DATASHEET

NSFOCUS

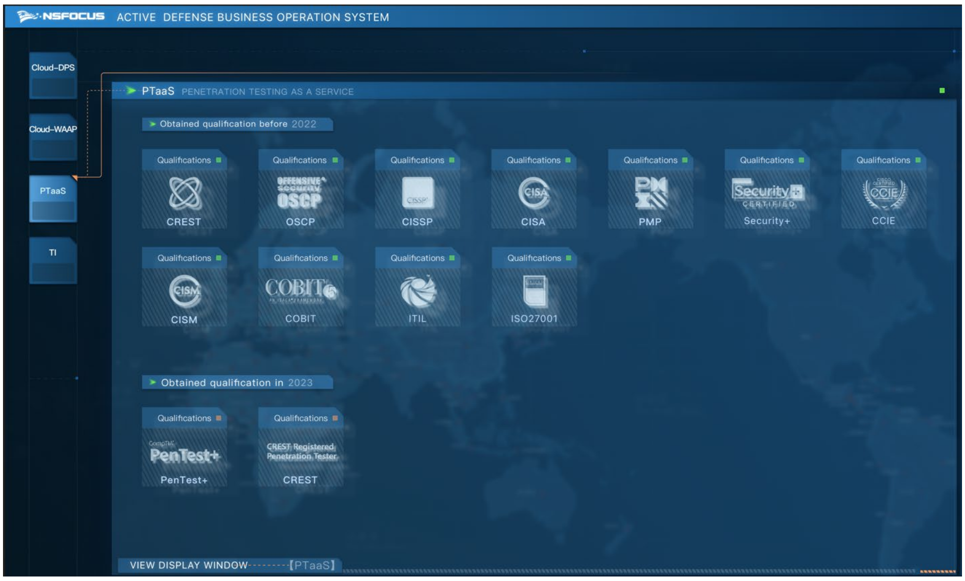
NSFOCUS PTaaS

NSFOCUS SECURITY SERVICE

OVERVIEW

The conventional process of conducting penetration testing is no more capable of keeping pace with the fast-moving nature of agile development. On top of that, performing manual pen-testing is costly in terms of resources, time, and money, while automated scanners produce many inaccurate results, leading to wasted time.

Powered by NSFOCUS SAAS Platform-ADBOS, NSFOCUS Penetration Testing as a Service (PTaaS) is a more efficient and cost-effective solution for organizations. It accelerates the process of pen-test project, provides in-depth assessment for testing targets to evaluate security status.



NSFOCUS PTAAS COVERS:

- Web, mobile application, and API
- IOT, Cloud, Desktop
- Network, WiFi, Red Teaming
- OWASP TOP 10
- Business logic vulnerabilities
- Compliance framework support for ISO, PCI, CREST, NIST, ISSAF, and more.

KEY BENEFITS

Fast

Schedule a pen-test project and retest faster than ever, even in the same business day

Real-time visibility

Get the latest updates at the earliest possible time. No waiting for the final report to start the remediation process.

Professionalism

Security experts with different skillsets and certificates such as OSCP, CREST, CEH, CISSP, Security+ can provide in-depth assessment results.

Data Analysis

NSFOCUS PTaaS analyzes the testing data, helps user know where to focus more of attention and provides valuable insights from multiple perspectives.

Access to security experts

Fixing vulnerabilities can be tricky. NSFOCUS security experts who are experienced in security field are ready to help.

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

NSFOCUS PTAAS LIFECYCLE

Plan

Define the scope of work, project requirements and preferred time slot to carry out the test.

Onboard

NSFOCUS will assign a dedicated project management to ensure the project can be implemented smoothly and successfully to reach the agreed goal. During this stage, NSFOCUS will work with you to set up the test environment, define the scope of work, and nail down the project implementation timeline.

Test

Security experts will be assigned to the project based on project requirements and individual skillsets. A variety of testing methodologies will be used to ensure no stone is left unturned. Issue found during the test will be updated to the platform in real-time to ensure corresponding teams can access the issue detail in the earliest possible.

Remediate

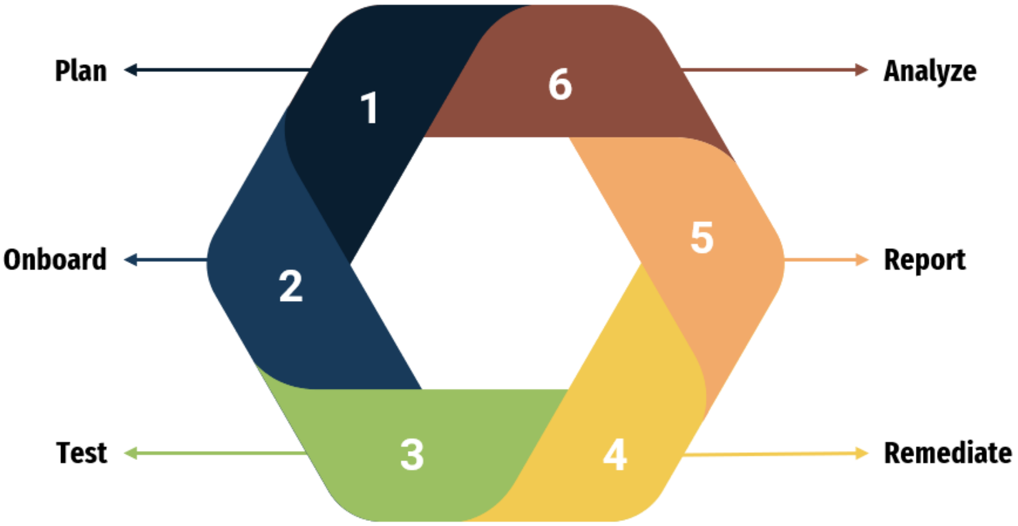
Your team or suppliers start to fix issues with the help of NSFOCUS security experts via PTaaS platform.

Report

A comprehensive report will be generated after all tests are done. Executive summary, re-production procedures, remediation suggestions are included in the report so that it provides insights both for your executive team and technical team.

Analyze

The SAAS platform houses all the penetration tests and their outcomes, which enable you to obtain an ongoing trend analysis throughout the year and allow you to track the progress of your remediation efforts for all vulnerabilities.



WHY NSFOCUS

Strong Attack and Defense Capabilities

- 8 Security Research Labs: **200+** security experts specializing in cloud computing security, IOT, Internet of Vehicles, Industrial Internet, AI-based intelligence defense, big data, offensive and defensive.
- 4 Attack and Defense Teams: specialize in attack and defense practices (Capture the Flag, cyber drills). The experience is accumulated and leveraged in our VAPT testing process.
- Comprehensive Security Qualifications: CCIE, Security+, CISSP, OSCP, CREST, CISM, CISA, Pentest+, PMP, ITIL, COBIT5.
- CERT Team: a dedicated group of experts who handle computer security incidents for customers worldwide 24/7.

Strong Vulnerability Mining Capabilities

- Over the years, NSFOCUS has dug out 230+ high-risk CVE vulnerabilities on popular IT products from Microsoft, Adobe, Google, Sun, Cisco, HP, IBM, etc.
- Awarded by Microsoft Bug Bounty Program for 7 consecutive years.
- Awarded by Mitigation Bypass Bounty program for 6 consecutive years