FAQ

SECUREAUTH

CYBER RISK SERVICES

Frequently Asked Questions

What is Penetration Testing and what to expect from it?

What is a Penetration Test?

A Penetration Test is a practice of testing your organization's computer systems, network and application to find vulnerabilities and exploit them, mimicking attackers actions.

Which are the main categories when thinking about Penetration Test scope?

+ **Network:** External and Internal, Wired and Wireless.
+ **Applications:** Web, Web Services, Desktop, Mobile, IoT.
+ **Social Engineering:** phishing campaigns, Open Source Intelligence.

What is a Red Team Project?

A Red Team practice is aimed at testing the resilience of your organization against real-world attackers. We will find and exploit vulnerabilities while using tactics and techniques and procedures to avoid detection and persist.

How do you quote a Penetration Test or Red Team project?

We have a series of questionnaires we use to learn about the project size, for example, for a basic External Network Penetration Test, we take into account the total number of IP addresses and the number of live IP addresses, for a Web Application the number of functions or dynamic forms.

What is the outcome of Penetration Test project?

Our standard deliverable is a final report which contains an executive summary, the attacks we executed, conclusions and recommendations to improve the overall security. Additionally, we include an appendix of the vulnerabilities found. Each vulnerability includes technical details and remediation strategies.

Is it Safe?

Do you store sensitive information if a compromise occurs?

We do not. We just extract proof for reporting purposes. The information we store is the one we use to create the final report.

Do you follow testing industry standards?

We follow best practices and industry standards OWASP, OSSTMM. Our Security Consultants hold computer science/engineering degrees, CISSP and OSCP certifications.

Application Security Testing

Do you evaluate the security of an application?

We do. This practice is usually referred to as Application Penetration Test or Application Security Assessment depending on a couple of factors and is specific to an application. Applications could be mobile, web, desktop and IoT applications among others.

Do you ask for the source code of the application?

It depends on the approach of the project, it could be black-box, without source code or white-box with the source code. In the case of white-box, we not only uncover vulnerabilities but also check for secure coding practice and evaluate attack vectors that could not be exposed for attackers directly. Regardless of the approach we always encourage our customers to share if not all, certain sections of the source code.

Do you test cloud-based applications or infrastructure?

Yes, we do. Cloud providers usually have a procedure in place to alert them that a Penetration Test will be executed prior to the project start.

Is it Disruptive?

Does a Penetration Test or Red Team Project require significant involvement of Customer resources?

It does not. Mimicking attackers has to do with having some level of knowledge of the targets but limiting the interaction with the stakeholders to make the exercise as real as possible.

How long does it take to execute a Penetration Test?

Depending on the scope of work, for standard projects, between 5 and 10 business days.

Is a Penetration Test disruptive to my infrastructure?

We follow a series of procedures aimed at ensuring that we do not take down any device, server or network. There are some corner cases (less than 3%) that some downtime happens. We always take into account customer's advice on specific assets that showed performance issues in the past.

Do I need to perform the Penetration Test off-hours or weekends?

Not really, almost 95% of the projects are conducted business hours without any noticeable impact to the infrastructure or applications.

Do you execute the projects remote or at customer's office?

Both options are available. Remote options may include VPN or a SecureAuth supplied appliance to access internal network and systems if needed.