FORTRA

DATASHEET *(Cybersecurity)*

Fortra Penetration Testing Services

Infrastructure Protection Services by Trusted Cybersecurity Experts.

Trusted by clients for more than 35 years, the security services teams at Fortra is composed of experienced, certified cybersecurity professionals who deliver expert security assessments and penetration testing services. Our expert-led tests use the latest ethical hacking tactics to find security gaps and potential attack paths, helping you shore up weaknesses and adhere to compliance standards.

Select the Right Security Service to Meet Your Needs

We know each organization has unique security objectives, and we strive to tailor our services to meet your needs. We offer one-time and recurring service engagements which can be customized for your specific environment. Whether you need a basic pen test or a complex engagement with sophisticated attack emulation, the Fortra team can provide the right level of services.

Penetration Test Types

Pen tests are ideal for evaluating the resilience of your organization against real-world attacks. Pen testing reports are also commonly used to demonstrate compliance to industry regulations.

Our testers will find and exploit vulnerabilities while challenging security controls in your infrastructure to get access to privileged systems and information with the goal of determining and prioritizing risk. Upon completion of a pen test, you will receive a full report specifying attack paths and proposals for remediation.

Network Security

Using internal penetration testing or external penetration testing, our certified testers will uncover vulnerabilities that may exist in your internal or external networks, as well as associated devices like routers and switches, and network hosts. Fortra's pen testers will exploit flaws in these areas, like weak passwords or misconfigured assets, in order to gain access to critical systems or data.

Application Security

Web Applications: Adhering to the OWASP Application Security Verification Standard, pen testers identify weaknesses in web applications through tailored evaluations and detailed source code inspection.

Mobile Applications: Our pen testers use OWASP Top 10 for Mobile Risks as a standardized approach based on the most prevalent mobile app risks, such as improper credential usage and inadequate supply chain security.

Application Programming Interface (API): APIs are another top application target, and the OWASP Top 10 for API Security Risks helps pen testers identify security misconfigurations, improper inventory management, and other major API security weaknesses.

Remote and On-Site Social Engineering

Using phishing test tools, tailored emails, phone calls, USB device delivery, and more, remote pen testers will assess the detection and reaction capabilities of your employees to find susceptible individuals and

defensive security measures that need improvement. On-site social engineering pen testers pose as visitors, vendors, or employees to attempt entry to restricted areas, revealing the effectiveness of on-site security measures.

IoT Security

With the vast world of IoT, pen testers will tailor each assessment to the specific device, which may include threat modeling, hardware and firmware analysis, or source code review.

Red Team Exercise Types

Red team exercises fully simulate a cyberattack to help measure how effectively your organization can detect, defend, and withstand threats by malicious actors. Our red teamers use the latest tools and methods real hackers use to evade detection while discovering exploitable areas of the network, applications, credentials, and devices. Upon completion of a red team project, you'll receive a thorough report detailing their findings, as well as suggestions for closing security holes uncovered during the exercise.

Red Teaming

These engagements deploy the tried-and-true red teaming playbook to evaluate the strength of your organization's security posture. First, red teamers will attempt to gain initial access via phishing attempts and direct attacks on external systems. They will then function as embedded adversaries in internal networks, and lastly, they will try to copy and exfiltrate sensitive sample data to see if your organization's data loss prevention solutions can be bypassed.

Control Verification

These high-level engagements validate standard security controls within your organization's network. The red team will use various tools to run a breach and attack simulation in order to verify that security tools are working.

Purple Teaming

For these engagements, in addition to infiltrating and testing the environment, the red team will also serve as trainers for the internal blue team. Our offensive experts can run through different tactics, demonstrate evasions, and make recommendations on where your organization should bolster defenses.

Adversary Simulations

The red team will be given access to simulate an active intrusion, executing an objective focused attack chain to challenge the blue team's reactions to a live, adaptive adversary emulating the actions of real-world entities such as nation state threat actors or ransomware gangs. This allows for blue teams to test and identify potential gaps in their security strategies and processes.

Black Box Testing

Black Box tests are a full scope exercise that provide an end-to-end attack scenario. These comprehensive engagements are ideal for assessing the maturity of your organization's security program, providing a thorough picture of adversarial efforts, exposing potential gaps in both active and static defensive strategies.

To determine the scope for your testing projects, please contact us.

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.

