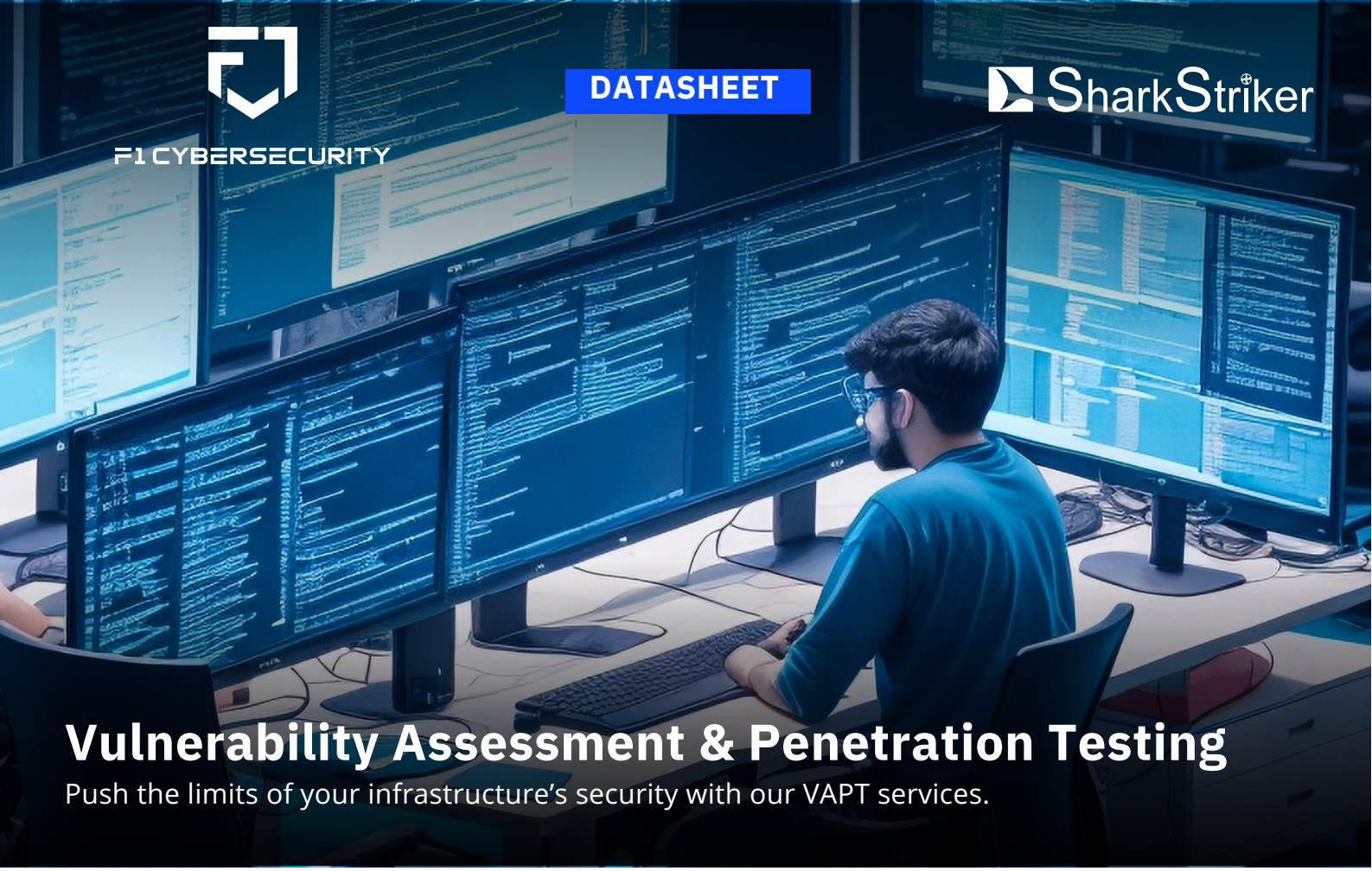
F1 CYBERSECURITY

DATASHEET

SharkStriker



Vulnerability Assessment & Penetration Testing

Push the limits of your infrastructure's security with our VAPT services.

What is VAPT?

It is an expert-driven cybersecurity testing method wherein they scan and test the status quo IT infrastructure or aspects of your IT infrastructure for security vulnerabilities using real-world techniques deployed by cyber attackers.

Vulnerability and Penetration Testing is a culmination of Vulnerability Assessment and Penetration Testing. Vulnerability assessment is using techniques to scan the IT infrastructure for security vulnerabilities, analyzing the impact of those vulnerabilities, and prioritizing them as per their severity.

Penetration testing is about using offensive automated and manual real-world techniques to exploit all the weak security measures of an IT infrastructure in place to test the strength of the existing security posture and plan steps to improve them.

What are the business benefits of VAPT

1.It helps improve your cybersecurity posture

Through VAPT, businesses can identify and categorize all the existing security vulnerabilities, take measures to treat them and implement cybersecurity best practices to improve cybersecurity posture overall.

2.Boosts reputation

By deploying best-in-class cybersecurity practices for securing all sensitive information assets and IT infrastructure, a business assures that their customer's data is in safe hands, and it builds its reputation among customers.

3.Saves money with enhanced posture?

By assisting in developing security strategies through effective identification and prioritization of vulnerabilities in the IT infrastructure, VAPT saves time and money otherwise lost in cyberattacks.

4.Gives a comprehensive view of all the security flaws and errors that may expose them to cyber attacks

VAPT offers a granular view of the nature of security vulnerabilities in the IT infrastructure. Through categorization, it provides a detailed idea of the severity of threats that may expose them to cyber attacks.

5.Renders a strategy to manage risks better across the IT infrastructure

Through this unique combination of vulnerability assessment and penetration testing, a cybersecurity expert can easily form a strategy to manage risks both internally and externally across the IT infrastructure.

6.Helps protect user data from data loss and unauthorized access

They can create strategies to secure all of their sensitive information and data assets from getting exposed, prevent data from being accessed by an unauthorized entity, and prevent it from being lost in a cyber attack.

7.Assists in meeting compliance requirements

VAPT is a must in many regulatory and global compliances. Therefore, any business that engages in the VAPT process automatically fulfills one requirement of compliance. They needn't worry about the assessment of the vulnerabilities and security flaws in their IT infrastructure.

8.Assesses the Incident Response in place

Through a systematic evaluation of the status of security measures in place, VAPT ensures that a business takes necessary measures for incident response and plans steps and proactive measures for incident response in their organization.

| What makes Our VAPT different?

We use highly offensive manual and automated real-world testing methods to help you detect the inherent security vulnerabilities in your IT infrastructure. Once we have identified the vulnerabilities, we categorize them as per their severity.

We assess the security of the IT infrastructure based on all the commonly known vulnerabilities, including those mentioned in the OWASP's top 10 list.

Through our expertise, you can effectively improve the posture of IT infrastructure and its components as per regulatory and global compliances.

What we cover

The types of assessments we cover include:

Mobile application pen testing

We assist our clients in assessing and pen-testing their mobile applications for security flaws before they release them to the app store to secure them from monetary and reputational loss.

Web application pen testing

Our end-to-end web application pen testing services are for comprehensive evaluation of cybersecurity posture. They are for identifying and addressing the most undetectable vulnerabilities in the web environment.

API Pen testing

Since API is the most commonly exploited vulnerability, we ensure that even the most unknown and hidden vulnerabilities in the API are identified and addressed before the cybercriminals can make their move. Based on the identification of the security vulnerabilities and security loopholes we recommend some of the industry best practices to improve the cybersecurity posture of the API.

IoT pen testing

To ensure that the IoT environment is operational smoothly without any disruption from cyber attacks, we engage in a comprehensive evaluation of the IoT environment using some of the most offensive real-world techniques. Based on the security loopholes and vulnerabilities that are identified, we recommend some of the plausible security measures sand best practices that are best suited for augmentation of the cybersecurity posture of the IoT environment.

Network pen testing

Our expert pen testers engage in comprehensive scanning and rigorous testing of the internal and external network of our client to identify some of the most commonly found and severe vulnerabilities that can cause a serious threat to network security. Based on the scanning and testing of the network using some of the most offensive real-world attack techniques deployed by attackers, we recommend security measures based on the benchmarked security standards of the industry. Our primary aim is to help our clients discover the most severe and commonly found vulnerabilities in their network and improve its posture using some of the industry's best practices.

The Shark Striker & F1 Cybersecurity approach

We are veterans in our field, having worked with multiple businesses across the industries. We have gathered experience tailoring our security testing to meet specific global and regulatory compliance requirements. Through our tailored VAPT services, we have assisted our clients in augmenting their cybersecurity posture to meet the most immediate and long-term needs of the cybersecurity and compliance landscape.

Step:1 - Prepare the scope of test

The first step of the VAPT process is to ascertain the scope of the VAPT process. We define the aspects of the IT infrastructure that are to be covered in the VAPT process. This includes the assets, applications, network, endpoints, etc. that are to be covered in the scope of the test.

Step:2 - Scan the environment for security vulnerabilities

The next step is to scan the environment for security loopholes and vulnerabilities. It also involves using the most offensive real-world techniques to uncover the weaknesses of the status quo cybersecurity measures.

Step:3 - Risk treatment plan

The next step after the identification and categorization of security vulnerabilities is done, we prepare a detailed risk treatment plan to treat all the existing risks and suggest measures that will help an organization improve its cybersecurity posture. We recommend the security measures, controls, configurations, rules, patches, and technology be implemented for effective treatment of all cybersecurity risks.

Step:4 - Implementation

We implement the risk treatment process with the correct set of people, processes, and technology to address risks across different levels of our organization. We ensure that we implement industry best practices as recommended by OWASP.

Step:5 - Reporting

Once we are done with the entire process, we prepare a detailed report with a list of recommended steps to further improve the cybersecurity posture. We prepare the report such that it can be used for the effectively achievement of the recommendations stipulated in compliance.

About Us

We are a global security services vendor with SOCs and offices across the globe. We are your cybersecurity team. We are the gatekeepers of your network. We ensure that you get maximum value from your cybersecurity framework.

Our purpose-built cybersecurity-centric, AI/ML-powered platform with a well-honed adversarial orientation delivers all-encompassing protection to the organization through - proactive protection, automated detection, machine learning-based response, threat intelligence, incident management, compliance management, and security awareness.

Our focus is simple – address threats before they become a problem.

Our Certifications and Awards

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2023

MSSP Alert Top 250 MSSPs 2022 EDITION

2023 CYBERTECH 100

2023 GLOBEE AWARDS WINNER INFORMATION TECHNOLOGY

MSP INNOVATION AWARDS EUROPE 2023 powered by CHANNELPARTNERINSIGHT

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022

GDPR

MITRE ATT&CK™

Information Security Management ISO 27001 Certified