Sahil Borse

Computer Science Student Specializing in Cybersecurity and Threat Intelligence

linkedin.com/in/sahillborse | sahilllborse@gmail.com | 88281 12802 | Nashik, Maharashtra

SKILLS

- Security Tools: Wazuh, Velociraptor, OpenCTI, TheHive, Cortex, MISP
- Digital Forensics: Volatility 3, REMnux, Flare VM
- Log Analysis & Threat Detection: ELK Stack, Sysmon, Winlogbeat
- Network Security: pfSense, IDS/IPS

PROJECTS

Windows EDR Attack & Defense Simulation using LimaCharlie

GitHub: github.com/Nucl3arAt0m/EDR-Attack_and_Defense

Tools & Technologies: Limacharlie, Sysmon, VMware, Linux

Skills: Endpoint Detection & Response (EDR), SIEM, Threat Hunting, Adversary Simulation, Log Analysis

- Simulated cyber attacks using Sliver C2 framework to validate EDR functionality on a Windows 11 endpoint.
- Deploy LimaCharlie EDR to detect and react to sophisticated attacks such as credential dumping and memory analysis.
- Carried out credential access attacks such as LSASS memory dumps and NTLM hashes to test mitigation and detection capabilities.

Windows Endpoint Detection & Response (EDR) System using Wazuh

Tools & Technologies: Wazuh, Sysmon, Winlogbeat, Elasticsearch, Kibana, YARA, Sigma

Skills: Endpoint Detection & Response (EDR), SIEM, Log Analysis, Threat Hunting

- Installed Wazuh on Windows as an EDR tool to detect and scan security logs for real-time threat analysis.
- Configured Sysmon and Winlogbeat to log centrally, boosting endpoint visibility by 40%.
- Enhanced alerting and threat incident response procedures using Wazuh and Kibana, reducing response time by 30%.
- Conducted threat hunting and forensic analysis to determine attack patterns and minimize security threats.

Threat Intelligence Platform with OpenCTI & MISP

Tools & Technologies: OpenCTI, MISP, VirusTotal API, AbuseIPDB, Docker, MITRE ATT&CK

Skills: Threat Intelligence (CTI), IOC Analysis, Indicator Enrichment, Automation

- Built a Threat Intelligence Platform (TIP) based on OpenCTI and MISP to centralize and visualize cyber threat intelligence.
- Created an OpenCTI threat data dashboard in real-time, enhancing incident response efficiency by 30%.
- Effective threat intelligence procedures cut IOC analysis time by 25% by automating and integrating.

WORK EXPERIENCE

Front-end web developer Intern – May 2023 – July 2023

Oasis Infobyte, Remote

- Built responsive web applications using HTML5, CSS3, and JavaScript, achieving a 90% cross-browser compatibility rate.
- Developed reusable React.js components, reducing development time by 15% and improving code maintainability

EDUCATION

Vellore Institute of Technology, Amaravati, Andhra Pradesh

Bachelor's Degree in Computer Science 2021–2025

Pace Junior Science College, Mumbai

Higher Secondary Certification in Science 2018–2020

CERTIFICATIONS

Google Cybersecurity Professional Certification, 2024

TryHackMe SOC Level 1 Learning Path Certification, 2025