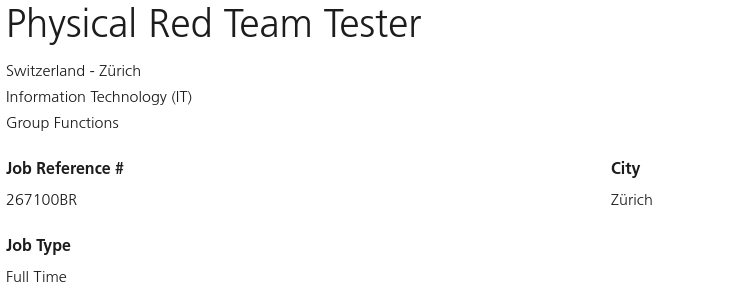
****

**Your role**

Have you successfully participated in a cyber security red team testing service?

Do you understand how red team exercises work?

Are you familiar enough with the tech details to be fluent when meeting with Stakeholders?

This is an excellent opportunity for a strong and forward-looking red teamer (adversary attack simulation) to join a world-class red teaming capability at UBS. The successful Red Team Tester will join a team of testers and will contribute to the bank's efforts in adopting and maintaining a system-wide view of threat-driven risks, with the goal of working with senior management to control these risks.

The ideal candidate will be responsible for executing Red Team Testing activities including security knowledge development under the supervision of a senior Red Team Testing lead. The role will be located in Switzerland and reporting into the global CIS Attack Testing Team, part of the Cyber & Information Security (CIS).

Duties & Responsibilities include:

• Work with Cyber Threat Intelligence function to develop red team scenarios consistent with real attacks as well as business lines understanding their threats

• Work with Security Operations function to ensure a smooth execution of testing activities (e.g. red/purple teaming, competitive cyber games, etc.)

• Plan and execute red-team exercises by replicating, in a safe way, the tactics, techniques and procedures of threat actors, including periodic reporting of progresses to stakeholders

• Develop and submit detailed reports of findings, analysis and recommendations

• Coordinate Red Team operational briefings and presentations to non-technical audience and executive management, as required

• Provide Information and Cyber Security technical expertise to the CIS Attack Testing Team and to the Cyber & Information Security (CIS) function overall.

**Your team**

You will be working closely with the global CIS Attack Testing Team, with presence in Israel, Singapore, Zurich and the US.

**Your expertise**

• At least 6 years of experience with increasing responsibility in Information Technology, Information and Cyber Security and Compliance that includes a combination of hands on/technical and project leadership skills

• Minimum of 4 years’ experience executing penetration testing / red team testing assessments of high-consequence systems (including execution of CBEST/ iCAST exercises and alike)

• In depth knowledge of enterprise architectures and operations

• Detailed and up-to-date knowledge of threat and vulnerability management techniques and tools

• Strong knowledge of e.g. OSI Model, MITRE ATT&CK Framework, Firewalls, IDS/IPS, Web Proxies and DLP amongst other

• Well versed in a wide range of security tools like Burp, Nessus, Metasploit, Empire, Cobalt Strike, etc. and familiarity with common reconnaissance, exploitation, and post exploitation frameworks

• An inquisitive mind and passion for security researching

• Knowledge of exploit crafting/handling/development, malware packing, delivery and obfuscation/evasion techniques

• Ability to automate tasks using a scripting language (Python, Perl, Ruby, etc)

• Strong knowledge of networking protocols and packet analysis

• Able to operate at an advanced level of written and spoken communication in English; write and speak effectively with impact

• Strong project management skills

Desired Background:

• B.Sc. / M.Sc. in Computer Science, Computer Engineering, Information Security or equivalent

• ISC2 Certified Information System Security Professional (CISSP)

• One or More certifications related to Red Team Qualifications / and or Cyber Security such as:

o CREST Certified Simulated Attack Manager (CCSAM) or CREST Certified Simulated Attack Specialist (CCSAS) – Highly preferred

o Offensive Security (OSCE, OSCP)

o CREST Registered Penetration Tester

o GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT)

o Certified Ethical Hacker (CEH)

o CompTIA PenTest+

o GIAC Penetration Tester (GPEN)

o Offensive Security Certified Professional (OSCP)

o Certified Penetration Tester (CPT)

o Systems Security Certified Practitioner (SSCP)

o CompTIA Advanced Security Practitioner (CASP+)

o GIAC Certified Incident Handler (GCIH)

o Certified Information Systems Security Professional (CISSP)

o Certified Information Systems Auditor (CISA)

o Certified Information Security Manager (CISM)

**About us**

UBS is the world’s largest and only truly global wealth manager. We operate through four business divisions: Global Wealth Management, Personal & Corporate Banking, Asset Management and the Investment Bank. Our global reach and the breadth of our expertise set us apart from our competitors.

With more than 70,000 employees, we have a presence in all major financial centers in more than 50 countries. Do you want to be one of us?

**How we hire**

This role requires an assessment on application. Learn more about how we hire: www.ubs.com/global/en/careers/experienced-professionals.html

**Join us**

At UBS, we embrace flexible ways of working when the role permits. We offer different working arrangements like part-time, job-sharing and hybrid (office and home) working. Our purpose-led culture and global infrastructure help us connect, collaborate, and work together in agile ways to meet all our business needs.

From gaining new experiences in different roles to acquiring fresh knowledge and skills, we know that great work is never done alone. We know that it's our people, with their unique backgrounds, skills, experience levels and interests, who drive our ongoing success. Together we’re more than ourselves. Ready to be part of #teamUBS and make an impact?

Link (likely expired): https://jobs.ubs.com/TGnewUI/Search/home/HomeWithPreLoad?partnerid=25008&siteid=5012&PageType=JobDetails&jobid=269951#jobDetails=269951\_5012