Shield-CyBot: Unique Automated PEN Testing

Now you can perform comprehensive and dynamic security testing 24x7

Our unique solution, Shield-Cybot, operates inside your network detecting real ways hackers could disrupt your business. It anticipates cyber-attacks before they occur by using unique and innovative algorithms that imitate the behavior of human hackers. You work smarter because it provides continuous automated Penetration Testing capabilities. It identifies and maps Attack Path Scenarios that an actual hacker might exploit. Most leading brands only test your perimeter from the outside. This still makes you vulnerable. So Shield-CyBot tests from the inside out.

The main features of Shield-CyBot are:

- Anticipates different types of Cyber Attacks (Unauthorized access to various systems and asset vulnerabilities that can lead to Remote Code Execution and more).
- Cyber-BI (Business Intelligence) that displays the exposure of an organization under various parameters over time.
- Allows the design of efficient, effective, and sophisticated protection of enterprise resources.
- Provides recommendations for immediate fixes of vulnerabilities, and M2M instructions enabling security equipment to block intruders.
- Intended for use in IT systems, thus, enabling IT Security Managers to immediately deal with vulnerabilities in a more effective manner.
- Allows performing multiple continuous pre-defined scans without external interaction.

Shield-CyBot scans all IP-based components in any environment. Its proprietary Reasoning Engine (patent pending) uses real-time information about identified vulnerabilities to predict multi-level, dynamic, and complex attacks that hackers can exploit. It patented scanning technology is 100 times faster than all other existing technologies. Unlike human penetration testers that reach 1-10 assets per day, Shield-CyBot can check hundreds of thousands of assets per day. As new assets are added to the network (even ad hoc) it will scan them. This ensures that you aren't surprised by new possibly unsecured assets on your network.

How it works: *Shield-CyBot enables organizations to accurately evaluate their resiliency against cyber threats. With it they can proactively adjust their security protection strategies to mitigate these risks.*

- Imitates human hacker behavior to predict sophisticated and dynamic attack path scenarios.
- Provides timely attack path scenario analysis critical to IT and business divisions.
- Facilitates security Business Intelligence.
- Provides real-time risk mitigation – enables organizations to respond immediately to cyber threats.
- When deployed in a global, multi-site environment, shares information across all sites to depict global attack scenarios.
- Proprietary Reasoning Engine (patent pending) predicts attack path scenarios at a rate of one path per second. As up to 100 Shield-CyBots can be deployed in an organization up to one million scenarios can be checked in only three hours.

The most powerful benefit of Shield-CyBot lies in its value as a training tool for network security staff. Without live, real-time tests of actual vulnerabilities in a company's actual network no security team can

know how well their defences will work against real threats. Shield-Cybot provides the necessary detailed information to secure your assets and data against these threats. You can easily access the security business intelligence (BI) data and risk maps needed to also mitigate future sophisticated cyber-attacks. This makes for efficient investments in the best cyber security strategy for your organization.

Minimum Requirements:

The computer that hosts Shield-CyBot should have the following minimal hardware and software prerequisites in order to work properly:
CPU: 4 Cores
Memory: 8 GB
Storage Space: 100 GB
Network: 1Gbe or 2 x 1Gbe
Hypervisor: VMware ESXi v5.5 and up
Internet Browser: Google Chrome
Ports need to be opened: 445/139, 22 (WMI,SSH)

With Shield-CyBot you can stop cyber criminals before they get your sensitive data!