FORTRA.

Offensive Security Suite
Core Impact, Cobalt Strike, and Outflank Security Tooling (OST)

Fortra's Offensive Security Suite is comprised of three distinct enterprise-grade tools: Core Impact tests exploitation paths and lateral movement, Cobalt Strike enables advanced adversary tactics for Red Team operations, and OST provides a broad arsenal for evasive attack simulation. Additionally, this suite provides exclusive Cobalt Strike Research Labs access plus operator training.

Ideal for dynamic proactive assessments, each solution delivers specialized attack capabilities while combining seamlessly to efficiently test defenses, validate exploitability, and emulate sophisticated attacks even in mature, high-security environments.

Layered Security: Integrations and Interoperability

The Offensive Security Suite maximizes attack potential through interconnected platforms and mutual resources, expanding testing capabilities through additional functionality like:

- **Strategic Attack Framework:** Leverage Cobalt Strike's malleable framework, Core Impact's systematic, automated testing, and OST's research-driven, cutting edge evasion techniques.
- **Unified Operations:** Enable interaction through session passing and tunneling capabilities, Outflank C2 deployment, and cross-platform session passing.
- **Enhanced Adversary Simulation:** Extend reach of engagements through shared BOFs, reflective DLL loading, and OST's payload obfuscation techniques.
- **Single-Vendor Portfolio:** Get centralized technical support for all three solutions to eliminate multi-vendor coordination issues.

Offensive Security Suite Advantages

Beyond Core Impact, Cobalt Strike, and OST, the Offensive Security Suite provides:

Cobalt Strike Research Labs

- Exclusive Research Output – Cutting edge offensive capabilities designed to bypass contemporary defensive measures and replicate current threat actor techniques
- Community Collaboration – Private Slack workspace connecting you with other red team operators
- Documentation and Guidance – Comprehensive knowledge base covering implementation and operational use cases
- Ongoing Innovation – New releases delivered as threats and defenses evolve.

Operator Training Offerings

- Multi-Platform Curriculum – Both Cobalt Strike Certified Operator (CSCO) and Core Impact Certified Operator (CICO) training.
- Progressive Skill Development – Begin with platform fundamentals and workflows and advance into complex customization, with new training content added to keep capabilities current.
- Adaptable Training Schedule – Asynchronous delivery enables teams to complete coursework when it fits their operations.

Penetration Testing with Core Impact

Core Impact validates vulnerabilities across networks, applications, and endpoints with automated exploitation capabilities to effectively prioritize risk. Key features include:

Exclusive Crafted Exploits: Leverage an expert-validated exploit library that is regularly tested and updated for modern platforms and applications.

NTLM Relay Attacks: Trigger system authentication with Coercer module, then use NTLMrelayx to redirect connections for automated agent deployment, certificate generation, LDAP queries, and more.

Ransomware Simulation: Evaluate security controls by paring phishing capabilities with the ransomware simulator, which mimics multiple ransomware families to encrypt files.

Compliance Documentation: Generate detailed technical reports to help plan remediation and prove adherence to industry requirements and government regulations, like PCI DSS, GDPR, HIPAA.

Advanced Threat Emulation with Cobalt Strike

Cobalt Strike enables adversary emulation through its post-exploitation framework and covert communication channels. Key capabilities include:

- **Advanced Post-Exploitation:** Deploy Beacon, Cobalt Strike's signature payload, to gather information, execute commands, move laterally, elevate privileges, and more.

- **Flexible Framework:** Customize operations using malleable C2 profiles, UDRLs, sleep masks, and tailored scripts to mimic advanced attackers.

- **Community-Driven Extensions:** Leverage 100+ user-developed tools from a curated library, including custom BOFs, aggressor scripts, and post-exploitation modules.

- **Team-Based Operations:** Coordinate red team activities through team servers with shared access to compromised systems and collected data.

Evasive Attack Simulation with OST

OST is a red team toolkit engineered by active practitioners to simulate sophisticated APT techniques and evasive tradecraft in mature, security-hardened environments. Key features include:

Advanced Evasive Movement: Avoid detection using the most up-to-date research and technology for bypassing defensive measures and solutions like EDR and antivirus.

Multi-phase Tools: Accelerate operations through purpose-built tools for access, evasion, and covert lateral movement.

Rapid Expansion: Take advantage of cutting-edge techniques, as OST continuously evolves through expert-driven research and regular tool releases.

Tradecraft and Community: Get exclusive access to regular tradecraft sessions and a forum for OST users to discuss attack strategies and methodologies.

Get custom pricing for the Offensive Security Suite at **Cobaltstrike.com**

FORTRA®

Fortra.com