Utkarsh Prajapati

Phone: +918085009499
Email: Prajapatiutkarsh399@gmail.com
LinkedIn: linkedin.com/in/utkarsh-prajapati-70a9b611a/

PROFESSIONAL SUMMARY

Cybersecurity professional with 6+ years of experience in Endpoint Detection & Response (EDR), Threat Analysis, and Blue Team operations. Skilled in network security monitoring, forensic investigations, and SIEM platforms. Proven ability to analyze, detect, and mitigate cyber threats using CrowdStrike, Sentinel, QRadar, and forensic tools like FTK.

KEY SKILLS

- **Security Solutions:** Firewalls, IDS/IPS, Antivirus
- **Offensive & Defensive Techniques:** Brute Force, Phishing, DOS/DDOS, MITM, Sniffing, Spoofing
- **Endpoint Detection & Response (EDR):** CrowdStrike Falcon, Sentinel, Carbon Black
- **Threat Intelligence & SIEM:** QRadar, Microsoft Sentinel, Splunk
- **Incident Response:** Security Incident Management, Vulnerability Scanning, Patch Management
- **System Administration:** Windows Server (2008-2019), Active Directory, Server Hardening, Group Policy
- **Network Security & Monitoring:** Zeek, Suricata, Wireshark
- **Disaster Recovery:** Backup & Recovery Solutions, Business Continuity Planning
- **Forensics & Incident Response:** FTK, Autopsy
- **Penetration Testing:** Network, Web, Mobile Application Testing
- **Compliance & Regulatory:** Data Protection, Encryption, Security Audits, PCI-DSS, HIPAA

PROFESSIONAL EXPERIENCE

Cyber Security & IT Officer

Indore Cloth Market Co-Operative Bank
October 2024 – February 2025

- Implemented QRadar SIEM real-time security monitoring system to enhance early detection of security threats.
- Conducted threat analysis using EDR tools like CrowdStrike Falcon & Sentinel to detect advanced persistent threats (APT).
- Mitigate the third-party scanned report of Network, Web and Mobile application testing vulnerabilities.
- Investigated security incidents & forensic evidence using FTK and network monitoring tools.
- Developed custom detection rules for threat hunting and malware analysis.
- Ensured compliance with data protection laws and cybersecurity standards for sensitive customer data.
- Developed disaster recovery and business continuity plans to protect critical IT infrastructure.
- Generated detailed reports and audits for regulatory bodies and senior management.
- Worked closely with the Blue Team to enhance security posture and defend against cyber threats.

System Analyst I
Oracle Cerner
May 2021 – October 2024

- Monitored network traffic and endpoint behavior using SIEM & EDR solutions.
- Performed system integrity checks, performance tuning, OS upgrades, and RHEL/OL patching for Cerner solutions servers.
- Assisted in incident response & remediation strategies to contain security incidents.
- Developed and implemented monitoring systems for applications and servers, responding to alarms to prevent client impact.
- Developed threat-hunting playbooks using MITRE ATT&CK framework.
- Successfully upgraded systems to mitigate log4j vulnerabilities, enhancing security posture.
- Collaborate with SIEM & SOAR teams for critical clients.
- Mentored and trained junior staff, fostering knowledge transfer and team development.

Server Security Engineer
Rack Bank Data Centre Pvt. Ltd.
November 2018 – April 2021

- Configured and deployed Windows Server environments (2008-2019) and managed Active Directory and Group Policies.
- Conducted server migrations using Acronis Backup and ensured secure server operations.
- Implemented and managed firewall and Iptables for server security.
- Administered VMware ESXi, Proxmox, and Virtualizor for virtualization and server provisioning.
- Performed troubleshooting for Windows IIS and managed DNS services.
- Provided end-user support, resolving technical issues through support tickets.
- Managed server security policies and monitored server performance and health.

EDUCATION

Master of Computer Applications (MCA)
APJ Abdul Kalam University
Year of Graduation: [2021]

Bachelor of Science (B.Sc.)
Acropolis Institute of Management and Research
Year of Graduation: [2017]

CERTIFICATIONS

- Post Graduate Program in Cyber Security | **Great Lakes**
- Certified Ethical Hacker (CEH) | **EC-Council**
- Computer Hacking Forensic Investigator (CHFI) | **EC-Council**

ADDITIONAL INFORMATION

- **Languages:** [English, Hindi]
- **Interests:** [Ethical hacking, Networking, Cyber defense, Forensics]

TECHNOLOGIES & TOOLS

- **Networking:** TCP/IP, OSI Model, DNS, VPN, Routing & Switching
- **Security:** Firewalls, IDS/IPS, Nessus, Splunk, QRadar, Wireshark, VirusTotal
- **Operating Systems:** Windows Server (2008-2019), Linux (RHEL, OL)
- **Cloud & Virtualization:** VMware ESXi, Proxmox, Virtualizor
- **Others:** Nessus, Virustotal, MXToolbox, URLVoid, Ophcrack