Find your vulnerabilities before your attackers do.

The internet is still very much the wild west, where malicious individuals and 'state-sponsored actors' can cripple your business and hijack your data with a few well-executed keystrokes. Whether financial information, system passwords, or intellectual property, a data breach can expose your business to an incredible amount of risk.

There are so many ways your security can fail, making the task of finding vulnerabilities during testing that much more critical. Which is why it's crucial to test your security with our highly experienced security professionals.

With spriteCloud, you are in safe hands. We're the experts at uncovering vulnerabilities, and we handle your information with the utmost discretion and confidentiality.

Penetration Testing Services

- Vulnerability scanning
- Cyber threat intelligence (OSINT)
- Wireless network penetration testing
- Web application penetration testing
- Mobile application penetration testing
- Infrastructure penetration testing

spriteCloud

Vulnerability scanning

Unlike how a penetration test tries to exploit vulnerabilities, vulnerability scanning merely identifies potential vulnerabilities in network devices like routers, servers, firewalls and applications. Running a vulnerability scan is lower in cost than a penetration test but it only identifies that vulnerabilities exist, it does not provide detail into how seriously it could be exploited. We use enterprise-level products for vulnerability scanning to ensure you get the best results.

As data breaches are often the result of unpatched vulnerabilities, vulnerability scanning provides a proactive approach for identifying and eliminating these security gaps. We recommend regular vulnerability scans to ensure that you are not left exposed to new vulnerabilities. We provide on-demand both credentialed and non-credentialed scans from both external and internal perspectives.

Cyber threat intelligence (OSINT)

The cyber threat intelligence using the open-source intelligence (OSINT) methodology entails collecting information about your organisation from public sources. Our goal is to provide you with a threat assessment based on information that hackers are known to use.This information can be used to help impersonate a high-level decision maker, launch more effective phishing attacks, social engineering campaigns, and subsequently compromise your security. We don't simply collect data, we provide data analysis and give it to you in terms of actionable recommendations.

Our service includes gathering general information about the target organization, performing a thorough network analysis through DNS and subdomain enumeration techniques, identifying the organisation's internet footprint including information on key personnel and source code leaks, and a non-invasive assessment to discover weaknesses that are exploitable.

Call us at +31 (0) 20 61 59 155 or email at info@spritecloud.com

Cyber attacks are on the rise, even for SMBs.

"Unless you plan to eliminate the WIFI networks in your organisation, assessing their vulnerabilities is a must."

Wireless network penetration testing

Wireless communications are essential in our modern way of life, but wireless networks are one of the most common entry points that attackers use to gain access to your enterprise network. Wireless networks are difficult to control, monitor, and protect from penetration which is why wireless network security experts are often hired to test the network.

Penetration testing your wireless network can help your organisation overcome three important issues:

- attackers using wireless network as an entry point into the organisation
- attackers manipulating communications to their own advantage
- the privacy of other wireless users being threatened

Our wireless network penetration tests are designed to employ the latest techniques to identify possible vulnerabilities in WEP, WPA-PSK, WPA2, WPA3 encrypted networks as well as checking for rogue access points (i.e. entry already gained). This can act as an important measure to increase awareness of effective security protocols, and prevent costly security breaches.

Web application penetration testing

A web application penetration test uses manual and automated approaches to identify security threats or vulnerabilities in your web application. The purpose of these tests is to determine possible threats and identify ways to mitigate them across the whole application and its components (database, source code, back-end services). Our team of OSCE and OSCP certified 'ethical hackers' use exploits (like SQL injections and XML External Entity (XXE) injections) to constantly probe ways to gain control of your web application; so that you can prevent others from doing so.

We offer three approaches to web application penetration testing:

Black-box

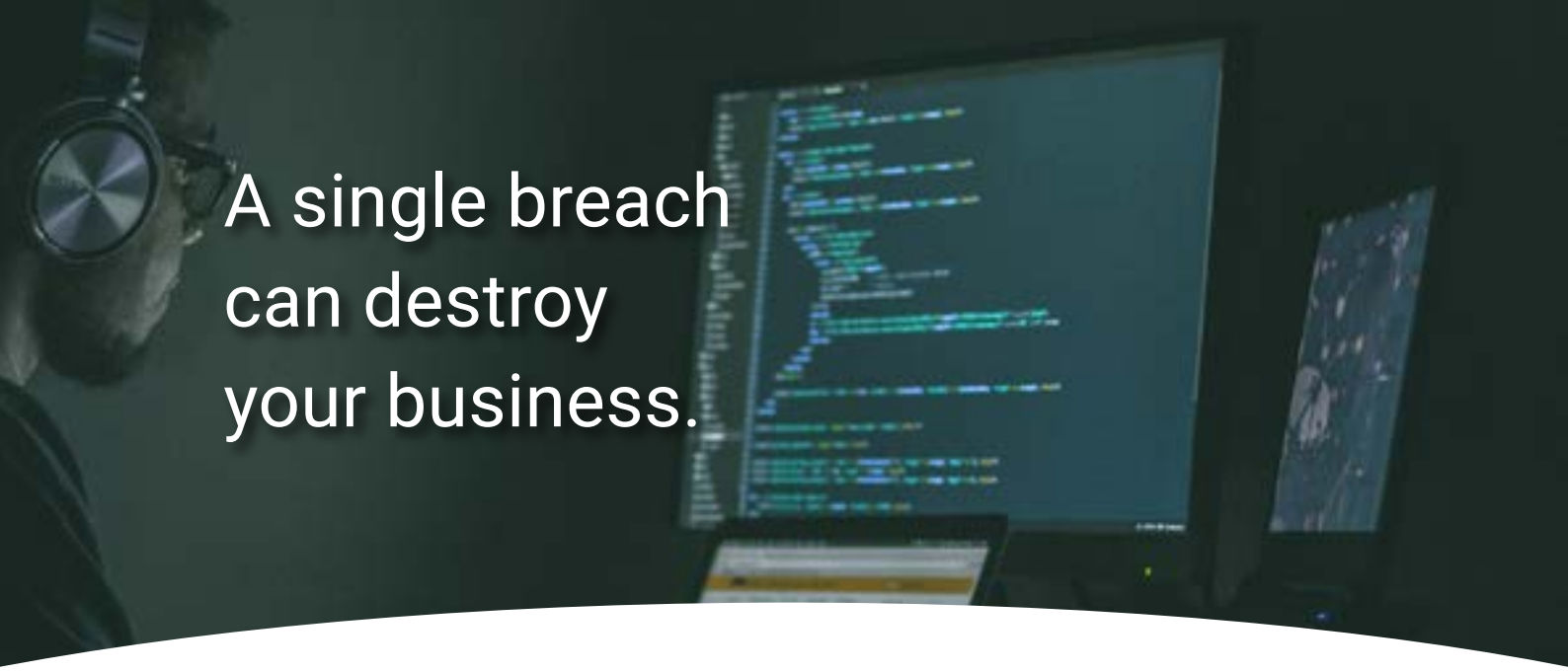
The tester is placed in the shoes of a normal internet user with no knowledge of how the application works or access to its source code. This method is closest to what a real hacker would face when trying to penetrate your application.

Grey-box *(our most common request)*

A combination of black and clear box testing, testers can create exhaustive tests while remaining close to realistic attack conditions. Testers are given knowledge of the internal workings and functionalities of the applications but without access to the source code. Testers use their knowledge of the system to test the application more thoroughly.

Clear-box

This testing approach requires the tester to have access to the source code of the application. This allows the tester to check the quality of the code, within a larger scope normally provided by a developer. While not representative of real-life conditions, it does allow for the more effective securing of applications.



A single breach can destroy your business.

Infrastructure penetration testing

With multiple computer systems, devices and users, your infrastructure has many points through which malicious actors can gain entry and wreak havoc. Our infrastructure penetration testing gives you a head start by helping you plug gaps in your defences and ensure that your customer data, intellectual property and financial information remains secure from threats, both external and internal. Our certified security experts are trained to help you turn your network into a virtual fortress.

We offer two approaches to infrastructure penetration testing. These methods are 'black box' external infrastructure testing and internal infrastructure testing.

External infrastructure testing

Exposures due to weak firewall configurations, flaws in application code or patch issues can leave you open to attackers gaining entry to your system. An external infrastructure penetration test helps identify these possible points of entry and provides an assessment as to how they can be secured. This is a 'black box' method. This method is meant to replicate how an attacker, with no knowledge of the system, would approach your infrastructure.

Internal infrastructure testing (assume breach)

An internal penetration test looks for security issues within your network. A compartmentalised network ensures that malicious employees or attackers that have gained access to your internal network, are mitigated. These internal network attacks are just as damaging as and more frequent than external attacks. These engagements follow the 'assume breach' mindset utilising the MITRE ATT&CK framework to test security gaps and SOC detection capabilities.

"Your information and that of your customers must be kept private. Your reputation and your bottom line depend on it."

Mobile application penetration testing

Just as quickly as mobile devices and mobile applications have become a part of daily life, so too have security breaches and attacks increased in frequency. A major cause of this is the increased time pressures that developers face to provide new functionalities and bring the apps to market.

All these reasons make frequent mobile application penetration testing crucial in order to protect the reputation of your app and your business. It only takes a little bit of bad press to doom a mobile app at launch. Our team of security experts will help you uncover vulnerabilities and secure them.

Are your applications, networks and systems secure? Now is the time to find out, before an attacker does.

Contact spriteCloud now for more information on how our security testing services can help keep your organisation and customers secure in these volatile times.

Call us at +31 (0) 20 61 59 155 or email at info@spritecloud.com