
procorre
Automated Penetration Testing

Automated Pen-Testing Platform

A thousand Pen-Testers at your service. Not on your Payroll.

The Challenge:

As hackers become more sophisticated, corporate security officers and regulators become more aware of the need to integrate the hacker's perspective into their ongoing cyber defence strategy.

Traditionally penetration testing has been done manually by service firms, deploying expensive labour to uncover hidden vulnerabilities, producing lengthy reports, with little transparency along the way. Professional service-based penetration testing, as we know it today, is time-consuming. It represents a point in time snapshot and cannot comply with the need for continuous security validation within a dynamic IT environment.

The solution:

Our partner's automated penetration-testing platform focuses on the inside threat and mimics the hackers' attack - automating the discovery of vulnerabilities and performing ethical exploits while ensuring an undisrupted network operation. Detailed reports are produced together with proposed remediations, one step ahead of tomorrow's malicious hackers.

Benefits of our partner penetration testing platform

Continuous protection - Test as frequently as needed (daily, weekly or monthly)

Because networks, users, devices and applications constantly change and expose vulnerabilities, it is critical to pen-test continually. It allows you to validate your cybersecurity posture as often as you need, keeping your guard up at all times.

Consistent Validation - Hold all your networks to the same high standard

It is critical to consistently check your security controls and defences across your organisational networks. The automated penetration testing platform tests your entire infrastructure with a wide array of hacking techniques ensuring that you remain resilient regardless of how the hacker is trying to break in.

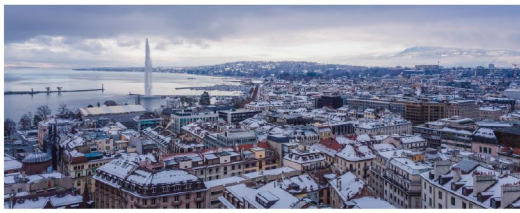
Current defence - Keep up with the latest hacking techniques

Malicious hackers constantly evolve their techniques and tools; therefore, it is critical that your risk validation tools evolve as fast as the hackers. The platform assures that you match and evolve the depth of ''off the books'' Pen-Testing techniques.

Easy Deployment:

Our partner's software is locally installed on your network, effectively securing your vulnerabilities from the internet and the outside world. The software requires standard hardware, and installation only takes a few hours, at the end of which the entire functionality is accessible to you in any environment.





Machine-based PT VS Human-based Penetration Testing

A global shortage of information security professionals and the increase in cyber threat sophistication drives the need for automated Penetration testing software.

We improve the way organisations validate their cybersecurity risk, by delivering the most sophisticated, continuous and cost-effective penetration testing platform.

Criteria	Automated PT	Human-Based PT
Test Frequency	Continuous/On Demand	Annual/ Quarterly
Speed	Minutes-Hours Per Full PT Run	Days- Weeks Per limited PT Run
Consistency	Highest-Software runs millions of attack vectors, non-stop	Partial and Highly Dependant on the individuals performing the act
Scope	Entire Network/Complete Coverage	Based on time and the number of PT consultants Deployed
Project Approach	None. It's a Plug-In And Play System	The intense project team needs to be assigned & vendors personnel involved
Privacy	Pt findings only visible to company's personnel	External PT consultants exposed to confidential information, intrusive, unpleasant.
Most Current	Automated PT is Updated Monthly with latest Vulnerabilities and exploits	Highly dependant on the PT Company Playbook that is often outdated

About the platform:

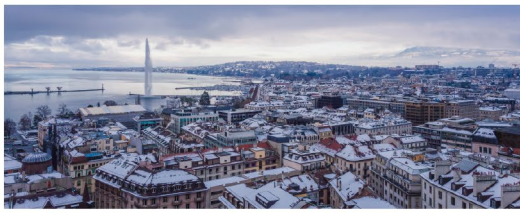
The platform delivers an automated penetration-testing platform that assesses and reduces corporate cybersecurity risk. By applying the hacker's perspective, our software identifies, analyses and remediates cyber defence vulnerabilities. Security officers and service providers around the world use the platform to perform continuous, machine-based penetration tests that improve their immunity against cyber attacks across their organisational networks.

Product Features:

Agentless - Zero agent installations or network configurations. Penetration testing starts with physical LAN access without any credentials. Just like a hacker would.

Harmless Exploits - Like a hacker, we perform real exploits without disruption of service, for example, reconnaissance, lateral movement, remote execution, credential reply, Password cracking, ethical malware injection and privilege escalation,





Attack vector visibility - Every step in the attack vector is presented and reported in detail to document and explain the attack 'kill chain' and select the minimal amount of vulnerabilities to stop the attack,

Automated - Press 'Play' and get busy doing other things while the penetration tests progress. All you need to do is define a range of IPs and check the type of tests you want to perform.

Attack checkpoints - for mission critical systems, a company's security officer can assume discreet control for higher -order exploitive stages to selectively control the intrusiveness level of the attack.

Prioritised remediation - get a clear packaged summary of the critical remediation steps to perform based on the threat facing priorities that are relevant to your organisational network and critical assets.

Latest hacking Techniques- Know that your penetration testing techniques are the most up to date.

Custom Business Alerts - you can set any starting point and penetration testing target and run a targeted attack to allow testing for a specific weakness or for the cyber resilience of specific applications.