RAVI BHADAURIA

Dublin, Ireland
0892419942
ravi.bhadauria1994@gmail.com

PROFESSIONAL SUMMARY

Cybersecurity professional with 6+ years of experience in leading Security Operations Centers (SOCs) and specializing in incident response, threat hunting, and log analysis. Skilled in leveraging SIEM platforms (IBM QRadar, Splunk, LogRhythm) and endpoint protection tools (CrowdStrike Falcon, Palo Alto Networks) to detect, analyze, and mitigate complex security incidents. Proven track record at Ernst & Young (EY) in leading cross-functional teams, integrating threat intelligence, and applying frameworks like MITRE ATT&CK to proactively identify and mitigate emerging risks. Expertise in SOAR, network security, cryptography, forensics, and malware analysis. Currently pursuing a Master's in Cybersecurity at the National College of Ireland to stay ahead of evolving threats and enhance technical capabilities.

WORK HISTORY

Cyber Security Consultant, 08/2021 – 01/2025
Ernst & Young (EY), Bangalore, India

- Successfully contained and mitigated 19 critical security incidents, preventing potential data breaches and minimizing organizational impact.
- Worked across multiple attack vectors, including phishing, ransomware, DDoS, insider threats, and web application attacks.
- Improved threat detection and reduced false positives through network flow analysis using LogRhythm and Splunk.
- Leveraged CrowdStrike Falcon to support vulnerability assessment programs and decrease vulnerability remediation time.

SKILLS

- Cybersecurity & SIEM Tools (IBM QRadar, Splunk, LogRhythm)
- Incident Response & Malware Analysis (Static Analysis, Forensics)
- Networking, Network Security, & IDS/IPS
- Advanced Threat Hunting & Log Analysis (Alert Monitoring, EDR tools like CrowdStrike Falcon)
- Cyber Kill Chain & MITRE ATT&CK Framework
- Vulnerability Scanning, Penetration Testing, & Risk Management
- Event Log Analysis across diverse devices and environments
- Scripting & Automation (Python, Bash)

- Spearheaded the integration of advanced threat intelligence tools, such as ThreatConnect and Anomaly, improving detection and prevention capabilities within the SOC.
- Led and coordinated cross-functional teams to respond to large-scale security incidents, improving collaboration and communication to drive faster threat mitigation.
- Mentored junior analysts on incident response, threat analysis, threat hunting, malware analysis, forensics, and security tool utilization.

Cyber Security Consultant, 12/2020 – 07/2021
Aujas Networks, New Delhi, India

- Successfully contained a malware outbreak by isolating endpoints with CrowdStrike and analyzing alerts with Darktrace. Performed initial forensic analysis.
- Played a key role in containing and neutralizing 6 major cyberattacks, protecting the organization's sensitive data and reducing overall risk.
- Focused on various attack vectors such as malware, SQL injection, advanced persistent threats (APTs), and credential stuffing, fortifying defenses against diverse cyberattack methods.
- Decreased high-risk vulnerabilities by 15% through vulnerability management and mitigated multiple attempted breaches.
- Strengthened perimeter security by proactively monitoring firewall logs and threat feeds, blocking malicious connections. Refined firewall rules.
- Uncovered and remediated two previously unknown vulnerabilities through proactive threat hunting using threat intelligence and MITRE ATT&CK.
- Mentored junior analysts on security tools, incident response, vulnerability management, and threat hunting.
- Maintained expertise in current threats and vulnerabilities, sharing knowledge and improving security awareness training.

SLK Global Solution, Pune, India

- Identified malicious files via static malware analysis of Office 365 logs and alerts using Azure Sentinel.
- Detected and reported suspicious log activity, providing clear reports and visualizations to clients.
- Improved detection and response by conducting threat intelligence research, threat hunting, and developing incident use cases.
- Automated security report generation in Azure Sentinel, providing clients with timely security insights.

Security Analyst, 01/2018 - 04/2019
SISA Information Security, Bangalore, India

- Mitigated multiple security incidents through alert monitoring, threat hunting, and incident response.
- Deployed and configured ELK-based SIEM for 30+ clients, integrating and managing logs from 500+ devices (firewalls, IDS/IPS, proxies, log servers, security tools), significantly improving threat detection.
- Performed regular log analysis, identifying and reporting vulnerabilities across diverse operating systems (Windows, Linux) and applications, enhancing security posture.

EDUCATION

MSc in Cybersecurity. **01/2025 – 01/2026**
Cyber Security (Forensic, Malware Analysis, Cloud Architectures and Security, AI/ML in Cybersecurity, Cryptography and Blockchain, Secure Web Development)
National College of Ireland – Dublin

Bachelor of Technology (B. Tech), Computational Science and Engineering**. 06/2015**
Uttar Pradesh Technical University - Lucknow

LANGUAGES

Hindi: Native language

English: Proficient