VAIBHAV KUNJIR

SECURITY RESEARCH ENGINEER

CONTACT

vaibhavskunjir@gmail.com

+91 86862 82890

Pune, Maharashtra, India

vaibhavkunjir.in

github.com/prismaticworks

Vaibhav Kunjir

SKILLS

- Security Tooling & Automation (Python, Java, TypeScript/React)
- Offensive Security Tooling (Nuclei, scanner development, automated vuln verification)
- Backend & Infrastructure (PostgreSQL, AWS, Docker, REST API development)
- Detection Engineering & Rule Tuning (SIEM/EDR, CI/CD deployment)
- Query Languages (AQL, KQL, SPL, YARA, PowerQuery)
- SIEM Platforms (Splunk, QRadar, Azure Sentinel, Google Chronicle, LogRhythm, Exabeam, Devo)
- EDR & Host Investigation (CrowdStrike Falcon, SentinelOne, Microsoft Defender, Cortex XDR, Carbon Black)
- Malware Analysis (PE/non-PE, Office macros, scripts; code injection, hooking, process hollowing)
- DFIR (Velociraptor, Redline, Mandiant IOC Editor, security log analysis)

CERTIFICATION

Cybersecurity Architect Expert (SC-100)
Microsoft · Issued Jul 2024
Credential ID: BBA40851F9C8D8B7

Security Operations Analyst Associate (SC-200)
Microsoft · Issued Jan 2024
Credential ID: 6BEDFC54D5D693EF

Microsoft 365 Security Administration (MS-500)
Microsoft
Credential ID: CC-1c6faeb6-cfc3-4a7f-8197-675613ecb42e

LANGUAGE

- English (Full professional proficiency)
- Hindi (Full professional proficiency)
- Marathi (Native)

PUBLICATION

Secrypt | Cloud Based Password Manager
International Journal of Scientific Research in Engineering & Management (IJSREM) · Mar 2023
End-to-end encrypted password manager built on AWS with Node.js, React.js, and MySQL, securing credentials with AES-256 and Bcrypt via an HTTPS-enabled RESTful API.

PROFILE

Security Research Engineer with nearly five years across offensive security tooling and threat detection. Currently building security scanners, platform integrations, and automation at NetSPI in Python, Java, and TypeScript/React. Previously a Threat Detection Developer and recognized Subject Matter Expert (SME) in QRadar and Azure Sentinel at ReliaQuest, developing detection rules through continuous R&D and deploying them via CI/CD pipelines. Earlier SOC background spanning malware analysis, email security, and digital forensics and incident response.

WORK EXPERIENCE

NetSPI | Pune

Security Research Engineer — JUN 2025 – PRESENT

- Design and develop security scanners and automation tooling in Python, Java, and TypeScript/React.
- Build and maintain platform integrations across backend APIs, databases, and UI for offensive security workflows.
- Improve scanner reliability, detection coverage, and operational visibility for security consultants.
- Automate vulnerability verification and template management, reducing manual review effort.
- Collaborate with engineering and security teams on tooling, research, and platform enhancements.

ReliaQuest | Pune

Cyber Security Specialist — FEB 2025 – JUN 2025

Threat Detection Developer — SEP 2023 – FEB 2025

- Developed and continuously improved threat detection rules through ongoing R&D, in direct collaboration with customers.
- Conducted in-depth threat analysis and presented findings and security-posture recommendations to clients.
- Worked with cross-functional teams to strengthen incident response procedures against emerging threats.
- Integrated current threat intelligence into detection coverage across QRadar, Splunk, Azure Sentinel, Chronicle, LogRhythm, Exabeam, and Devo.

SecurityHQ | Pune

Senior Analyst — JUN 2023 – SEP 2023

Cyber Security Analyst — APR 2022 – JUN 2023

Security Engineer — NOV 2021 – APR 2022

- Analyzed security events across QRadar and Azure Sentinel, delivering actionable mitigation guidance.
- Monitored and managed endpoints using Microsoft Defender, Carbon Black, Cortex XDR, and CrowdStrike.
- Performed malware analysis on PE, non-PE, PDF, Office macro, and script samples, examining API calls, code injection, hooking, and process hollowing.
- Handled phishing and spam analysis across O365 AIR, Mimecast, and Proofpoint, alongside O365, ATP, DLP, proxy, firewall, and IDS/IPS log review.
- Part of digital forensics and incident response engagements, including ransomware cases, through to remediation.

EDUCATION

Bachelor of Engineering – Computer Science

Anantrao Pawar College of Engineering & Research, Parvati | SPPU, Pune
CGPA: 8.54

AUG 2020 – MAY 2023

Diploma in Computer Science

Padmashri Dr. Vitthalrao Vikhe Patil College of Engineering, Ahmednagar | MSBTE
Grade: 98.47%

2017 – 2020

PROJECTS

Auto Verification Service
Service that drives the Nuclei scanner to re-verify each reported finding individually and record a verification result. Works against external targets as well as assets sitting behind VPN- or firewall-protected environments. Lets consultants confirm a finding is not a false positive, and lets customers retest a finding themselves once it has been patched.

Asset Inventory Scanner — NetSPI Hackathon
Web-based platform for real-time vulnerability assessment across IT infrastructure. Maps services from a PostgreSQL asset inventory to known CVEs using NIST NVD CPE data, with CVSS risk scoring, host-grouped dashboards, and CSV/JSON export.

List Management System
Python GUI application that centralizes management of SIEM reference sets, providing an interface to create, modify, and delete their data via the SIEM's API.