Akash Patel

Cyber Security Analyst L2

Address:	Magarpatta, India
Mobile phone:	+91 8054981513
E-mail:	akashpatel1786@gmail.com
LinkedIn	https://www.linkedin.com/in/akash-patel-097610202/
Personal web	*https://www.cyberengage.org/about-8*

Personal profile

Highly Skilled CYSA+ Certified professional expertise in identifying and mitigating security threats, implementing robust security measures, and ensuring the integrity of organizational systems. Adept at enhancing security posture in collaboration with internal teams and MSSPs (Managed Security Service Providers). Seeking a challenging opportunity put up to security initiatives and further develop expertise in a dynamic organization.

KEY NOTES OF PROFILE

- CYSA+ Certified specialist
- Successfully completed the **SANS 508 (2020 edition) Course** (Not certified)
- Hands on Multiple security tools with Communication proficiency of 7 (C1) Bands

Education

2017 – 2020	Guru Nanak dev university Bachelor of Computer Application (CGPA 2.7/4)	Amritsar, India
2014 – 2016	Senior school certificate Physics, Chemistry, Math, Computer Science	Amritsar, India

Work experience

06/09/2022 – Present

Cyber Security Analyst L2 — Pune, India

ConnectWise, Pune

Main responsibilities*:*

- Analyses events generated from IDS/IPS, SIEM, EDR/MDR/XDR, Log-Based Alerts as well hands on tools Like Nessus, Qualys, Sentinel One, Perch, Bit defender, MS defender for business.
- Conducted regular vulnerability assessments and active threat hunting to identify and mitigate potential security risks.
- Guided clients through the security incident response process, from preparation to recovery.
- Adheres to relevant policies, procedures, standards, and security practices such as NIST, GDPR, Cyber Essential.
- Spearheaded the development and implementation of comprehensive incident response plans, enabling swift and effective response to cyber threats and minimizing potential damage.
- Worked on Ransomware, Lock bits, Mimi Katz, Droppers, Viruses, and daily emerging new threats.
- Oversaw and maintained security systems such as firewalls, intrusion detection and prevention systems, and antivirus software, guaranteeing optimal performance and safeguarding against cyber threats.
- Handle the escalation of Cases for harmful events or cases related to cyber incidents. Seamlessly working with various teams, including NOC, Infosec and CRU.

10/04/2021 – 2022

Cyber-Operation Executive — Pune, India

Infosys

Main Responsibilities:

- Monitored security alerts and incidents to identify threats and vulnerabilities.
- Manage governance of firewall rule bases and the associated change management process.

- Conducted log analysis and alert handling to assess security events and determine their severity.
- Perform risk analysis and intelligence information analysis to determine likely threats.
- Documentation of security incidents, procedures, and response actions
- Assistance in chat support, calling queue as well quick responsive and resolving the issue within maintaining the SLA/SLO.
- Conducted Assessments for Clients and prepared reports about the findings.
- Actively engaged handling security events to protect critical assets.

Certifications

2022	Sentinel One **Threat Hunting, Incident response**	Pune, India
2023	FedVTE (USA based learning) **Cyber risk management**	Pune, India
2023	Qualys **Vulnerability management**	Pune, India
2024	Qualys **Vulnerability Application Scanning**	
2023	CompTIA **CYSA+**	Pune, India
2022	EC-Council **Ethical Hacking Essentials**	Pune, India

Upskills

Languages	Native - Punjabi, Hindi English **– fluent (C1)** (IELTS: - BAND 7)
Technical Skills	**Endpoint detection and response**: - Sentinel One, Qualys EDR, Microsoft defender for business **XDR**(Antimalware): - Bit Defender, CrowdStrike (Falcon) **Vulnerability Assessment**: - Nessus, Qualys VMDR, Acunetix **Log Analysis**: - Chainsaw, Hayabusa, LogParser, EvtxECmd. **DFIR**: - Redline, FTK Imager, Autopsy, Cyber triage, OS forensics **Memory Analysis**: - Volatility 3, WinPmem **IDS/IPS**: - Suricata **SIEM**: - Perch **Other Tools: -** Kape, Log2timeline (Plaso).
Core Competencies	Threat/Incident Analysis Vulnerability Assessment Monitoring and responding Incident response/Mitre Framework EDR/XDR/SIEM Log Analysis Security Controls Effective communication

"I hereby affirm that all the information provided in this resume is accurate and true to the best of my knowledge."

Akash Patel