YASH KANZARIYA

Surendranagar Gujarat - 363020 | yashkanzariya50@gmail.com | +91 95120 90484 | linkedin

SUMMARY

As a postgraduate student in Cybersecurity and Digital Forensics, I bring a well-rounded foundation in key cybersecurity domains with hands-on experience in Security Operations Center (SOC) environments, digital forensics, and cloud security. I am adept at monitoring and analyzing security events, managing incident response workflows, and conducting forensic investigations to trace and contain threats. My skill set includes log analysis, threat detection, and the application of security best practices across both on-premise and cloud infrastructures. With a strong understanding of access controls, firewall policies, and compliance frameworks, I am well-prepared to support and enhance organizational security posture in dynamic, technology-driven environments.

EDUCATION

MSc in Cybersecurity & Digital Forensics **2023-2025**

Rashtriya Raksha University, Gandhinagar

Bachelor of Computer Applications (BCA) **2020 - 2023**

C.U. Shah University Surendranagar

- CGPA: 8.77

PROFESSIONAL EXPERIENCE

Cyber Security Analyst **Jan 2025 - Present**

Infopercept Pvt Ltd, Ahemdabad

As a SOC Analyst at Infopercept, I monitor and investigate security events using the Invinsense SIEM platform to ensure timely detection and response to threats. I perform log analysis, threat hunting, and forensic triage across hybrid environments, leveraging tools such as TheHive for case management, cloud security services, Check Point and Sophos firewalls, Trend Micro EDR, Seqrite endpoint protection, and MISP for threat intelligence. Additionally, I assist in firewall policy management, endpoint security monitoring, and generate detailed reports to support continuous improvement of the organization's security posture.

SOC Level 1 Intern **May 2024 - july 2024**

Soebit Cyber Security, Netherlands

Gained foundational knowledge in SOC operations, including Splunk basics, networking fundamentals, and basic log analysis. Monitored and analyzed security alerts and potential threats using SIEM tools, classified incidents, and assisted in incident response following SOPs. Developed skills in documenting incidents, optimizing security tools, and escalating complex cases. Ensured compliance with security policies, stayed updated on cybersecurity trends, and supported security awareness initiatives.

Training Assistant and Red Team Member **April 2024**

NCIIPC SecEx, 2024, Delhi

Contributed to the design and delivery of cybersecurity training programs aimed at enhancing the skills and awareness of employees in critical infrastructure sectors. Played a pivotal role in crafting realistic and complex cyber threat scenarios to ensure practical relevance and effectiveness of training sessions. As a Red Team member, actively participated in a rigorous 3-day live-fire cyber exercise, executing advanced attack simulations targeting Windows servers, web servers, Active Directory, DMZ zones, routers, and firewalls. This exercise tested organizational defenses, uncovered vulnerabilities, and provided actionable insights to strengthen overall security posture.

Digital Forensic Intern **Febuary 2024 - March 2024**
Cyber Dosti

Performed forensic analysis of digital media to uncover and document evidence of cybercrime using specialized tools such as Redline, Autopsy, Plaso, FTK Imager, Volatility, Belkasoft, and RAM capture techniques. Applied file system forensics methods, including analysis of registry hives, LNK files, and memory forensics, to reconstruct user activity and system behavior. Ensured evidence integrity and chain of custody while assisting in detailed forensic reporting to support investigations and legal proceedings.

Java Developer - Intern **Jun 2023 to Oct 2023**
Tops Technologies, Ahmedabad

Worked as a backend developer focusing on building and enhancing server-side components using Java, Spring Boot, MVC, JSP, and Servlets. Played a key role in designing and implementing a complete e-commerce project, including features like product management, user authentication, and order processing. Collaborated with the team throughout the software development lifecycle, ensuring robust, scalable, and efficient backend services.

TOOLS AND TECHNICAL SKILLS

- Programming & Scripting: Proficient in C, C++, Java, Python, PHP, JavaScript and Shell scripting.
- Cybersecurity: Skilled with IDS/IPS, SIEM Systems, Malware Analysis, FTK Imager, Nmap, Autopsy, Wireshark, and Metasploit. Experienced in digital and mobile forensics, multimedia forensics, cloud forensics, Windows Internals, Active Directory Investigations
- Networking & Data Analysis: understanding of networking and protocoals, firewall configurations, log analysis, Network Assessment.
- Endpoint & Cloud Security: Hands-on experience with endpoint protection tools (Seqrite, Trend Micro EDR), cloud security services (AWS fundamentals), and security operations in hybrid environments.
- Software & Tools: Experienced with SQL databases (Oracle, MySQL, SQL Server), web technologies (HTML, JavaScript, PHP), and frameworks (CodeIgniter, Spring, Hibernate).
- Collaboration & Case Management: Proficient in using case management tools like TheHive and security incident response workflows

CERTIFICATIONS

- CEHv12 Certified
  - EC-Council
  - Certification Date: 7 October 2024
- Intern of 9th Batch of Gurugram Police Cyber Security Summer Internship (Online)
  - GPCSSI-2021
- CPIA (Certified Process Injection Analayst)
  - CWL (Cyber Warefare Labs)
- Certified Cyber Warrior
  - HackingFlix Academy
- CRT-COI (Red Team – CredOps Infiltrator)
  - CWL (Cyber Warefare Labs)
- Cybersecurity Essentials
  - Cisco Networking Academy
- RHCSA
  - Ongoing

ACADEMIC PROJECTS

Automated Threat Intelligence-Driven SOC Integration

Developed an automated Security Operations Center (SOC) framework by integrating open-source tools Wazuh (SIEM) and MISP (Threat Intelligence Platform). Enabled real-time threat detection, automated incident correlation, and enriched threat analysis, improving response efficiency and security visibility.