OUTFLANK

clear advice with a hacker mindset

Enhancing Red Team Efficiency

- **Meeting Growing Demand:** The demand for red team activities is steadily increasing as organisations recognize the importance of cybersecurity.
- **R&D Talent Challenge:** Finding individuals with the unique combination of red teaming experience and software development expertise is a significant challenge in today's competitive job market.
- **High Hiring Costs:** To secure such talent, Company A might need to allocate substantial budgets, potentially exceeding $250,000 in salary depending on the region and experience level.
- **Productivity Limitation:** Even after hiring, in-house R&D teams face inherent limitations, producing only a few tools each year due to the complexity of their work. Outflank OST had 26 releases in 2023.
- **Solution: Outflank OST's R&D Outsourcing:** Outflank OST offers an innovative solution by completely outsourcing R&D, allowing us to overcome these challenges efficiently.

OUTFLANK

clear advice with a hacker mindset

Benefits of Outflank OST

- **Stealth & Evasion:** By outsourcing R&D to Outflank OST, we empower our red team to maintain a high level of stealth and evasion during engagements. This is critical for avoiding detection by Endpoint Detection and Response (EDR) and antivirus tools.
- **Increased Firepower:** Our team can punch above our weight by leveraging OST's external development power. The OST toolkit provides our team with shortcuts for hard stages like initial access, EDR evasion, and OPSEC-safe lateral movement. OST also includes techniques that have not yet been published or weaponised by other solutions or services.
- **Cost-Efficiency & Scalability:** OST is continuously updated with new offensive techniques and procedures by a team of ethical hackers and developers. This minimises the costs associated with hiring and maintaining in-house specialists, ensuring cost-efficiency. Moreover, it offers scalability, allowing us to meet the increasing demand for our red team services without overburdening our organisation.
- **Quantifiable Time Savings:** Recent client analysis demonstrates substantial time savings, with individual red team members reducing preparation time by over 50% per engagement cycle, leading to increased productivity.
- **Competitive Edge:** Embracing Outflank OST positions Company A as a pioneering leader in the red teaming space, enhancing our reputation and attractiveness to clients.
- **Risk Mitigation & Client Satisfaction:** By investing in Outflank OST, we mitigate the risks associated with in-house talent turnover and knowledge gaps, leading to consistently high-quality services that result in greater client satisfaction.
- **Strategic Long-Term Investment:** Outflank OST represents a strategic long-term investment in our red team capabilities, ensuring our readiness to meet evolving client needs and maintain our industry leadership.
- **Education For Your Red Team:** OST is continuously updated with the latest offensive techniques by the seasoned professionals at OST who are dedicated to rigorous R&D, allowing our red team to deploy elite, realistic engagements that help our clients stay one step ahead of adversaries. Along with these regular updates and extensive documentation, our users have access to a private Slack community monitored by OST developers for support and knowledge sharing with other users.

Why Choose Outflank Security Tooling (OST)?

The benefit of expert tools and ongoing research for a fraction of the cost

OUTFLANK

clear advice with a hacker mindset

*The **OST toolkit** enables your red team to perform dynamic engagements with evasive adversarial techniques that will challenge and prepare blue teams for today's skilled attackers. With OST you are not only purchasing the current toolkit, you also get exclusive access to new tools that incorporate ongoing research. By leaving research and development needs up to the Outflank team, advanced red teams can save time and reduce costs and still benefit from cutting edge tools that help simplify complex tasks and evade modern day EDRs.*

What is OST?

Outflank Security Tooling (OST) is a set of offensive security tools created by the specialists of Outflank that they use in their operations, covering every significant step in the attacker kill chain. In addition to the well-documented toolset, users also get access to an active community of vetted red teamers that share knowledge and tradecraft.

Who is Outflank?

Every member of the Outflank team has over a decade of red teaming experience and hold industry certifications such as CISSP, OSWP, CISA, OCSP, and more. Known for their advanced operations, the team has spent years developing this innovative toolset to complement their expertise.

What types of tools are included with OST?

OST regularly adds new tools to provide the most effective solution possible. A sample of the current tools include:

- The **Office Intrusion pack** and the **Payload Generator** can be used for mimicking the strategic, stealthy breaches of advanced attackers, giving clients a realistic experience of spear phishing.
- **Sharpfuscator** and the **Stage1 implant** will help the team to establish and maintain a position on an infected machine while combining careful recon with novel evasive techniques that minimize the chances of being detected in this phase.
- **Lateral Pack**, **Credential Pack** and the various **BOF packages** will support teams in obtaining a position in the network by performing state-of-the-art lateral movement in **Cobalt Strike** or **Stage1**.
- The completion of simulations can also be enhanced with **FakeRansom**, which provides the shock effect of a full-blown ransomware attack without the actual risk of data loss.

Alongside all these tools, the documentation, the community and private slack channels are available to ask questions and gather the knowledge needed and periodic knowledge sharing by the Outflank team, where they share private tradecraft.