DATASHEET

NSFOCUS

NSFOCUS SAS

Build Resilient Security Over Your 5G Networks to Protect Against Threats Both Predictable and Unpredictable

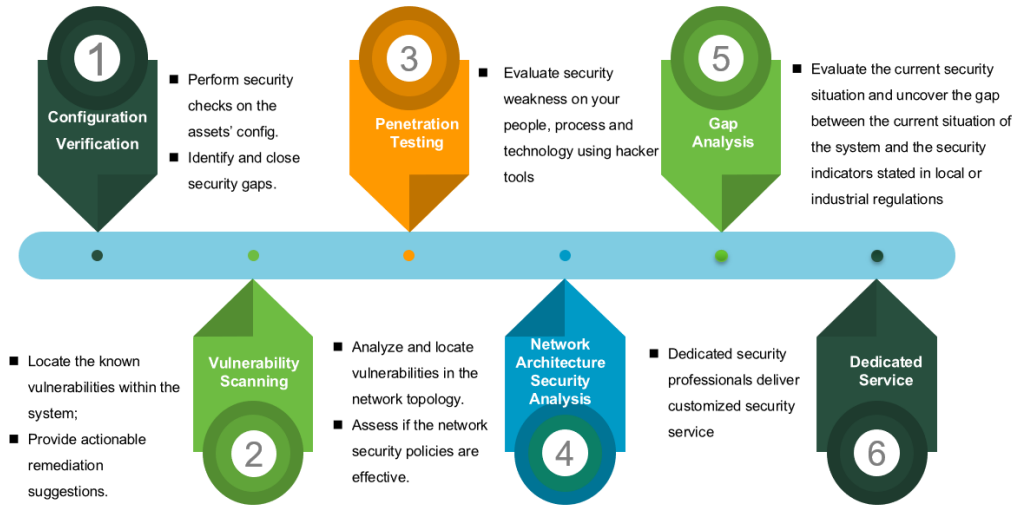
The Covid-19 pandemic has accelerated the organization's progress of hybrid work and the shift to the cloud, which poses challenges for the chief information security officers to secure an increasingly distributed environment. An organization cannot handle vulnerabilities, weak points, or defects effectively and efficiently if they are unaware or invisible.

Meanwhile, vulnerabilities discovered or disclosed daily in operating systems, networking devices, applications, middleware, databases, and protocols overwhelm your IT professionals. It's a big challenge for organizations to keep pace with the increasing number of attacks and sophisticated attack vectors if they lack security professionals or expertise. As a result, many organizations suffer from denial of service attacks, web and application threats, or data breaches from time to time, leading to enormous reputational and economic loss.

Dedicated to identifying the flaws, defects, and weaknesses across your IT environment, NSFOCUS Security Assessment Services provide complete visibility of your current security status and guide you to enhance your security posture.

A Complete Set of Security Service Portfolio

No matter what industry you are in, how complicated security threats you encounter, and what regulations you need to meet, you can always find an answer in our broad security service portfolio. The Security Assessment Security Services encompass configuration verification, vulnerability scanning, penetrating test (Lite, Standard, and Red team & Blue team), network architecture security analysis, and dedicated service.



KEY BENEFITS

Identify risks, improve security posture, and protect valuable assets with actionable fix suggestions

Lite PenTest is quick and friendly to low-budget organizations

Clear reports facilitate your vulnerability remediation process

Up-to-date vulnerability database and global threat intelligence empower emerging threats discovery

Flexible subscription plans to satisfy your personalized demands

Cost-effective security service with no hardware, license, or personnel required.

World-class security research labs with 200+ full-time security experts specializing in cloud computing security, IoT, IoV, industrial internet, AI-based defense technologies, big data, and offensive and defensive drills

Comprehensive security qualifications like ISO, GDPR, CNVD, CCIE, Security+, CISSP, OSCP, CCSC, CCSP, CISSE, and CCSRP

Values of NSFOCUS Security Assessment Services

Reduce Security Risks

With the security assessment service, we can identify any security hole in your entire digital environment by using NSFOCUS web vulnerability scanner combined with third-party open-source tools. The scanning scope includes your intranet, external network, web and mobile applications, security devices, secure configurations, employee security awareness, and more. All risks are prioritized to ensure you can fix the most critical ones effectively.

Flexible Solution

NSFOCUS provides flexible solutions to meet different requirements.

- Lite PenTest is tailored for organizations that want to get the assessment done in a short period with a limited budget.
- Standard PenTest is for organizations that want to dig deeper into security problems and enhance security posture to address severe security threat challenges or strict regulatory compliance.
- Red Team & Blue Team, performed by NSFOCUS PenTest experts, aims to find as many security threats as possible by simulating adversary actions. A red team poses as a group of cybercriminals attempting to breach your security mechanism. A blue team, on the other hand, is a security team that monitors your assets, identifies security threats, and recommends remediation plans to stop adversary actions.

Enhance Your Cybersecurity Posture

We can enhance your cybersecurity posture by:

- Evaluating the effectiveness of your deployed security controls, processes, and people when facing real-world security threats;
- Exposing vulnerabilities and weaknesses that seriously impact your business availability; and
- Providing actionable advice to enhance your cybersecurity posture.

Meet Regulatory Compliance

Increasing regulations and standards from governments and supervisory authorities require customers to comply with, like GDPR, PCI-DSS, and ISO 27001, to name a few. The Security Assessment Services help you identify defects that may violate compliance requirements. Comprehensive security reports present detailed risk descriptions, potential impact, and hardening suggestions to facilitate your regulation process.

Why NSFOCUS Security Assessment Services?

CREST-Accredited Vulnerability Assessment and Penetration Test Services

When buying any professional service, organizations need assurances that the supplier they engage is reputable, trustworthy, and competent. Clients of CREST members will receive high-standard services that are quality assured by CREST's rigorous quality assurance process and internationally-recognized security testing methodologies.

Standard Testing Process

To guarantee service delivery quality, we follow a standard process to conduct security testing:

- In the planning stage, we discuss requirements with the customer in detail. Define test scope, and develop an implementation plan accordingly. Then, sign an NDA agreement, obtain authorization from the customer, and guide the customer in preparing the test environment.
- In the implementation stage, we conduct the test on the targets and identify and exploit vulnerabilities. Meanwhile, collect data, analyze results, and generate test reports.
- Schedule technical meetings to explain test results and recommendations that can guide you to fix the vulnerabilities.

- After you confirm that you have already fixed the vulnerabilities, we carry out a re-testing to verify whether the vulnerabilities are fixed effectively or not.
- Before project closure, we will clean up the environment and ensure no related data are retained in any of our storage media, appliances, or platform.

Service Availability Assurance

To ensure that the customer's system runs stably and securely during testing, we endeavor to avert risks and incidents through:

- Object Selection
- To minimize risks and incidents, we tend to carry out the test on the backup system because there are few differences between the backup system and the live system in the installed applications and carried data. Moreover, the backup system is less demanding for stability.
- Time Control
- To minimize the workload on the test system, we will perform tests during off hours.
- Technical Means
- Before each step, we will estimate the possible impact, record, and skip any action that may have a negative effect. Then we carry out the step with your approval.
- Monitoring Measures
- Before each test, we will notify the system owner so that they can closely monitor the workload of the target system and stop testing immediately when any exception occurs.
- Use of Tools
- We will try to alleviate the system's workload by setting parameters such as the number of threads and plug-ins. We will also remove any plug-ins that may harm the target system.

INQUIRIES AND ORDERS

https://nsfocusglobal.com/contact-us/

Asia Pacific: apmarketing@nsfocusglobal.com

Latin America: contato@nsfocusglobal.com

Greater China: gcrmarketing@nsfocusglobal.com

Other Regions: bd@nsfocusglobal.com