ENTERPRISE IT SUPPORT | CYBERSECURITY | NETWORK SECURITY

Ravi Prajapati

Cybersecurity & Enterprise IT Portfolio

IT Support Specialist (Working Student) | BSc (Hons) Cyber Security completed - final result received, degree certificate pending

Enterprise IT experience. Security-focused development.

4+ years of enterprise IT support across Germany and India, with current EMEA support at Simon-Kucher in Cologne. Cybersecurity capability developed through a completed BSc, research, authorised labs, and six technical projects.

TARGET ROLES

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

4+	**230+**	**800+**	**6**
Years enterprise IT support	Employees at current Cologne office	Largest enterprise user environment	Completed cybersecurity projects

Cologne / North Rhine-Westphalia, Germany | Available for full-time opportunities | Germany-first, open across Europe

prajapatiravi141@gmail.com **linkedin.com/in/ravi-prajapati-it** **github.com/raviprajapati-it**

PORTFOLIO OVERVIEW

Professional foundation & technical toolkit

Enterprise IT experience is shown separately from academic, research, lab, and project-based cybersecurity work so the scope of experience remains clear and defensible.

PROFESSIONAL FOUNDATION

Enterprise IT Support

- Simon-Kucher: 230+ Cologne employees plus remote support across EMEA; TOPdesk, Windows, Microsoft 365, Active Directory, VPN, endpoint deployment, NAC, MDM, asset lifecycle.
- Iron Systems: 500+ users across three locations; 50-60 weekly ServiceNow tickets; 300+ endpoints; new engineering-office infrastructure rollout.
- NTT DATA: multi-site financial-services support; Windows migration, AD, VPN, LAN/Wi-Fi, remote-work enablement and approximately 90% SLA compliance.
- IMSI Staffing: 800+ users; ServiceNow, Windows deployment, Active Directory, hardware repair, asset lifecycle and data-recovery recognition.

CYBERSECURITY DEVELOPMENT

Degree, research & projects

- BSc (Hons) Cyber Security completed; final result received; formal degree certificate pending.
- Six completed technical projects across network forensics, ransomware analysis, AI-assisted incident classification, enterprise network design, authorised penetration testing, and secure coding.
- ISC2 Certified in Cybersecurity (CC) training completed in July 2026; no active CC certification claimed.
- Historical CEH and CompTIA Network+ certifications expired in 2018 and are shown only as historical credentials.

ENTERPRISE / NETWORK

Applied professionally + through projects

- Windows 10/11, Microsoft 365, Active Directory, TOPdesk, ServiceNow
- Endpoint deployment, Matrix42, Ivanti MDM, PacketFence / NAC
- TCP/IP, DNS, VPN, LAN/Wi-Fi, VLANs, routing/switching, firewalls, IPsec

SECURITY / ANALYSIS

Academic, research & lab context

- Incident response, network forensics, malware analysis, digital forensics, threat analysis
- MITRE ATT&CK, vulnerability assessment, penetration testing, OWASP Top 10, secure coding
- Wireshark, NetworkMiner, Nmap, Burp Suite, PEStudio, Process Monitor, Python, ML/NLP

PROJECT 01 | NETWORK FORENSICS

Network Forensics & Malware Traffic Analysis

Malware-traffic investigation using Wireshark, NetworkMiner, and a custom Python PCAP-analysis script to reconstruct suspicious host behaviour and command-and-control activity.

600+ MB
Malware PCAP analysed

2.47M
Packets linked to primary suspicious host

1.64 GB
Traffic associated with the host

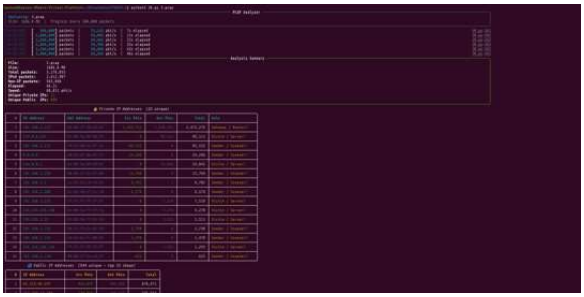
TLS
Later encrypted C2 communication

APPROACH & FINDINGS

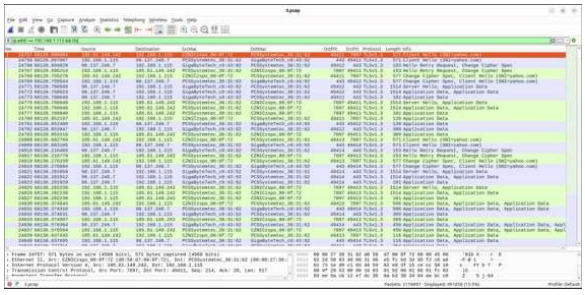
- Reviewed endpoints, conversations, DNS, HTTP behaviour, transferred artefacts, and traffic volume to isolate anomalous activity.
- Used a custom Python PCAP-analysis script to support repeatable host-level investigation and traffic analysis.
- Reconstructed HTTP beaconing, proxy registration, backconnect infrastructure, configuration activity, and later encrypted TLS communication.
- Evidence was consistent with potential data exfiltration, but the PCAP did not support claiming confirmed successful exfiltration.

SECURITY RELEVANCE

- Packet-level investigation and traffic baselining
- Endpoint correlation and command-and-control reconstruction
- Evidence handling and disciplined limitation reporting
- Analytical scripting for repeatable network investigation



Host-level PCAP analysis identifying the primary suspicious system and quantifying activity.



Later-stage traffic showing the transition toward encrypted TLS communication.

EVIDENCE BOUNDARY

Potential data exfiltration was investigated, but the available PCAP did not provide sufficient evidence to claim confirmed successful exfiltration.

Ransomware Analysis - LockBit & BlackCat (ALPHV)

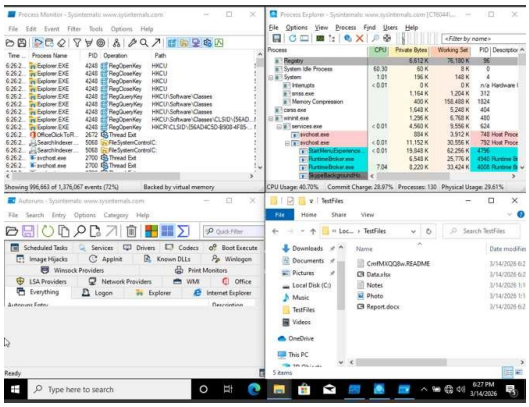
Comparative static and dynamic malware analysis of two ransomware families inside an isolated Windows laboratory environment.

METHOD

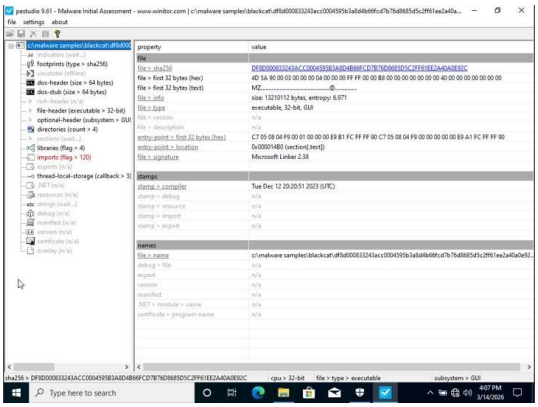
- Isolated Windows lab with networking disabled and recoverable snapshots
- Static analysis with PEStudio
- Dynamic analysis with Process Monitor, Process Explorer, Autoruns, and Event Viewer
- Controlled test files and documented sample hashes

OBSERVED BEHAVIOUR

- Controlled test-file encryption
- Ransom-note behaviour and LockBit wallpaper modification
- Process and file-system activity during execution
- BlackCat reconnaissance-related behaviour



Dynamic LockBit analysis inside the controlled Windows laboratory.



PEStudio static analysis of BlackCat (ALPHV) sample characteristics.

SAFETY & EVIDENCE BOUNDARY

All dynamic analysis was performed inside an isolated laboratory environment using controlled test files. The portfolio documents investigation methodology and evidence only; malware samples are not hosted or distributed.

PROJECT 03 | AI / MACHINE LEARNING

Cybersecurity Incident Classification - NLP, ML & MITRE ATT&CK

BSc dissertation research evaluating an AI-assisted cybersecurity incident-classification pipeline using text features, transformer embeddings, structured security metadata, and ensemble machine-learning models.

50,000
Security incident records

694
Engineered hybrid features

69.28%
Best reported test accuracy

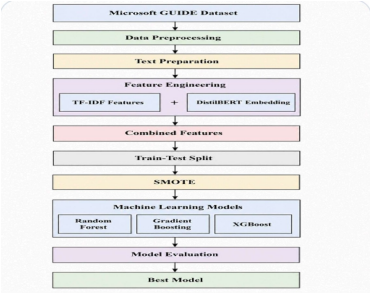
75.96%
Cross-validation accuracy

RESEARCH APPROACH

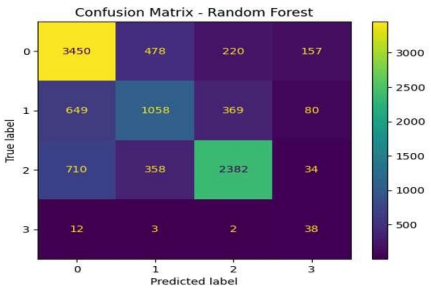
- Prepared a 50,000-record research subset from Microsoft GUIDE
- Combined TF-IDF, Sentence Transformer embeddings, and structured metadata
- Used SMOTE and benchmarked Random Forest, Gradient Boosting, and XGBoost
- Evaluated accuracy, weighted F1, cross-validation, confusion matrices, ROC and precision-recall analysis

KEY RESULT

Random Forest
69.28% test accuracy
0.6963 weighted F1
75.96% cross-validation accuracy



Experimental pipeline combining GUIDE data, NLP features, metadata, SMOTE, and ensemble models.



Random Forest confusion matrix used to inspect class-level performance and errors.

RESEARCH BOUNDARY

Academic research prototype only - not production deployment, autonomous SOC decision-making, or live-enterprise operational performance.

Secure Enterprise Network Design

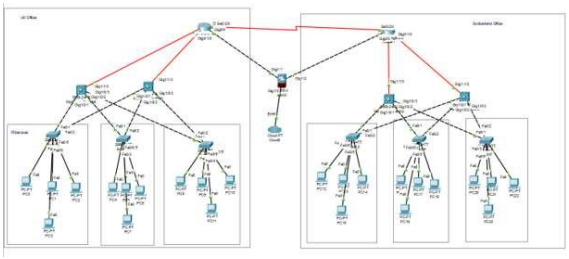
Three Cisco Packet Tracer enterprise-network architecture case studies covering multi-site connectivity, secure data-center design, segmentation, firewall controls, secure administration, and VPN architecture.

TECHNICAL IMPLEMENTATION

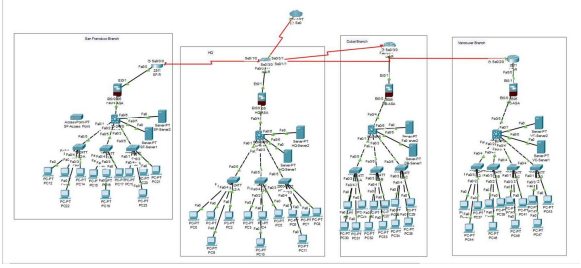
- VLAN segmentation and IPv4 subnetting
- Layer 3 switching, static routing, OSPF, and DHCP
- ACLs, Cisco ASA, NAT/PAT, SSH, DMZ architecture
- Site-to-site IPsec VPN and multi-site connectivity

PROJECT SCOPE

- UK-Switzerland multi-site enterprise architecture
- Secure data-center redesign
- Global HQ-to-branch architecture spanning San Francisco, Dubai, and Vancouver
- Original topologies and configuration evidence preserved in the technical project



Original Packet Tracer topology for the UK-Switzerland multi-site case study.



Global HQ-to-branch Packet Tracer architecture.

EXPERIENCE BOUNDARY

These architectures were designed and documented as academic/technical case studies in Cisco Packet Tracer. They demonstrate network-design and security concepts but do not represent production networks professionally operated for the organisations shown in the scenarios.

Offensive Security & Application Security

Controlled assessment and remediation work in authorised or deliberately vulnerable project environments.

PROJECT 05

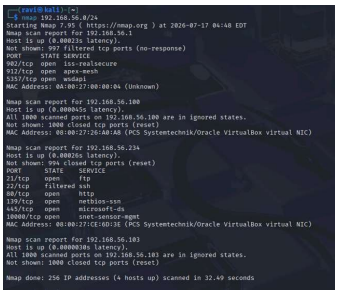
Internal Network Penetration Testing

- Authorised assessment against an intentionally vulnerable lab
- Nmap reconnaissance, SMB / enum4linux, Burp Suite, SQL injection and sqlmap
- Webmin 1.984 / CVE-2022-0824 assessment with controlled RCE/root validation
- Controlled post-exploitation, persistence-risk analysis and remediation recommendations

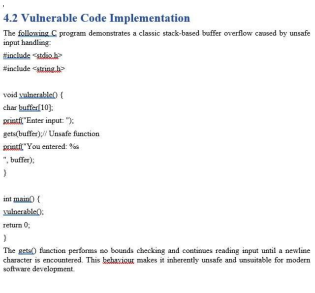
PROJECT 06

Secure Coding & Application Security

- Five case studies across C, Java, PHP, and Python
- Buffer overflow, SQL injection, reflected XSS, hardcoded credentials, insecure deserialization
- Controls included bounded memory handling, parameterized queries, context-aware encoding, externalized secrets, and restricted deserialization
- Workflow: vulnerability -> remediation -> security re-test



Initial service discovery against the authorised lab target.



4.2 Vulnerable Code Implementation

The following C program demonstrates a classic stack-based buffer overflow caused by unsafe input handling:

```
#include <stdio.h>
#include <string.h>

void vulnerable() {
char buffer[10];
printf("Enter input: ");
gets(buffer);// Unsafe function
printf("You entered: %s
", buffer);
}

int main() {
vulnerable();
return 0;
}
```

The gets() function performs no bounds checking and continues reading input until a newline character is encountered. This behaviour makes it inherently unsafe and unsuitable for modern software development.

Controlled testing of a vulnerable buffer-handling implementation.

AUTHORISATION BOUNDARY

Testing was confined to an authorised, intentionally vulnerable laboratory. Detailed exploit instructions are intentionally omitted from this portfolio summary.

SECURITY BOUNDARY

Vulnerable examples exist only for controlled security education, analysis, remediation, and validation; they are not presented as deployment-ready software.

PROFILE SIGNAL

Education, credentials & languages

A security-focused profile grounded in real enterprise IT support.

EDUCATION

BSc (Hons) Cyber Security
University of Gloucestershire
Sep 2023 - Aug 2026
Completed - final result received; degree certificate pending

PROFESSIONAL DEVELOPMENT

ISC2 Certified in Cybersecurity (CC) Training
Completed Jul 2026 - training completion only; certification not claimed.

Historical: CEH and CompTIA Network+ expired in 2018.

LANGUAGES

- English - Professional Working
- German - A1-A2 / Basic, actively improving
- Hindi - Native / Bilingual
- Gujarati - Native / Bilingual

TARGET ROLES

- IT Support Specialist
- IT Support Engineer
- Infrastructure Support Engineer
- Junior Cybersecurity Analyst / Junior SOC Analyst

CONNECT & CONTACT

Germany-first job search, open to suitable opportunities across Europe. Available for full-time opportunities.

prajapatiravi141@gmail.com **linkedin.com/in/ravi-prajapati-it** **github.com/raviprajapati-it**

Cologne / North Rhine-Westphalia, Germany