FORTRA®

DATASHEET (OFFENSIVE SECURITY)

Elite Bundle

Fortra's Elite Offensive Security Bundle is comprised of three distinct enterprise-grade tools: Fortra VM scans networks for vulnerabilities, Core Impact pen tests exploitation paths and lateral movement, and Cobalt Strike simulates advanced adversary tactics for Red Team operations.

Ideal for proactive security testing, each solution excels independently while uniting effectively to serve different aspects of the security assessment lifecycle to fully manage an infrastructure's attack surface.

Layering Security: Integrations and Interoperability

With the combination of scanning, testing, and attack simulation tools into a connected security testing workflow, additional functionality includes:

Progressive Testing Process: Each tool's data informs the others, validating and advancing assessments: Fortra VM scans detect weaknesses, Core Impact validates exploitability, and Cobalt Strike tests defensive responses.

Technical Integration: Core Impact imports Fortra VM scan results directly while maintaining bi-directional communication with Cobalt Strike through session passing and tunneling capabilities.

Shared Resources: Common modules and extensions reduce complexity, increase efficiency, and enhance testing workflows.

Single-Vendor Support: Centralized technical support handles all three solutions, eliminating multi-vendor coordination issues.

Additional Product Features

Rapid Risk Discovery with Fortra VM

Fortra VM is a cloud-native, vulnerability management SaaS solution that provides network security assessments that detect weaknesses, prioritize risks, and track remediation. Key features include:

- **Intelligent Scanning:** Perform automated scans that utilize both external data and proprietary technology for vulnerability discovery, identification, and remediation management.
- **Compliance Auditing:** Execute CIS Benchmark scans to validate system configurations against industry-standard security controls and compliance requirements.
- **User Accountability:** Implement role-based access control and data segmentation for precise user permission management and information compartmentalization
- **Reporting:** Swiftly create targeted reports using template selection and data filtering.

Automated Penetration Testing with Core Impact

Core Impact automates repetitive and time-consuming pen testing tasks to enable efficient exploitation of security weaknesses associated with networks, people, web applications, endpoints, Wi-Fi, and SCADA environments. Key features include:

- **Rapid Pen Tests:** Use step-by-step Rapid Penetration Tests (RPTs) to discover, test, and report all in one place, optimizing the use of your security resources.
- **Core Certified Exploits:** Leverage an expert-maintained exploit database, continuously tested and updated with new exploits for different platforms, operating systems, and applications.
- **Clean-Up:** Deploy Core Agents, binary implants injected into the memory or file system of a targeted or compromised remote host, with automated cleanup functionality to prevent unauthorized post-test access.
- **Reporting:** Generate detailed reports to support remediation efforts and prove compliance for regulations like PCI DSS, GDPR, and HIPAA.

Advanced Red Teaming with Cobalt Strike

Cobalt Strike is a threat emulation tool that provides a post-exploitation agent and covert channels, replicating the tactics and techniques of an advanced adversary in a network. Key features include:

- **Post-Exploitation Agent:** Deploy Beacon, Cobalt Strike's post-exploitation payload, to execute advanced adversary tactics including gathering information, run commands, and deploying additional payloads.
- **Flexible Framework:** Adapt Cobalt Strike into a tool that suits your needs, with tailored scripts, C2 profiles, UDRLs, sleep mask kit, mutator kit, and more.
- **Community-Driven Extensions:** Utilize the Community Kit, a curated repository of over 100 user-developed extensions, including custom BOFs, aggressor scripts, and post-exploitation modules.
- **Collaborative Operations:** Centralize red team operations through team servers, allowing shared control of compromised systems and access to sessions, host data, and exfiltrated files.

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.