FORTRA

DATASHEET *(Cybersecurity)*

Security Consulting Service

Infrastructure Protection Services by Trusted Cybersecurity Experts.

Trusted by clients for more than 35 years, our Security Consulting Services (SCS) deliver expert security assessments, penetration tests, and red teaming exercises. SCS assists in improving your security stance and reducing your risk with program offerings and tests that find security gaps, help you adhere to compliance standards, train security operations, and secure IT assets. . The SCS team is composed of experienced cybersecurity professionals, specializing in security exercises that help your organization protect itself from real world attackers.

Services Offered

Infrastructure Security Testing

Pen tests are ideal for evaluating the resilience of your organization against real-world attacks and are commonly used to demonstrate compliance to industry regulations. Our testers will find and exploit vulnerabilities while challenging access controls in your infrastructure to get access to privileged systems and information in order to determine and prioritize risk. Upon completion of a pen testing project, you will receive a full report specifying attack paths and proposals for remediation.

Red Team Exercises

Red Team exercises fully simulate a cyber-attack scenario to help measure how effectively an organization can detect, defend, and withstand cyber threats by malicious actors. Our Red Teamers use all the industry leading 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.

Application Security Testing

Our consultants will evaluate the security of desktop, mobile, or web applications from an attacker's perspective. Ideal for applications in development or prior to its latest release, these tests use real-world strategies, targeting coding errors, broken authentication or authorization, and injection vulnerabilities. In addition to dynamic testing, experts can further evaluate applications by performing source code audit of new or existing applications. Upon completion of an application security test, you'll receive a complete report with suggestions to further harden your applications.

Select the Right Security Service to Meet Your Needs

We know that each organization has unique security objectives, and we strive to tailor our services to meet your needs. We offer customized service engagements unique to your specific environment, whether it be a basic pen-test or a complex engagement with sophisticated attack emulation.

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

Penetration Test Types

Network Security

Testers will uncover vulnerabilities that may exist in either your internal or external networks, as well as associated devices like routers and switches, and network hosts. SCS pen testers will exploit flaws in these areas, like weak passwords or misconfigured assets, in order to gain access to critical systems or data.

Web Application

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

Social Engineering

Using phishing test tools and emails tailored to your organization pen testers will assess the detection and reaction capabilities of your employees to find susceptible individuals, as well as defensive security measures that need improvement.

Cloud Security

Working with cloud providers and third-party vendors, pen testers will validate the security of your cloud deployment, identify overall risk and likelihood for each vulnerability, and recommend how to improve your cloud environment.

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

Control Verification

These high-level engagements validate standard security controls within an 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 the organization should bolster defenses.

Adversary Simulations

The Red Team will be given access to simulate an active intrusion, executing an objective focused attack chain in order to challenge the Blue Team's reactions to a live, adaptive adversary. 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 an organization's security program, provide a thorough picture of adversarial efforts, exposing potential gaps in both active and static defensive strategies.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.