Medicare Network
More intelligent, More Secure

Crown Commercial Service Supplier

AI-Powered Automated Penetration Testing

Availability | Integrity | Confidentiality | Accountability

The Challenge

As hackers become more and more sophisticated, cyber security personnel and regulators become more aware of the need to integrate the hacker's perspective into their on-going cyber defence strategy. Traditionally penetration testing has been completed manually by consultancy firms, deploying expensive labour to uncover hidden vulnerabilities and produce lengthy reports, with little transparency along the way.

Professional services-based pen-testing, as we know it today, is time consuming, intrusive, costly, represents a point-in-time snapshot and cannot comply with the need for continuous security validation within a dynamic IT or Enterprise environment.

Manual penetration methods and services to secure your networks, systems and data has been presented several drawbacks:

- It requires exorbitant amount of time and effort depending on the scope,
- It reveals internal confidential information to the person performing the test,
- It only provides a snapshot of the organisation's immediate security posture, and
- It is extremely expensive to continuously pen-test.

Traditional pen-testing requires highly skilled ethical hackers (also known as white-hat hackers) to undertake many man-hours of work, which does not include any associated hidden costs.

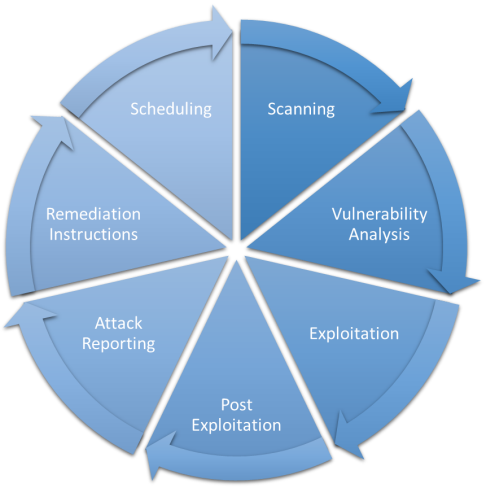
The Solution

Tap into the world's leading black/grey box artificial intelligence (AI) powered machine learning pen-testing solution that dramatically reduces the attack surface by identifying, analysing and prioritising remediation of vulnerabilities, improving efficiency, cost and saving valuable time and effort.

The AI-Powered platform mimics the hacker's mindset and automated discovery of dynamic vulnerabilities, threats and ethical exploits while ensuring a smooth network operation. Detailed reports are produced together with proposed remediations to help you stay, one step ahead of tomorrow's malicious hackers.

Methodology and Approach

The methodology and approach are based on the same best practices, as a manual pen-test, while utilising the advantages of AI-Powered, machine based, self-learning, continuous ethical hacking and working for you 24x7.



Key Functionality

- Level 1 - Full vulnerability scanning that can replace tools like NESSUS, Qualys, Tenable and Rapid7 that perform static vulnerability scanning.
- Level 2 - Black/Grey box pen-testing performing AI-Powered penetration vectors by applying safe exploitations, providing remediation recommendations and attack vectors reports.
- Level 3 - Ethical hacking performing bespoke use cases and business impact analysis showing potential breach of critical services and data.

By distributing nodes throughout your environment, provides the flexibility to run a wide variety of attacks across your entire Enterprise, managed centrally. Furthermore, deployment and on-going pen-testing can be securely performed remotely without impact to operational services.

Human vs Machine-Learning

Human pen-testing is becoming outdated. As the methods used to perform malicious breaches of your data improve, machine-learning is becoming a necessity because it can perform the same tasks a human can within hours, not weeks.

It can be used continuously and on-demand and can perfectly replicate malicious attacks without the ethical challenges provided by human testing.

It is faster, more efficient and ultimately more productive to switch to AI-Powered pen-testing.

Criteria	Automated	Manual
Test Frequency	Continuous/ On-Demand	Annual/ Quarterly
Speed	Hours per full scan	1-2 weeks per full scan
Consistency	Highest - software runs millions of attack vectors, non-stop	Partial and highly dependent on the individuals performing the act
Scope	Entire network	Specified segment only
Project Approach	It is a Plug-and-Play solution	Full project team needs to be assigned and external vendor
Privacy	Findings only visible to company's security personnel	External consultants exposed to confidential information

"There are only two types of companies; those that have been hacked and those that will be."

Key Benefits

Agentless
Plug & Play solution

Zero agent installations or network configurations, nor allocation of IT resources. One can focus on the process rather than having to experiment with technical barriers, thus saving time. Pen-testing starts with physical LAN access without any credentials, as if you were a hacker.

Continuous Protection
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 AI-Powered pen-testing platform tests your entire infrastructure with a wide array of hacking techniques ensuring that you remain resilient, regardless of how the hacker tries to compromise your organisation.

Consistent Validation
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. The AI-Powered pen-testing platform allows you to validate your cyber security posture as often as you need, maintaining your minimum-security baseline.

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 AI-Powered pen-testing platform assures that you match and evolve the depth of "off the books" pen-testing techniques.

About Medicare Network

Medicare Network is an agile, forward-thinking Cyber Security and Risk Management company, product agnostic that offers a range of industry-leading and advanced secure solutions, leveraging award-winning AI and Machine Learning technologies to identify, respond and protect against sophisticated cyber-attacks.

20 Mortlake High Street | London | SW14 8JN | United Kingdom
UK +44 (203) 355 3785 | **US** +1 (702) 605 4601
www.mednetsec.com