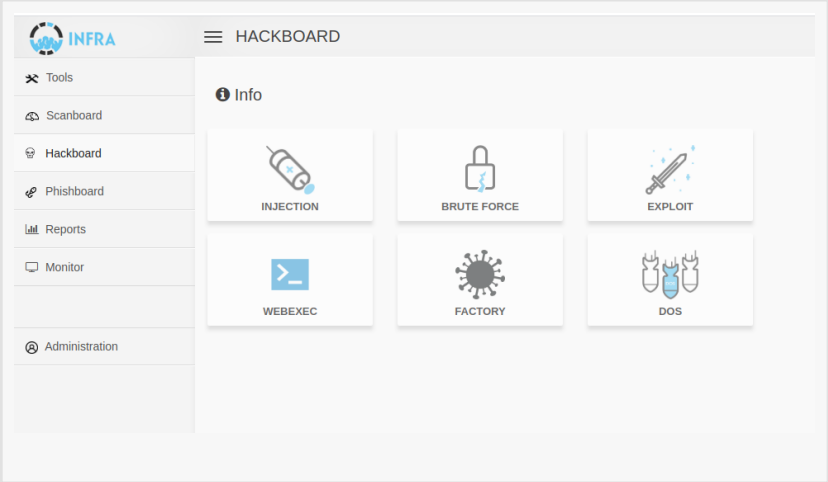
HACK ATTACK! The Intelligence Framework (INFRA) Fights Cyberwarfare With Ethical Attacks

Trusted by governments and corporations to fortify security, INFRA's powerful ethical hacking platform addresses cyber threats' complex needs.



NEW YORK, NEW YORK, UNITED STATES, April 23, 2021 /EINPresswire.com/ -- As we move into a future where geopolitical conflicts are played out in the digital realm, the race is on to build cyber defenses.

The New Cold War might be characterized by covert digital missions that could bring a power grid or water treatment system down, undermine public trust, or sway opinions and ideologies.

The objective of the game is pretty straightforward—undermine the enemy without getting exposed.

Countries including the United States, United Kingdom, Russia, India, Pakistan, Uzbekistan, China, Israel, Iran, and North Korea have active cyber capabilities using digitized tactics, techniques, and procedures. Between 'low and slow' attacks that steal data and persist unnoticed, digital assaults are increasingly becoming harder to catch and even harder to attribute.

Teams carrying out cyber warfare are called Advanced Persistent Threats (APT). An APT is a stealthy threat actor, typically a nation-state or state-sponsored group, who gains unauthorized access to a computer network and remains undetected for an extended period.

As states explore the use of combined capabilities, the likelihood of a cyber operation increases.

According to research, Cyber Warfare market revenue is set to grow at a yearly rate of 14.3 % during 2019-2025, while its valuation is predicted to jump from 20590 Million USD in 2019 to

35190 Million USD in 2025. Leading contenders within the product terrain include Lockheed Martin, General Dynamic, BAE System, Airbus, Intel, Raytheon, DXC Technology, and IBM.

Espionage through hacking or sabotage using Denial of Service (DoS) is an elemental cyberwarfare attack. But how do they do it?

Companies and organizations are increasingly testing their own IT networks with hardware and software designed to find holes in their security. The process is called "Ethical Hacking," and there are now a variety of products to perform these "Vulnerability Assessments" and "Penetration Tests" to identify and resolve these weaknesses.

In cyber warfare, ethical lines are blurred, particularly if one entity feels they are experiencing a legitimate threat to their security. This circumstance requires ethical hacking systems with a unique understanding of APT's and the consequences of digital attacks on military and government systems.

INFRA (www.infrascan.net) is an ethical hacking platform designed to address the complex needs and threats of cyber warfare. INFRA was co-founded by the state government of Virginia in the United States and currently protects military and government systems in Asia and the Americas. The platform not only performs the standard Vulnerability Assessment and Penetration Tests, but automates the process of exploiting vulnerabilities (aka "hacking with one click"), sends fake emails with phishing, features custom trojans, and protects against DoS network sabotage.

The Intelligence Framework (INFRA) is a powerful engine vital for gathering information, assessing vulnerabilities, and analysis. It has added support for commercial and open-source plug-in modules, custom modules, and modular extensibility scanners, to fully adapt to the specific needs of an organization.

INFRA provides:
- Automated information analysis
- Real-time data, including DNS, network, databases, and web applications
- Social, commercial and financial records

INFRA is an automated solution that leverages AI for ethical hacking and intelligence. Tests conducted on IoT, servers, computers, and web applications are standardized and automated for faster, more efficient results that outperform standard security scanners. The platform provides a robust menu of intelligence, investigation, ethical hacking, and penetration testing for corporations, military, and government organizations requiring the highest security level in their IT infrastructures.

For a detailed list of INFRA security appliances, servers, and products, visit https://www.infrascan.net/products.html

Adam Nelson
WORKHOUSE
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/539267600

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2021 IPD Group, Inc. All Right Reserved.