Ravi Prajapati

IT Support Specialist | IT Support Engineer | Infrastructure Support | Junior Cybersecurity / SOC

Köln, Deutschland | +49 15566434608 | prajapatiravi141@gmail.com | linkedin.com/in/ravi-prajapati-it | github.com/raviprajapati-it

Vollzeit verfügbar | Schwerpunkt Deutschland | Offen für passende Positionen in ganz Europa

PROFIL

IT Support Specialist mit über 4 Jahren Erfahrung im Enterprise-IT-Support in Deutschland und Indien, in Umgebungen mit etwa 100 bis 800+ Anwendern sowie mit Remote-Support in der EMEA-Region. Aktuell arbeite ich als IT Support Specialist (Werkstudent) bei Simon-Kucher in Köln. Den BSc (Hons) Cyber Security habe ich abgeschlossen; das finale Ergebnis liegt vor, die formale Abschlussurkunde steht noch aus. Berufliche Erfahrung umfasst Windows, Microsoft 365, Active Directory, ITSM, Endpoint-Rollout, Network Access Control, Mobile-Device-Administration, Asset Lifecycle, VPN-/Netzwerk-Troubleshooting und On-/Offboarding. Cybersecurity-Kompetenz wurde durch Studium, Forschung, autorisierte Labore und sechs abgeschlossene technische Projekte entwickelt und wird nicht als frühere professionelle SOC- oder Penetration-Testing-Tätigkeit dargestellt.

KERNKOMPETENZEN

Enterprise IT: Windows 10/11, Microsoft 365, Active Directory, TOPdesk, ServiceNow, PacketFence/NAC, Ivanti MDM, Matrix42, Endpoint-Rollout, Softwarezuweisung, IT Asset Lifecycle, On-/Offboarding

Netzwerk & Infrastruktur: TCP/IP, DNS, VPN, LAN/WLAN, VLANs, Routing/Switching, Firewalls, IPsec, Netzwerk-Troubleshooting, Cisco Packet Tracer

Cybersecurity & Analyse: Incident Response, Network Forensics, Malware-Analyse, MITRE ATT&CK, Vulnerability Assessment, Penetration Testing, OWASP Top 10, Secure Coding, Wireshark, NetworkMiner, Nmap, Burp Suite, PEStudio, Python

BERUFSERFAHRUNG

IT Support Specialist (Werkstudent) | Simon-Kucher

Jan. 2026 - heute | Köln, Deutschland

- Support für 230+ Mitarbeitende in Köln sowie Remote-Support für Anwender in der EMEA-Region in einem internationalen Beratungsumfeld.
- Bearbeitung von etwa 20-30 TOPdesk-Incidents und Service Requests pro Woche für Windows, Microsoft 365, VPN, Netzwerk, Hardware, Software, mobile Geräte, Drucker und Workplace-Technologien.
- Konfiguration, Rollout und Betreuung von 100+ Windows-Laptops sowie Unterstützung bei 50+ On-/Offboardings inklusive Active-Directory-Administration und sicherer Gerätevorbereitung.
- Unterstützung bei PacketFence Network Access Control, Ivanti-Firmen-iPhones, Matrix42 Endpoint-/Software-Management, Asset Lifecycle, Meetingraumtechnik und Workplace-Infrastruktur.

Deskside Support Technician | Iron Systems India Pvt. Ltd.

Nov. 2022 - Okt. 2023 | Vadodara, Indien

- Enterprise-Deskside-Support für 500+ Anwender an drei Standorten und Bearbeitung von etwa 50-60 ServiceNow-Incidents/Service Requests pro Woche.
- Konfiguration, Imaging, Rollout und Wartung von 300+ Windows-Laptops, Desktops und Thin Clients; RAM/SSD-Upgrades, VPN-Konfiguration, Drucker- und Active-Directory-Support.
- Mitwirkung beim Aufbau eines Engineering-Standorts mit strukturierter Verkabelung, Serverraum-Vorbereitung, Switches/Router, Glasfaser, WLAN, Cisco IP Phones, CCTV, Druckern und Meetingraumtechnik.

Technical Assistant - IT | Spandana Sphoorty Financial Limited

Apr. 2022 - Nov. 2022 | Vadodara, Indien

- Täglicher IT-Support für etwa 30-40 Anwender an fünf Standorten: Microsoft 365, Endgeräte, Drucker, Software-Installation, Dokumentation und IT-Asset-Daten.
- Regelmäßiger Vor-Ort-Support in Niederlassungen sowie Pflege von Inventar und Workplace-Technologien.

BERUFSERFAHRUNG - FORTSETZUNG

Field Tech Associate | NTT DATA Information Processing Services Pvt. Ltd.

Feb. 2020 - Feb. 2022 | Vadodara, Indien

- Support für etwa 100 Anwender in Vadodara, Ahmedabad und Surat sowie Bearbeitung von etwa 40-50 ServiceNow-Incidents pro Woche in einem geschäftskritischen Finanzdienstleistungsumfeld.
- Unterstützung der Migration von Windows 7/8 auf Windows 10 inklusive OS-Imaging, Application Deployment, Domain Join, Active-Directory-Administration, Shared-Drive-Berechtigungen, VPN, LAN/WLAN, Drucker, mobile Geräte, Hardware und Software.
- Unterstützung der COVID-19-Umstellung auf Remote Work durch Gerätevorbereitung und VPN-/Remote-Access-Support bei etwa 90 % SLA-Erfüllung.

Desktop Support Engineer | IMSI Staffing Pvt. Ltd.

Mai 2019 - Feb. 2020 | Ahmedabad, Indien

- Enterprise-Desktop-Support in einem dreiköpfigen Team für 800+ Anwender in zwei Bürogebäuden und Bearbeitung von etwa 60-80 ServiceNow-Incidents pro Woche.
- Unterstützung bei Endpoint-Rollout, Windows-Migration, Active Directory, Hardware-Reparatur, Druckern/Scannern, Asset Lifecycle sowie On-/Offboarding.
- Wiederherstellung von etwa 80 % geschäftskritischer Daten einer ausgefallenen Executive-Laptop-Festplatte mit Anerkennung durch das Senior Management.

AUSGEWÄHLTE CYBERSECURITY-PROJEKTE

Network Forensics & Malware Traffic Analysis: 600+ MB Malware-PCAP; Wireshark, NetworkMiner, eigenes Python-PCAP-Analyse-Skript; ca. 2,47 Mio. Pakete / 1,64 GB; HTTP-C2, Backconnect und spätere TLS-Kommunikation; Evidenz für **potenzielle**, nicht bestätigte, Datenexfiltration.

Ransomware-Analyse - LockBit & BlackCat: Isolierte Windows-Laborumgebung mit PEStudio, Process Monitor, Process Explorer, Autoruns und Event Viewer für vergleichende statische/dynamische Analyse und dokumentiertes Ransomware-Verhalten.

Cybersecurity Incident Classification: 50.000 Microsoft-GUIDE-Datensätze, 694 hybride Features, drei Ensemble-Klassifikatoren; Random Forest 69,28 % Test-Accuracy, 0,6963 Weighted F1, 75,96 % Cross-Validation; Forschungsprototyp.

Internal Network Penetration Testing: Autorisiertes, absichtlich verwundbares Labor mit Nmap, SMB-Enumeration, Burp Suite, SQL Injection, sqlmap, Webmin 1.984 / CVE-2022-0824, kontrollierter Impact-Validierung und Remediation.

Secure Enterprise Network Design: Cisco-Packet-Tracer-Fallstudien mit VLANs, IPv4-Subnetting, Layer-3-Switching, OSPF, DHCP, ACLs, Cisco ASA, NAT/PAT, SSH, DMZ und Site-to-Site-IPsec-VPN.

Secure Coding & Application Security: Fünf kontrollierte Fälle in C, Java, PHP und Python zu Buffer Overflow, SQL Injection, Reflected XSS, Hardcoded Credentials und unsicherer Deserialisierung mit Remediation und Re-Test.

AUSBILDUNG

BSc (Hons) Cyber Security | University of Gloucestershire | Sep. 2023 - Aug. 2026 | Abgeschlossen - finales Ergebnis erhalten; formale Abschlussurkunde ausstehend

Diplom in Information Technology | The Maharaja Sayajirao University of Baroda | Juli 2016 - Apr. 2019 | Second Class

WEITERBILDUNG & ZERTIFIZIERUNGEN

- ISC2 Certified in Cybersecurity (CC) Training - abgeschlossen im Juli 2026; nur Trainingsabschluss, keine CC-Zertifizierung behauptet.
- Incident Response Planning - LinkedIn Learning, Aug. 2026.
- Learning Cyber Incident Response and Digital Forensics - LinkedIn Learning, Aug. 2026.
- Practical Cybersecurity for IT Professionals - LinkedIn Learning, März 2026.
- Advanced Pen Testing Techniques for Active Directory - LinkedIn Learning, Apr. 2026.
- OpenAI ChatGPT: Creating Custom GPTs - LinkedIn Learning, Apr. 2026.
- Historische Qualifikationen: Certified Ethical Hacker (CEH) - abgelaufen 2018; CompTIA Network+ - abgelaufen 2018.

ZUSÄTZLICHE ERFAHRUNG & SPRACHEN

Weitere Erfahrung: Ops Associate Plus, Flink, Köln (Teilzeit parallel zum BSc-Studium), Aug. 2024 - Dez. 2025.

Sprachen: Englisch - Professional Working | Deutsch - A1-A2 / Grundkenntnisse, aktive Weiterentwicklung | Hindi - Muttersprache/Bilingual | Gujarati - Muttersprache/Bilingual