Lokesh Kumar

Boston, MA 617-708-5882 lokesh5671@gmail.com exzekai exzekai exzekai.com

Education

Northeastern University - Khoury College of Computer Sciences **Sep. 2021 – May 2023**
Master of Science in Cyber Security, GPA 3.625 *Boston, MA*

Odisha University of Technology and Research **Aug. 2012 – May 2016**
Bachelor of Technology in Computer Science and Engineering *Bhubaneswar, India*

Relevant Coursework

- Foundations of Information Assurance
- Network Security Practices
- Computer System Security
- Information System Forensics
- Security Risk Management
- Critical Infrastructure
- Governance, Risk and Compliance

Technical Skills

Languages: Python, SQL, Powershell, Bash
Technology: Docker, Terraform, GCP, AWS, Microsoft Azure, OWASP Top 10, NIST, MITRE ATT&CK, VMware, Microsoft 365 Defender, Virtual Box, Active Directory, IDS, IPS, Firewall, Kubernetes
Tools: Cortex XDR, Panorama NGFW, Zscaler Proxy, Proofpoint, Splunk, ELK, McAfee EPO, KnowBe4, Exabeam Data lake and Advanced Analytics, Anomali Threatstream, Alienvault, Wireshark, Burp Suite, RegRipper, Nmap, Metasploit, Hydra, Hashcat, John the ripper, FTK Imager, Autopsy , Cutter, Pfsense firewall, Snort IDS, Pestudio, x32/x64dbg, Caldera, Servicenow, Shodan, Spiderfoot, IDA
Certifications: CompTIA CySA+, CompTIA Security+, AWS Cloud Practitioner, Microsoft AZ-900
Operating System: Windows, Linux

Work Experience

Khoury College of Computer Science, Northeastern University **Jan. 2023 – Apr. 2023**
Graduate Teaching Assistant for Fundamentals of Cloud Computing, CS6620 *Boston, MA*

- Facilitated comprehensive understanding of AWS concepts and services, while providing doubt clearing sessions, grading assignments, troubleshooting lab issues for students.

Black Hills Energy **Jun. 2022 – Dec. 2022**
Cyber Security Intern *Rapid City, SD*

- Engaged in robust internal penetration testing, including detailed password audits and Active Directory Certificate Services (ADCS) checks.
- Identified, analyzed, and neutralized over 2000+ phishing emails, while crafting 12 intricate phishing templates for internal campaigns, leading to a 1.3% click-through rate.

Khoury College of Computer Science, Northeastern University **May 2022 – Jun. 2022**
Graduate Teaching Assistant for Fundamentals of Cloud Computing, CS6620 *Boston, MA*

- Expand on the different AWS concepts and services to students as well as conduct doubt clearing sessions and grade assignment and submissions, as well as troubleshoot lab issues.

Capgemini Engineering(formerly Altran) **Sept. 2020 – Aug. 2021**
Associate Engineer Operations *Gurugram, India*

- Managed comprehensive analysis and investigation of 5000+ events, while crafting global policies using Panorama and Cortex XDR, ensuring robust security posture as a Security Operations Analyst III.
- Accomplished a rigorous risk assessment,efficiently devising AppLocker security policies in just 2 months, half the expected timeline.
- Championed Threat Hunting with OSINT, MITRE ATT&CK and trend monitoring of malwares, resulting in improved documentation and enhancement of IR runbook.
- Optimized Splunk SIEM Enterprise Security use cases by analyzing hundreds of false positive events and providing recommendations to enhance the Splunk Security Dashboard.

Altran **Dec. 2019 – Sept. 2020**
Trainee *Gurugram, India*

- Coordinated incident response on 200+ malicious events using Palo Alto Traps EDR, isolating & terminating processes and endpoints, to maintain security posture.
- Advocated for advancements in the team's Incident Response Playbook by documenting thorough reports of incidents and remediation actions

Projects

Risk Assessment | *NIST* **Jan. 2023 - Apr. 2023**

- Performing risk assessment for Mobile Heartbeat's cloud deployment project.

Adversary Emulation | *Caldera, Ubuntu* **Mar. 2023**

- Conducted adversary emulation exercises on two systems utilizing Caldera, facilitating the analysis and understanding of attacker TTPs (Tactics, Techniques, and Procedures).

Malware Analysis Sandbox | *Virtual Box, SysInternals, x32/x64dbg, CAPA, PeStudio, Cutter* **Feb. 2023**

- Conducted detailed qualitative and quantitative examinations of malware specimens, successfully identifying indicators in dynamic & static analysis to classify threat level.