Optiuni de cariera

Cofinanțat de Uniunea Europeană

Proiect cofinanțat din Fondul Social European prin Programul Educație și Ocupare 2021-2027
Axa prioritara: P07
Titlul proiectului: Practică Racordată Actualității Constănțene în Tehnologia Informației și Comunicații
Contract: PE0/71/PEO _P7 /OP4/ESO4.5/PEO _A49/ G2024-63816/ SMIS 311134

Obiective

- perspectiva realista asupra rolurilor profesionale disponibile;
- informatii despre certificarile relevante si recunoscute international;
- recomandari pentru continuarea studiului si specializarii;
- sugestii de resurse, comunitati si experiente practice care pot accelera progresul profesional

Context, tendinte si directii viitoare in industrie

Industria securitatii cibernetice este intr-o expansiune continua, alimentata de cresterea numarului de atacuri, de reglementari tot mai stricte si de nevoia organizatiilor de a-si proteja datele si infrastructura. In acest context, rolurile de tip Blue Team capata o importanta tot mai mare.

Specialistii bine pregatiti sunt cautati atat in mediul privat, cat si in sectorul public, iar cererea pentru competente defensive depaseste in mod constant oferta disponibila pe piata.

Tendinte:

- Automatizarea și inteligența artificială în detecția și răspunsul la incidente.

Integrarea soluțiilor SIEM și SOAR pentru o viteză crescută de reacție.

- Necesitatea competențelor cloud și devsecops, având în vedere migrarea infrastructurilor.
- Accentul pe threat hunting și threat intelligence, pentru detecție proactivă.
- Orientarea către privacy și conformitate, în lumina reglementărilor GDPR, NIS2, etc.

Tipuri de cariere

Rolurile acopera un spectru larg, de la pozitii de inceput de cariera pana la functii strategice si de management:

• **Security Analyst (SOC):** monitorizeaza sistemele, investigheaza si prioritizeaza alertele de securitate.

• **Incident Responder**: gestioneaza incidentele de securitate si coordoneaza procesul de remediere.

• **Threat Hunter**: identifica in mod proactiv amenintari avansate care nu sunt detectate automat.

• **Vulnerability Analyst**: analizeaza vulnerabilitatile si propune masuri de reducere a riscurilor.

• **Security Engineer**: proiecteaza, implementeaza si configureaza solutii de securitate defensive.

• **Compliance Officer / Auditor**: verifica respectarea standardelor, politicilor si reglementarilor.

• **CISO** (Chief Information Security Officer): defineste si conduce strategia generala de securitate la nivel organizational.

.

Tipuri de cariere

Cum afecteaza AI piata de Blue Team?

- Scade cererea pentru task-uri “manuale” → entry-level SOC L1 devine mai mic ca volum si multe task-uri se muta in SOAR / AI agents
- Creste cererea pentru roluri de analiza si decizie → AI-ul realizeaza analiza la nivel de SOC L1, ca atare munca manuala scade, gandirea critica creste, analistul devine mai mult decident si inginer de Securitate decat operator de alerte

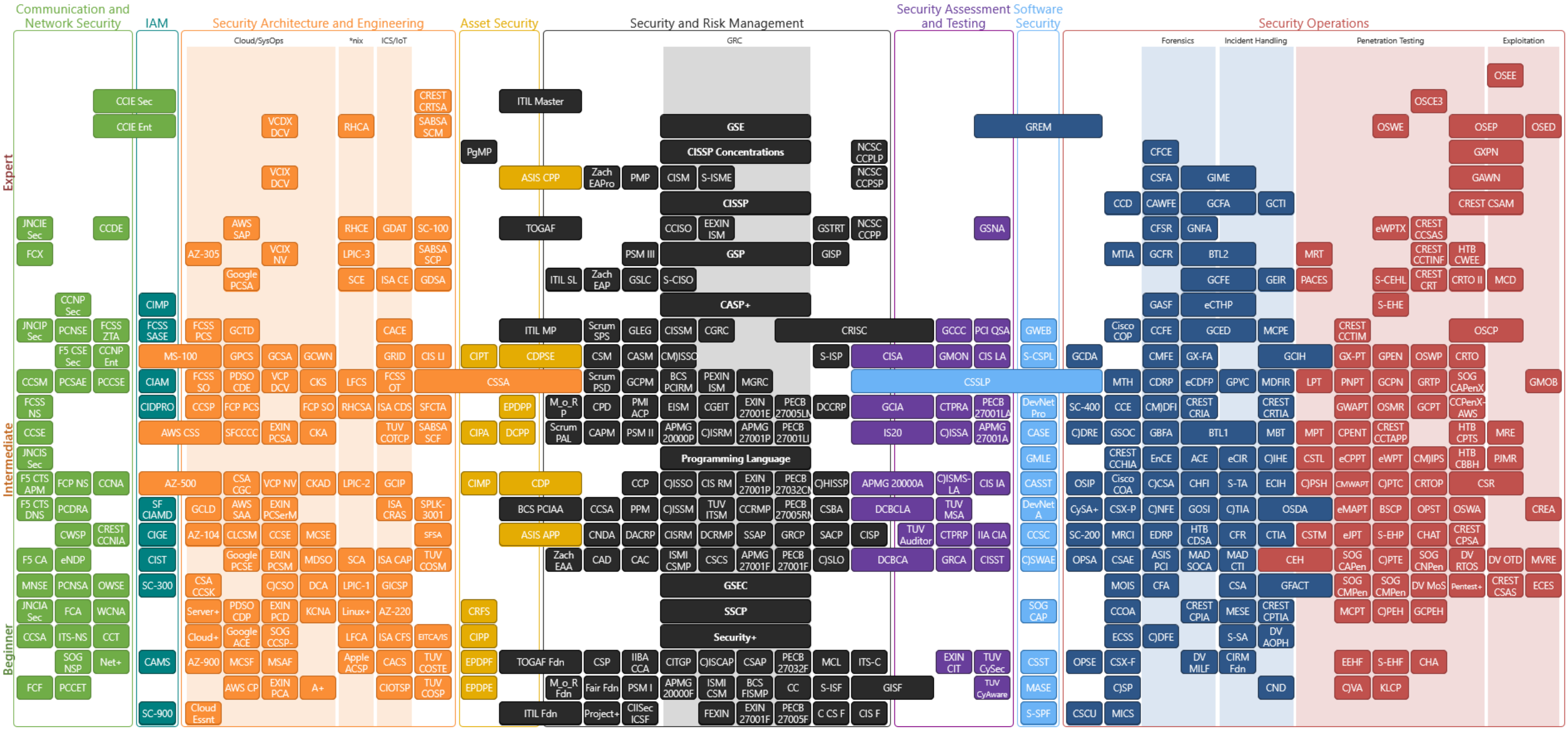
Joburi noi sau in crestere in Blue Team:

- **AI Security Analyst / AI SOC Analyst** (verifica alertele generate de AI, ajusteaza modele de detective, valideaza false positives AI)
- **SOAR / Automation Engineer [Security Automation]** (construire playbook-uri automate, integrare EDR + SIEM + Cloud, coordonare si automatizare a gestionarii incidentelor de securitate.
- **Detection Engineer** (scriere reguli de detectie (Sigma, KQL, Splunk), reducere false positives, mapping MITRE ATT&CK)

Tipuri de cariere

- **Cloud Security Engineer (Blue)** - AWS / Azure / GCP security, IAM misconfig detection, cloud posture management (CSPM), container security → atacurile se muta in cloud + AI ruleaza acolo
- **Threat Hunter (AI-assisted) -** hunting proactiv in logs, detectare comportamente anormale, folosire AI pentru pattern discovery
- **Security Data Engineer -** pipeline-uri de loguri, normalizare date security, ingestie SIEM scale mare, data quality pentru AI detection → fara acest element, AI in security nu isi poate indeplini rolul in mod eficient
- **Security Tooling / Platform Engineer** - administrare SIEM modern, integrare EDR/XDR, tuning platforme AI security → devine mai aproape de DevOps + Security

Security Certification Roadmap



Sursa:https://pauljerimy.com/security-certification-roadmap/

Exemple de certificari

Nivel	Certificare	Organizatie	Focus principal	Observatii
Incepator	CompTIA Security+	CompTIA	Fundamente cybersecurity (retele, threat-uri, IAM)	Cea mai comuna baza pentru Blue Team
Incepator	Microsoft SC-900	Microsoft	Security, compliance, identity basics	Bun pentru ecosistem Azure
Incepator	Google Cybersecurity Certificate	Google	Intro SOC, log analysis, basic IR	Foarte bun pentru entry-level SOC
Incepator	Cisco Certified CyberOps Associate	Cisco	SOC operations, monitoring, basic IR	Foarte orientat pe SOC L1
Incepator	Blue Team Level 1 (BTL1)	Security Blue Team	Hands-on SOC, IR, SIEM	Foarte practic, apreciat pentru entry Blue Team

Exemple de certificari

Nivel	Certificare	Organizatie	Focus principal	Observatii
Intermediar	CompTIA CySA+	CompTIA	Threat detection, behavioral analytics	Standard pentru SOC L2
Intermediar	Microsoft SC-200	Microsoft	Security Operations Analyst (Defender, Sentinel)	Foarte relevant pentru SOC modern
Intermediar	Splunk Core Certified User / Power User	Splunk	Log analysis, SIEM queries	Esential pentru SOC data analysis
Intermediar	GIAC GSEC - GIAC Security Essentials	SANS	Security fundamentals + defensive depth	Mai tehnic si mai scump
Intermediar	GIAC GCIH - Certified Incident Handler	SANS	Incident handling + IR advanced	Foarte respectata in IR

Exemple de certificari

Nivel	Certificare	Organizatie	Focus principal
Avansat	GIAC GCIH (Incident Handler)	SANS Institute	Incident response avansat, attack handling
Avansat	GIAC GCIA (Intrusion Analyst)	SANS Institute	Network traffic analysis, detection engineering
Avansat	GIAC GNFA (Network Forensics)	SANS Institute	Forensics avansat pe retea
Avansat	Microsoft SC-100 (Architect)	Microsoft	Security architecture end-to-end

Nivel	Certificare	Organizatie	Focus principal
Expert	GIAC Security Expert (GSE)	SANS Institute	Nivel elită, multi-domeniu (IR, forensics, detection)
Expert	CISSP (Blue-relevant dar broad)	$(ISC)^2$	Arhitectura securitate, governance, design

Resurse educationale

Step by step guide to becoming a Cyber Security Expert in 2026
https://roadmap.sh/cyber-security

Ultimate Cybersecurity Mastery Roadmap
https://github.com/Hamed233/Cybersecurity-Mastery-Roadmap

RangeForce Cloud-Based Cyber Range | Cybersecurity Training
https://www.rangeforce.com/

Blue Team Labs Online - A gamified platform for cyber defenders to test and showcase their skills
https://blueteamlabs.online/

Cybersecurity Blue Team Labs & Training
https://cyberdefenders.org/blue-team-labs/

Security Certification Roadmap
https://pauljerimy.com/security-certification-roadmap/

Cloud Security Engineer Roadmap
https://pwnedlabs.io/resources/cloud-security-engineer-roadmap

picoCTF
https://picoctf.org/

TryHackMe
https://tryhackme.com/

Root-Me
https://www.root-me.org/

Resurse educationale

Hack The Box
https://www.hackthebox.com/

RingZer0 Team CTF
https://ringzer0ctf.com/

MetaCTF
https://metactf.com/

SANS Institute
https://www.sans.org/emea

EC-Council
https://www.eccouncil.org/

Offensive Security
https://www.offsec.com/

INE Security
https://ine.com/security

CyberDefenders
https://cyberdefenders.org/

Security Blue Team
https://www.securityblue.team/

CompTIA
https://www.comptia.org/en/