VIVEK KUMAR

Mumbai, Virar West | 9016944818 / 8882341597 | vivek.2040@gmail.com | LinkedIn Profile

Lead Cybersecurity Consultant | Government Cybersecurity Projects | SOC & Detection Engineering | Threat Intelligence | Malware Analysis | Digital Forensics | XDR/EDR | 15+ Years' Experience

PROFESSIONAL SUMMARY

Cybersecurity Leader with 15+ years of experience in government and enterprise cybersecurity, specializing in **Security Operations, Threat Detection, Malware Analysis, Digital & Log Forensics, Detection Engineering (EDR/XDR), Honeypot & Sandbox Development, Incident Response, Threat Intelligence, Dark Web Intelligence, MITRE ATT&CK Mapping, Security Architecture, and Stakeholder Management**.

DOMAIN EXPERTISE

Government Cybersecurity
Banking, Financial Services & Insurance (BFSI)
Telecom
Enterprise Security
Critical Infrastructure

CORE COMPETENCIES

Domain	Competencies
Cybersecurity Consulting	Government Cybersecurity Projects, Security Consulting
Security Operations	Security Operations Center (SOC), SIEM Deployment, Endpoint Security
Threat Detection	Detection Engineering (EDR/XDR), **Threat Hunting**, **Threat Intelligence**
Incident Response	Incident Response, Log Forensics, Root Cause Analysis
Malware Analysis & Forensics	Malware Analysis, **Security Architecture**
Research & Intelligence	Dark Web Monitoring
Security Engineering	Custom Honeypot Development, Custom Sandbox Development
Leadership & Management	Client & Stakeholder Management, Risk Assessment

CERTIFICATIONS

Organization	Certifications
Appin Technology Lab	Diploma in Cyber Security & Ethical Hacking (ACSE)
EC-Council	Ethical Hacking Essentials (EHE), Network Defense Essentials (NDE), Introduction to the Dark Web, SQL Injection Attacks, Cybersecurity for Businesses, Practical Introduction to Cloud Computing

TECHNICAL SKILLS & TOOLS

Category	Tools / Technologies
XDR / EDR/EPP	Quick Heal (*Seqrite*), Sequretek percept xdr/EDR
SIEM & Log Management	Sequretek SIEM, Syslog, Windows Event Logs
Malware Analysis	IDA Pro, Ghidra, x64dbg, PE Studio, Detect It Easy (DIE), Cuckoo Sandbox, ANY.RUN, Hybrid Analysis
Threat Intelligence	MITRE ATT&CK, YARA, Sigma, VirusTotal, MISP, OpenCTI
Log Forensics	Hayabusa , Logstash
Honeypot & Deception	Dionaea, Cowrie, MHN, T-Pot, Custom Honeypots
Programming & Scripting	Python, PowerShell, Bash, SQL
Operating Systems	Windows Server, Linux, Ubuntu, Kali Linux
Virtualization	VMware Workstation, Oracle VirtualBox, Docker
Offensive Security	Metasploit, GoPhish, KnowBe4, Custom Security Awareness Platform
Collaboration & DevOps	Git, GitHub, Jira, Confluence

KEY ACHIEVEMENTS

- Successfully led government cybersecurity projects from solution design through implementation, deployment, and operational handover.
- Designed, architected, and deployed an on-premises Security Operations Lab incorporating Malware Analysis, Digital Forensics, XDR, and EDR solutions.
- Developed and optimized 200+ EDR/XDR detection signatures mapped to the MITRE ATT&CK framework.
- Built enterprise honeypot and sandbox environments to improve threat visibility and malware analysis.
- Automated IoC collection and **Threat Intelligence** workflows, improving detection efficiency and reducing manual effort.
- Led a 15-member cybersecurity research team delivering malware research, **Threat Intelligence**, and detection engineering initiatives.

WORK EXPERIENCE

Quick Heal Technologies | Pune / Goa | Jun 2026 – Present

Lead – Consultant

Lead government cybersecurity consulting engagements involving Security Operations Center (*SOC*) implementation, Security Operations Lab design, incident response, enterprise cybersecurity solution deployment, and stakeholder management.

- Lead and deliver government cybersecurity projects from planning through implementation and successful client handover.
- Design, architect, and deploy complete on-premises Security Operations Labs including Malware Analysis, Digital Forensics, XDR, EDR, Threat Hunting, and supporting security infrastructure.
- Lead end-to-end implementation of cybersecurity solutions aligned with customer and government security requirements.
- Perform cybersecurity incident analysis, malware investigation, Threat Hunting, root cause analysis, and remediation during security incidents.
- Collaborate with government stakeholders, OEMs, and technical teams to ensure successful project execution and client satisfaction.
- Provide **technical guidance**, **client training**, and **knowledge transfer** on cybersecurity platforms and best practices.
- Strengthen organizational security posture through **Security Architecture reviews**, compliance alignment, and continuous improvement initiatives.

Sequretek Technologies Pvt. Ltd. | Mumbai | Aug 2016 – May 2026

Team Lead (Sep 2020 – May 2026)

- Led and managed a **15-member cybersecurity research team** specializing in malware analysis, deception technologies, sandbox automation, and **Dark Web Intelligence** operations.
- Architected and deployed **enterprise-grade honeypot and deception frameworks**, enhancing early threat visibility and reducing incident response time by **25%**.
- Directed proactive **Dark Web monitoring** and **Threat Intelligence investigations**, identifying credential leaks, phishing infrastructure, ransomware campaigns, and emerging cyber threats.
- Oversaw advanced **Threat Hunting, Log Forensics, and Incident Investigations**, detecting and neutralizing sophisticated threats before exploitation.
- Led **EDR/XDR detection engineering initiatives**, improving detection coverage and reducing false positives by **20%** through behavioral analytics and signature optimization.
- Designed and executed P**hishing Simulations, red-team exercises, and tabletop scenarios**, strengthening enterprise security posture and employee cyber awareness.
- Provided **executive-level threat briefings and strategic advisory reports**, enabling informed risk management and security governance decisions.
- Mentored and developed cybersecurity analysts, fostering technical excellence in malware research, forensic analysis, and detection engineering.
- Collaborated with SOC, DevSecOps, and infrastructure teams to enhance intelligence sharing, detection automation, and operational resilience.

Principal Malware Research Engineer (Aug 2016 – Aug 2020)

- Conducted advanced **static and dynamic malware analysis** on PE, non-PE, and ELF binaries to extract IoCs and understand attack techniques.
- Performed reverse engineering using disassemblers and debuggers to analyze payload behavior and persistence mechanisms.
- Designed and implemented **custom sandbox environments** to automate malware behavior analysis.
- Developed and tested PoC exploits and payload simulations in controlled lab environments.
- Created and fine-tuned **EDR detection signatures** and behavioral rules to improve malware detection accuracy.
- Conducted detailed log analysis, memory forensics, and network traffic inspection for **Incident Investigations**.
- Contributed to **Threat Intelligence** reports documenting emerging malware families and attack campaigns.
- Collaborated with SOC teams to validate detection use cases and improve alert triaging processes.

Private Cybersecurity Firm | Delhi

Information Security Analyst (Exploit Department; Government Projects) | Apr 2011 – Mar 2016

- Developed proof-of-concept (PoC) exploits and engineered portable executable (PE) payloads to effectively bypass antivirus and endpoint security solutions.
- Applied advanced anti-analysis and obfuscation techniques to significantly increase exploit resilience and evade detection.
- Utilized Kali Linux, Metasploit, and other industry-standard offensive security tools for rigorous exploit development, testing, and validation.
- Collaborated with cross-functional cybersecurity and engineering teams to verify exploit reliability and ensure secure deployment of PoCs.
- Documented detailed technical procedures and best practices to facilitate the safe and compliant delivery of offensive security findings to government clients.

EDUCATION

- **Master of Computer Applications (MCA)** | Sikkim Manipal University (Distance) | 2011 – 2013
- **ACSE (Appin Certified Security Expert)** — Diploma in Information Security & Ethical Hacking | Oct 2010 – Mar 2011 (6 months) | Grade: A
- **Bachelor of Computer Applications (BCA)** | Boston College, Gwalior | 2007 – 2010
- **DOEACC O Level Certification** | Bokaro Steel City | 2006 – 2007