

# Akash Patel

Cybersecurity Incident Response,  
Associate (CYSA+ | CCFE)



**Address:** Magarpatta, India  
**Mobile phone:** +91 8054981513  
**E-mail:** [akashpatel1786@gmail.com](mailto:akashpatel1786@gmail.com),  
[Apatel19800@gmail.com](mailto:Apatel19800@gmail.com)  
**LinkedIn** <https://www.linkedin.com/in/akash-patel-097610202/>  
**Personal web** <https://www.cyberengage.org/about-8>

## Personal profile

Experienced Incident response professional specializing in incident investigations, forensic and mitigation. Proven ability to lead complex security incident investigations, analyse and interpret data to evaluate breaches, and communicate technical findings effectively to senior-level audiences. Proficient in conducting investigations and providing comprehensive solutions to restore trust and protect client assets. Seeking a challenging opportunity to put up security initiatives and further develop expertise in a dynamic organization.

### KEY NOTES OF PROFILE

- CYSA+, CCFE Certified specialist
- Successfully completed the **SANS 508, SANS 500 (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	Amritsar, India
2014 – 2016	Senior school certificate Physics, Chemistry, Math, Computer Science	Amritsar, India

## Work experience

05/2024 – Present                      Cybersecurity Incident Response, Associate                      Gurugram, India

### Ankura

Main responsibilities:

- Scoped and analysed breaches, determining impact and extent.
- Collected and analysed forensic artifacts using Velociraptor, KAPE, FTK, Axiom, and other tools for incident investigations.
- Led incident response for Business Email compromise and ransomware attacks, performing root cause analysis and memory investigation.
- Investigated and eradicated malware, restoring system integrity using EDR, XDR, CDR, AI Based tools.
- Conducted Windows, Mac, and Linux forensic/IR investigation to identify breaches and malware.
- Performed cloud-based investigations (MS365) and provided findings and recommendations to enhance client security posture.
- Created rule-based detections and conducted IOC based threat hunting on affected clients.
- Monitored affected systems to ensure complete threat eradication and prevent recurrence.
- Drafted comprehensive reports detailing incidents and remediation steps.

09/2022 – 05/2024                      Cyber Security Analyst L2                      Pune, India

### ConnectWise

Main responsibilities:

- Analyses events generated from IDS/IPS, SIEM, EDR/MDR/XDR, Log-Based Alerts, Microsoft Sentinel, Antivirus.
- Conducted regular vulnerability assessments/Management and active threat hunting with IOCs/IOAs/TTPs.
- Guided clients through the security incident response process, from preparation to recovery.

- Worked on Ransomware, Lock bits, Mimi Katz, Droppers, Viruses, and daily emerging new threats.
- Worked with different framework MITRE ATT&CK, NIST, Incident response, Cyber Kill chain
- Experience in scripting using PowerShell.
- Possess excellent communication skills, both verbal and written, with extensive experience in writing forensic incident investigation reports.

05/2021 – 09/2022

Cyber-Operation Executive

Pune, India

## Infosys

Main

Responsibilities:

- Experience in security monitoring, detection, and analysis methodologies and technologies.
- 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 with documentations.
- 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.

## Certifications

2022	Sentinel One <b>Threat Hunting, Incident response</b>	Pune, India
2024	Infosec (Certifying body: GIAC) <b>Certified Computer Forensic Examiner</b>	Pune, India
2023	CompTIA <b>CYSA+</b>	Pune, India

## Upskills

Languages	Native - Punjabi, Hindi English – <b>fluent (C1)</b> (IELTS: - BAND 7)
Technical Skills	<b>EDR:</b> - Qualys EDR, Carbon Black <b>MDR:</b> - Sentinel One <b>XDR:</b> - Bit Defender, CrowdStrike (Falcon), MDFE <b>CDR:</b> - Obsidian <b>SIEM:</b> -Microsoft Sentinel (IR Purposes) <b>Log Analysis:</b> - Chainsaw, Hayabusa, LogParser, EvtxECmd. <b>DFIR:</b> - Redline, FTK Imager, Cyber triage, OS forensics, Magnet Axiom, Vound Intella, Velociraptor <b>Memory Analysis:</b> - Volatility 3, WinPmem, MemProc5 <b>Other Tools:</b> - Kape, Log2timeline (Plaso), Kansa, Microsoft extractor Suite

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

**Akash Patel**