Saurabh Khadtare

Ballincollig, Cork, Ireland. | Mobile: +353 896029815 | https://www.saurabhkhadtare.com EmailTo: saurabhkhadtare0@gmail.com |
LinkedIn: https://www.linkedin.com/in/saurabhkhadtare

Summary:

Highly motivated and security-focused SOC Analyst with 3+ years of combined experience in security operations and penetration testing. Proficient in SIEM (Splunk), network security, incident response, and various security tools (Wireshark, NMAP, Metasploit). Proven ability to analyse security alerts, investigate incidents, and collaborate effectively with teams to resolve security issues. Eager to leverage experience and passion for cyber security to contribute to a secure IT environment. I've Excellent verbal and written communication skills, also actively involved with team collaboration or independently, providing guidance to teammates. I'm a quick learner and have fast understanding. I work at pace & goal oriented with a strong delivery focus attitude. I like to be a role model for best practice and actively promote it. As a person, I am curious and self-motivated.

Professional Experience:

Amazon

Physical Security Support Engineer II (Level 4)

Full-Time, Permanent | May 2021–June 2023 | Cork
In my role as a Physical Security Engineer at Amazon, I was responsible for:

- Managing and resolving critical security incidents, including site lockdowns, access provisioning, and troubleshooting server issues across multiple cloud Server workloads; to ensure uninterrupted operations and minimise downtime
- Resolving high **severity tickets** using SIM ticking portal, often addressing complex issues, Escalation appropriately & remediation while maintaining excellent communication with customers.
- Program physical access control and video systems to ensure compliance with company security standards & troubleshoot database with Bash, PowerShell.
- Managing Security integration group's Security events & active collaboration in global security team.
- Making sure all security operations are running smoothly under the umbrella of **Security Operations Center (SOC)**, including Access Control (**IAM**), **CCTV Surveillance**, **Visitor Management**, **Intrusion Detection & Prevention systems** (IDS/IPS) on large scale infrastructure.
- Amazon Phys Sec. Incident & event management (**SIEM**) with SumoLogic, Splunk.
- Investigate security issue & device failure issues with network scanning, system log analysis,
- I received the highest numbers of accolades in the team for best customer support & troubleshooting customer issues.
- work in an operational/shift-based environment with flexible working hours to include evenings and weekends.

Bugcrowd

Security Researcher / Pentester

Freelancing | September 2020 – Current
Location: Self-employed

- Independently discovered vulnerabilities on public and private bug bounty programs.
- **Utilised Security Tools / Software:** Wireshark, TCP Dump, Security Onion, Splunk, Kali Linux, Metasploit, NMAP, Nessus, Burp Suite.
- Network/host vulnerability analysis and penetration testing.
- Practising Linux fundamentals, & Linux kernel skills
- Scripting experience with Python, Bash, & PowerShell.
- Spend most time reading Technical documentation, and learning security best practices.

Paytm Payments Bank

IT Technical Support

April 2018 – August 2018
Location: Pune Area, India

- Increased customer satisfaction by 12% and resolved 80% of tickets within the SLA every month.
- Performed Troubleshooting customer issues with **Customer-centric** mindset.
- Received the best customer support award.
- Provided excellent customer IT-support through a variety of communication channels and provide better customer experience.

Skills:

- **Security Operations Center (SOC) Analyst:** SOC, security analysis, incident response, threat hunting, SIEM, log management, network security, endpoint security, IT security & management
- **Security Tools & Technologies:** Palo Alto Networks, Splunk, SumoLogic, Sentinel, Microsoft Defender (ATP, Sentinel, Defender for Identity), Windows Sysinternals, LOLBins, IDS/IPS, EDR, Cloud Security, Crowdstrike Falcon
- **Threat Analysis & Detection:** Threat hunting, investigative tactics, TTPs, incident response, incident reporting, threat intelligence.
- **Communication & Collaboration:** Communication, customer service, escalation, collaboration, teamwork, problem-solving.
- **Network Security Technologies:** firewalls, Switches & Routing, TCP/IP, Networking Fundamentals, Network Security, HTTP/HTTPS, DNS, VPNs, Linux/Unix administration.
- **Investigation & Forensics:** Digital forensics, network forensics, endpoint forensics, log analysis, incident handling.
- **Soft Skills:** Analytical thinking, critical thinking, problem-solving, adaptability, strong work ethic.
- **Cloud Security Fundamentals:** Cloud security concepts, cloud security principles, & Azure cloud security

Certifications:

- CompTIA CySA + (Cybersecurity Analyst)
- Java Programming
- Cyber Incident Response and Digital Forensics
- Cybersecurity Fundamentals (IBM-Skills Build)
- Intro to AWS
- TryHackMe Advent of Cyber 2023
- **RHCSA** (Redhat Certified System Administrator)
- Autopsy Forensic Tool
- **Lenel** IPS Programming & Management Certifications
- **Bosch** IDS Certificate & **Feenics** Certificate
- **Milestone** Certification
- Introduction to Cloud Computing
- AWS Identity and Access Management (IAM)
- CompTIA Security + Cert. Preparation certificate(LinkedIn)

Education:

Griffith College Limerick
Master of Science in Network & Information Security
Major in Cyber security

University of Pune
BCA - Bachelor of Computer Application
Major in Computer Science

LANGUAGES UNDERSTAND:

Human (Read, Write, Speak):
English, German (Basic), Hindi, Marathi.

Machine (Read, Write):
C, C++, Java, PHP, CSS, HTML, Perl, .NET, JavaScript, Python, Shell/Bash.

ACADEMIC SKILLS
- Information & Network Security Technologies: Network Security Monitoring (NSM).
- Legal and Ethical Aspects of Information Security.
- IT Infrastructure Protection and Ethical Hacking.
- Cryptography.
- Digital Forensics.
- Managing Information Security.(ISO/NIST Standards)
- Telecommunication Network and Services.
- Network/host vulnerability analysis

Extracurricular activities:
+ **Mobile Gaming:** I love to play mobile Team player games like PubG with my friends, also Xbox games.
+ **Hacking Challenges:** Participating in ethical hacking challenges and CTFs (Capture The Flags) on platforms like HackTheBox.eu, TryHackMe.com in their Lab environment or in test environments on VMware.
+ **FlipperZero:** Exploring Hardware security with FlipperZero. Its open source operating system & hardware allows us to build new apps & tools. I have learned to make c++ apps for IoT devices and learned about hardware built.