What it takes to be a Red Team Leader?

Joas A Santos

https://www.linkedin.com/in/joas-antonio-dos-santos

What is Red Team Leader?

- A Red Team Leader is a professional with great technical capabilities in offensive security and with experience in building a consolidated area and in creating processes and implementing technologies
- Leading the red team activities, improving the team's capabilities, interacting with organizations and advising on their security programs, maturity and outcomes of the red team services as well as coaching and leading the red team members on their assignments, development and growth are all part of a role.
- With a goal to further mature the red teaming capabilities (types of services, way of delivery, automation and customization required per environment etc), you'll keep on top of the constant changing knowledge of threat actors' tactics, techniques and procedures to bring realistic and meaningful solutions to clients. Working with IT security teams, blue teams and other IT stakeholders of the organization to help them utilize your findings and outcomes of your offensive activities to better defend and mature their security stance.

Knowledge required for a Red Team Leader

- Deep technical knowledge in offensive security activities, whether in PenTest, social engineering campaigns, adversary emulation and other Red Team activities;
- Experience building processes and complying with well-known security standards such as NIST, PCI, HIPAA, GDPR/LGPD, ISO 27001 and others;
- Experience and mindset in creating attack scenarios and developing TTPs, being inside frameworks and methodologies such as Miter Att&ck and Cyber Kill Chain;
- Ability to stay up-to-date on market trends and existing threats in the cyber world;
- Understand the defensive side and know the main solutions and processes used in the market;
- Good communication, writing and ability to work in a team, manage projects and create internal processes;

Responsibilities of a Red Team Leader

- Define internal and external Red Team procedures;
- Create a Red Team culture within the organization, collaborating with other teams on offensive security activities;
- Develop an operational support plan with KPIs, KRIs and other insights;
- Collaborate with the development of your team, both in training and in the personal development of each professional on the team;
- Lead technical discussions to improve security controls and present non-technical information to senior management;
- Guide in the deployment and management of implemented Red Team solutions, such as creating processes, playbooks, runbooks and providing support;
- Improve internal offensive security programs, in addition to creating recurring test plans such as Adversary Emulation and PenTest;

What makes a Red Team Leader different?

- Soft skills are important, knowing how to communicate, transmitting your knowledge to technical and non-technical people;
- Having a market vision is important, knowing the solutions sold both for Red Team and for other segments;
- Good technical skills, not necessarily being a complete expert in each domain, but understanding the fundamentals to manage, design and improve;
- Certifications are important, not only technical, but if possible those aimed at management as well, having both views is important for your personal development and that of your team;
- Knowing opponent behaviors and mapping them is important. Making contributions like this will increase your maturity, the maturity of your team and your organization;
- Analytical skills, programming knowledge and a business vision are differentials that will help immensely;

The role of a red team leader towards his team

Your team is fundamental, especially in the execution and delivery of specific and recurring activities, so consider some points to engage your team even more.

- Develop a collaborative culture, a space where knowledge can be shared and exchanged, whether in the creation of a knowledge base or in weekly meetings;
- Encourage participation in CTFs, Annual Challenges from certifying companies, report CVEs, contribute to a project and create internal challenges to engage the team;
- Talk to senior management to have that budget to obtain certifications that will make a difference in the lives of each one of your team, in addition to incentives in studies such as bonuses or any type of award that is possible;
- How about creating an internal event to exercise your team's softskill? Lectures and even training for employees of different types of knowledge and technical level;
- Coordinating the team in technical activities is important, but understanding the needs and impediments will generate trust, which is why communication is the key word, fundamental for any area;
- Feedback processes, recommendations, and even one-on-one chats are helpful. Especially in an era where many professionals are suffering from burnout;

Conclusion

- In summary, being a Red Team leader means having good technical skills, being able to manage offensive security projects and having excellent communication with internal and external people;
- Always be engaged in what is happening in the market and always propose new solutions to improve the company's security controls;
- Have a collaborative and people-oriented sense to understand the needs of your team, in addition to providing solutions that will be good for both parties;
- Finally, developing processes and the ability to report, generate indicators and create an area that is worth sustaining, in order to achieve a larger budget next year;