FORTRA®

DATASHEET

Red Team Suite

Cobalt Strike and Outflank Security Tooling (OST)

Cobalt Strike and Outflank Security Tooling (OST) are two red teaming solutions that enable operators to execute the diverse and varied tasks that each engagement requires. Cobalt Strike provides post-exploitation capabilities through its Beacon payload and malleable C2 framework, while OST is a curated set of offensive security tools that covers the full attack chain with emphasis on evasion techniques.

While both platforms operate as sophisticated standalone solutions, OST was developed to work in tandem with Cobalt Strike, extending the reach of both tools and enabling enhanced capabilities during operations. The Red Team Suite takes this partnership further by adding exclusive resources designed to keep red teams at the leading edge of offensive security.

Coordinating Red Teaming Tools for Advanced Engagements

Cobalt Strike's highly flexible command and control directly integrates with OST's end-to-end toolset through Beacon Object Files (BOFs) and reflective DLL loading techniques, adding functionality like:

- **Session Management:** Operators can leverage session passing between platforms, enabling seamless transitions between OST's initial access tools and Cobalt Strike's post-exploitation framework.
- **Centralized Testing Environment:** The combined architecture enables advanced post-exploitation tasks while maintaining operational security through tested and validated tool interactions.
- **Cohesive Portfolio:** Organizations improve efficiency not only with solution interoperability and centralization, but also by having a single point of contact for support of their offensive security strategy.
- **Boosted Payloads:** Red teams can simplify operations and augment Beacon payloads with OST's customized User Defined Reflective Loaders (UDRLs) and sleep masks.

Evasive Red Teaming: Technical Use Cases

Combining OST and Cobalt Strike enables red teams to run advanced attack simulations designed to bypass defensive measures and detection tools with ease.

- **Advanced Payload Operations:** OST's Payload Generator enhances Cobalt Strike's capabilities with additional anti-forensic features and evasion techniques for improved OPSEC during operations.
- **Covert Initial Access:** Outflank C2, staying under the radar of antivirus and EDR software during the initial access phase, enables operators to use session passing to quietly transition to Cobalt Strike for post-exploitation activities.
- **Enhanced Movement:** ShovelNG, a lateral movement toolkit for remote code execution, incorporates specialized techniques for moving undetected throughout the targeted environment and is easily integrated into Cobalt Strike using BOFs.
- **Full System Access:** Hidden Desktop, which enables a full, non-intrusive take over the desktop of a target user (including use of applications and hardware tokens), can be covertly deployed through Cobalt Strike with a custom implementation of "Hidden VNC."
- **Extended Capabilities:** OST 's collection of BOF capabilities for extending Cobalt Strike includes Kerberos interaction, novel coercion techniques, O365 token extraction, and more.

ADDITIONAL PRODUCT FEATURES

Empowering Operators with Cobalt Strike

Cobalt Strike enables security professionals to simulate the tactics and techniques of a long-term embedded attacker in an IT environment. Features include:

- **Versatile Post-Exploitation:** Beacon, Cobalt Strike's signature payload, can be deployed to quickly expand access and maintain persistence by completing tasks like gathering information, executing commands, and deploying additional payloads.
- **Flexible Framework:** The malleable C2 framework allows operators to tailor engagements to suit each unique environment through C2 profiles, UDRLs, sleep mask kit, mutator kit, and more.
- **Community-Driven Extensions:** The Community Kit provides a curated repository of over 100 user-developed extensions, including custom BOFs, aggressor scripts, and post-exploitation modules.

Prioritizing Stealth with OST

OST is a toolkit for red teamers by red teamers, built for performing in mature and sensitive target environments to efficiently simulate techniques currently used by APTs and other cyber attackers.

- **Attack Chain Coverage:** Innovative research and a rapid development pace ensures operators are using cutting edge techniques, with over 30 purpose-built tools for initial access, lateral movement, privilege escalation, and exfiltration phases.
- **Unique Evasion Tactics:** OST tools prioritize advanced anti-forensic techniques and EDR bypass capabilities, including unpublished techniques to avoid detection.
- **Advanced Tradecraft Education:** Exclusive technical deep dives cover OFFSEC topics including EDR evasion methodologies, Windows Kernel Driver manipulation, Azure AD attack vectors through ROADtools, and Office Security.

Exclusive Access to Cobalt Strike Research Labs

The Red Team Suite offers access to Cobalt Strike Research Labs (CSRL), an advanced development initiative that produces specialized offensive tools unavailable through standard product licenses.

CSRL works on advanced capabilities designed to emulate evolving attack strategies, releasing tools and techniques that help red teams attain operational effectiveness against modern defensive technologies. This output is built to be integrated directly into existing Cobalt Strike workflows, providing operators with enhanced evasion and novel attack techniques.

Users of this Suite also join a private Slack community connecting practitioners with the development team and peer operators, creating opportunities to exchange ideas and influence future development priorities.

Certified Operator Training

The Red Team Suite includes Cobalt Strike Certified Operator (CSCO) training, developed in partnership with Zero-Point Security to deliver expert guidance on using Cobalt Strike for adversary simulations.

The training program provides detailed overviews of both fundamental concepts and advanced workflows. Each learning module pairs instructional materials with hands-on labs, allowing operators to build practical skills in a guided environment.

CSCO training is designed to benefit both security professionals new to Cobalt Strike and experienced practitioners seeking to strengthen their operational foundations. The self-paced, on-demand format allows teams to learn at their own speed while immediately applying new techniques to real-world assessments.

Request Custom Pricing for Red Team Suite at Cobaltstrike.com

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.