

**Your role**

Have you successfully managed and coordinated physical penetration and social engineering exercises?

Do you understand how cyber red team and physical penetration exercises work?

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

This is an excellent opportunity for a strong and forward-looking red team leader (adversary attack simulation) to build a new, world-class red teaming capability with a focus on physical penetration and social engineering at UBS. You will hire a team of physical penetration testers, oversee implementation efforts to deploy the team’s technology stack, and ensure processes are fit for purpose and aligned with business priorities. Your team 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 role will be in the US and reporting into the global head of CIS Offensive Security for UBS, who reports directly to the Cyber & Information Security Officer.

We are looking for a Red Team Tester to:

• lead a world class team of Physical Penetration and Social Engineering testers

• provide oversight for Physical Penetration and Social Engineering test activities

• build relationships and interact with throughout the Business and Technology organizations

• manage highly complex tests, and coordinating with testing counterparts

• train and mentor staff

• work with Cyber Threat Intelligence function to develop red team scenarios that include physical penetration and social engineering components consistent with real attacks

• work with the physical security function to ensure a smooth execution of physical penetration testing activities

• plan and execute physical penetration and social engineering exercises by replicating, in a safe way, the tactics, techniques and procedures of threat actors, including periodic reporting of progresses

• 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 physical penetration and social engineering technical expertise to the CIS Offensive Security Team and to the Cyber & Information Security (CIS) function overall

**Your team**

You will be leading the physical penetration and social engineering aspects of the Offensive Security Team, with a presence in Israel, Singapore, Zurich and the US.

Diversity helps us grow, together. That’s why we are committed to fostering and advancing diversity, equity, and inclusion. It strengthens our business and brings value to our clients.

**Your expertise**

• ideally 15 years of experience with increasing responsibility in Physical Security, Social Engineering, Information and Cyber Security and Compliance that includes a combination of hands on/technical and project leadership skills

• deep knowledge of intelligence gathering methods, the OSINT framework, and familiarity with OSINT-related software

• ideally 8 years’ experience physical penetration testing / red team testing assessments of high-consequence systems

• in depth knowledge of physical security and social engineering subject areas

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

• an inquisitive mind and passion for security researching

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

• strong project management skills

• additionally, some knowledge of the Financial Services would be beneficial

• B.Sc. / M.Sc. in Criminal Justice, Security Management, Computer Science, Computer Engineering, Information Security or equivalent nice to have

• experience at high levels of corporate security and in the intelligence field

• experience with threat research, threat modeling, and information security threat assessments

• experience hunting threat actors

• expert knowledge of cyber security trends, technologies, and their applicability to the financial industry. Experience with security frameworks such as CIS Critical Security Controls, NIST Framework for Improving Critical Infrastructure Security.

\*LI-UBS

\*UBS-MOGUL