsoft Defender, Snort) in a **24/7 SOC environment**, reducing mean time to detection (MTTD**) by 35%** and protecting **950+** endpoints across enterprise systems.
- Assisted on full-lifecycle **incident response** for **major security incidents**, collaborating with **DevOps and IT teams** to remediate lateral movement, cloud misconfigurations, and insider threats.
- Configured and tuned **Cloudflare Web Application Firewall (WAF)** rules to block **80+ malicious domains**, enhancing web layer protection and reducing inbound threat traffic by 15%.
- Created and standardized **20+ incident response** playbooks in collaboration with multiple teams, covering scenarios like **phishing**, **malware**, unauthorized access, and data exfiltration, reducing average incident resolution time up to 45%.
- Developed and implemented **14+** automated security **workflows using** Python scripts and Tines SOAR for alert triage and data enrichment, eliminating **40% of manual** escalations and accelerating overall incident response times by **30%**.
- Improved **detection** by building and tuning **30+ Splunk** correlation **rules** aligned with **MITRE ATT&CK**, expanding **TTP** coverage and exposing previously undetected malicious activity.
- Implemented a **KnowBe4** security awareness program for **900+ employees**, reducing **phishing** click rates by **35%** in six months and strengthening organizational **security posture**.

Cyber Security Analyst Intern | *SSP Technology* JAN 2020 – JUNE 2020

- Hardened **Active Directory (AD) security**, implementing **group policy** restrictions, enforcing **least privilege** access, and monitoring login anomalies, reducing unauthorized access risks by 40% and blocking **100+ unauthorized login attempts.**
- Investigated and mitigated security incidents, analyzing **Windows Event Logs, Sysmon telemetry, and SIEM alerts**, detecting 30+ suspicious activities, and reducing incident resolution time by 35%.

JavaScript Developer | *Confiable Solutions* JUNE 2020 – JUNE 2021

- Managed profitable client relationships by developing and maintaining websites and creating dashboards for risk scorecards for international clients using **HTML, CSS, and JavaScript.**

CERTIFICATIONS & COMPETITIONS

Certifications:

- CompTIA Security+
- AWS Certified Solutions Architect - Associate
- ISC2 Certified in Cybersecurity

Competitions:

- 2nd place - NCAE Cybergames 2024, 2025
- Top 10% - TCM Security CTF
- Top 10% - National Cyber League 2023, 2024

EDUCATION

Master of Applied Science, Cyber Forensic and Security

Illinois Institute of Technology, Chicago, IL MAY 2025

Bachelor of Engineering, Information Technology

University of Pune, India OCT 2020

PROJECTS

Mistral-Driven SIEM Rule Generator: AI-Powered Threat Detection (Github)

- Built an **AI tool** using a fine-tuned **Mistral** model to generate detection rules from natural language prompts (e.g., “detect abnormal Okta logins”) and convert them to structured Sigma-style YAML.
- Translated **100+ rules** into platform-specific detection logic for **Splunk (SPL), SentinelOne, Panther SIEM, and Wazuh**, enabling plug-and-play deployment across varied SOC environments.
- Integrated **MITRE ATT&CK** mapping, **YAML** schema validation, and a **CLI** for batch conversion; improved detection engineering workflow speed **significantly** and reduced manual rule writing errors.

AI-Based Phishing Detection Tool

- Developed an **AI-based phishing detection tool** using machine learning to classify emails as phishing or legitimate based on content, subject lines, and sender information.
- Utilized Python and machine learning libraries like **Scikit-learn and NLTK** for natural language processing (NLP) to extract features from email data.
- Integrated **VirusTotal** for scanning email attachments for malware and used **Elastic** for detection of phishing-related threats.

Security Operations Center (SOC) Automation Lab

- Orchestrated a comprehensive **SOC** automation lab project, integrating **SIEM (Wazuh) and SOAR (Shuffle)** technologies to monitor and respond to security events such as Mimikatz detection.
- Configured Wazuh agent to detect and alert security events, ensuring the capture of critical telemetry with Sysmon integration.

Penetration Testing on a Box

- Performed password cracking using **John the Ripper and Hashcat** to gain access to the virtual machine and retrieve the system information with root privileges.
- Emulating real-world attacks, a pen test of the box utilized **Nmap and Metasploit** for network mapping and exploitation, identifying open ports, and fetching information.
- Executed **SQL injection** using sqlmap to retrieve database information, and version to determine the vulnerabilities which provided database details.

Active Directory Penetration Testing

- Established a virtual lab with a **domain controller and two user machines**, mirroring real-world network scenarios to assess to improve **logging, threat detection,** and reduce attack potential.
- Performed simulated cyber-attacks like **LLMNR poisoning, SMB relay,** keberoasting, AS-REP roasting **and pass-the-ticket** attacks to evaluate and improve security controls.

RESEARCH WORK

- Enhancing Cybersecurity through Effective Third-Party Risk Management and Supply Chain Security, **Illinois Tech**
- Design And Implementation of a Devs-Based Cyber-Attack Simulator for Cyber Security, **IJIRCC**