RĂZVAN COLIȚESCU

CYBERSECURITY ENGINEER — NETWORK & CLOUD SECURITY

DETAILS

Warsaw, Poland
Open for relocation within EU
+48 780 781 704
razvan.colitescu@outlook.com

LINKS

https://razvancolitescu.com/

CERTIFICATIONS

CCNA (Cisco) — Jun 2023
CompTIA Security+ — Jun 2024
AWS Certified Solutions Architect – Associate
In progress — exam not yet scheduled

LANGUAGES

English — Fluent
Romanian — Native
French — Basic

CORE SKILLS

- Cloud Security: Azure (Defender for Cloud) — hands-on; AWS — in progress
- SIEM: Splunk, Grafana, SolarWinds, Microsoft Sentinel
- EDR: CrowdStrike, Microsoft Defender
- Firewalls: Palo Alto (Panorama, Provider-1, PAN-OS, SASE), Check Point, Cisco ASA, Meraki
- Network Security Monitoring & Analysis
- Protocols: TCP/IP, IPsec, VPN (IKEv1, IKEv2)
- Scripting: Bash (comfortable), Python & C (basic)
- Threat Frameworks: MITRE ATT&CK, Cyber Kill Chain
- Vulnerability Management: Nessus, Indeni
- Compliance: ISO 27001, NIST, GDPR

Profile

Cybersecurity engineer with over three years progressing from SOC analysis into network security engineering at Visa, blending real-time defense, automation, and threat-driven design across high-stakes financial infrastructure. **Hands-on cloud security experience with Microsoft Azure (Defender for Cloud),** currently studying for the AWS Certified Solutions Architect – Associate certification to build equivalent depth on AWS, with AWS Certified Security – Specialty as the next milestone. Certified in CCNA and CompTIA Security+, proficient in SIEM monitoring, firewall administration, and network security tooling. A proactive, analytical defender focused on translating attacker tradecraft into resilient, cloud-aware security architecture.

EMPLOYMENT HISTORY

Cybersecurity Engineer – Network Security, VISA (Warsaw, Poland)

JULY 2025 — PRESENT ★ **Current Role — Promoted from SOC Analyst**

Operates at the intersection of network security engineering and adversarial thinking — securing Visa's global infrastructure through layered defence while studying how attackers think, move, and bypass controls.

- **Perimeter defence:** maintain and engineer perimeter defences using Check Point and Palo Alto (Panorama, Provider-1).
- **Policy tuning:** analyse and tune firewall policies with attacker TTPs and evasion techniques in mind.
- **Automation:** support rule management, configuration validation, and traffic analysis using scripting (Python, Bash) and APIs.
- **Threat hunting:** perform deep packet inspection and anomaly hunting during DDoS and traffic-based attacks.
- **Architecture:** collaborate with security architecture to simulate potential attack paths across services.
- **Incident remediation:** provide technical remediation for incidents involving lateral movement, tunnelling, or C2 behaviour.
- **Risk visibility:** support auditing and threat modelling using Tufin to visualize access exposure.
- **Offensive research:** researches offensive tooling (Metasploit, Nmap, DNS-based C2, malware IOCs) to align defence with emerging threats.

Cybersecurity SOC Analyst, VISA (Warsaw, Poland)

NOVEMBER 2023 — JULY 2025

- **Security monitoring:** continuously monitored and analysed alerts from Splunk, Grafana, and SolarWinds across network, application, and cloud environments.
- **Incident response:** led triage, investigation, and containment using playbooks, automation, and EDR platforms such as Microsoft Defender.
- **Network & endpoint security:** administered Palo Alto SASE, PAN-OS firewalls, BlueCoat proxies, Check Point firewalls, Arbor DDoS protection, and DLP systems.
- **Threat hunting:** proactively hunted threats using the MITRE ATT&CK framework and conducted vulnerability assessments with Indeni.
- **Cloud security operations: supported cloud security controls and configurations in Azure using Microsoft Defender for Cloud.**
- **Process optimization:** developed and refined SOC procedures, incident playbooks, and knowledge base documentation.
- **Reporting:** worked cross-functionally with IT and engineering teams, providing incident reports and risk assessments.

Key Achievements

- Configured SE-Linux for RHEL servers in collaboration with application teams.
- Enhanced SIEM event correlation to improve incident detection.
- Contributed to automation workflows for incident response using scripting (Python, PowerShell).

- Strengthened network defenses through effective WAF policy management.

Network Security Engineer, CISCO (Kraków, Poland)
JULY 2022 — OCTOBER 2023

- **Network design:** designed secure network topologies using Cisco Meraki with VLAN segmentation, firewall policies, and VPN configurations.
- **Firewall administration:** managed and optimized Cisco ASA and Meraki firewalls, configuring ACLs and VPN tunnels.
- **Threat analysis:** identified and resolved network vulnerabilities, including authentication issues and IP conflicts.
- **VPN management:** configured and troubleshot site-to-site VPNs using IPsec (IKEv1/IKEv2) protocols.

Key Achievements

- Built a Cisco Meraki lab environment for employee hands-on training.
- Contributed to network security playbooks and procedures.
- Delivered network security training and guidance to clients.

End User Computing Engineer, WIPRO (Bucharest, Romania)
AUGUST 2018 — JUNE 2022

- Provided premium end-user IT services and acted as escalation point for service issues and 3rd-party providers.
- Served as main point of contact for local IT security incidents, ensuring compliance with organizational standards.
- Performed complex troubleshooting to improve system reliability, scalability, and performance.

Infrastructure and Support Specialist, GENPACT (Bucharest, Romania)
OCTOBER 2016 — AUGUST 2018

- Managed DHCP configuration, VLAN assignment, and Cisco switch configuration.
- Administered Active Directory user/group management and RSA token provisioning.
- Created SOPs and trained new and existing associates.

IT Support Level 1 Agent, GENPACT (Bucharest, Romania)
AUGUST 2015 — OCTOBER 2016

- Provided Level 1 support for Genpact Europe employees, logging and triaging cases via ServiceNow.
- Supported remote access, network, server, and telephony issues using AD, RDP, and VPN.

EDUCATION

Bachelor of Science (BSc), Computer Science — In Progress
OPIT — Open Institute of Technology, Malta

Expected graduation: Spring 2028

BA in Social, Humanist and Nature Sciences — Geography
Hyperion University, Bucharest
September 2013 — September 2016