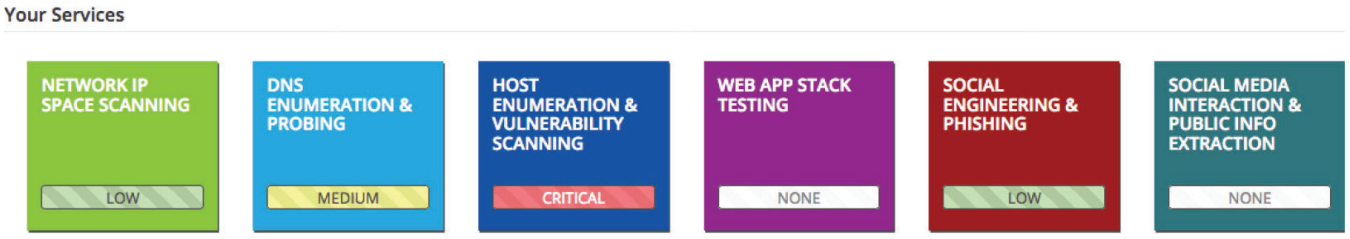
Cyber Security, Simplified.

CATO is an easy-to-use, web-based platform that automatically and randomly assesses your cyber security readiness.

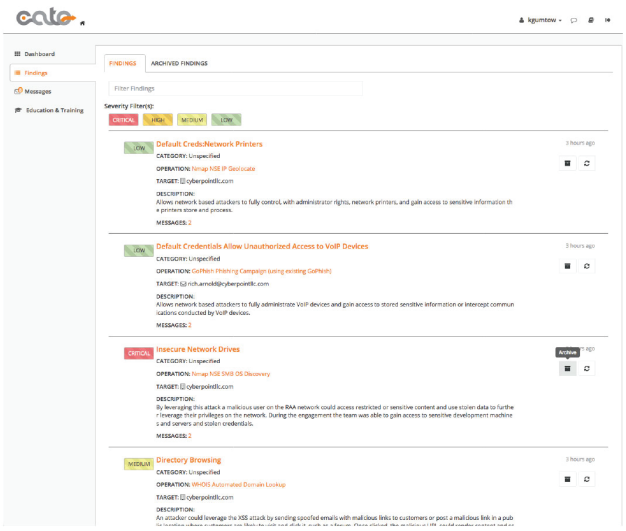
CATO matches the operational cadence of real-world attacks by executing proven campaigns, operations, and tasks honed over eight years and a million hours protecting CyberPoint's customers. The results, or CATO Findings, are automatically generated by our expert system or manually created by our experienced operators and presented to the customer through dashboard service tiles. At a minimum, each CATO Finding has a description, recommendation, and severity ranking.



A quick review of our dashboard services tiles shows you have a critical finding in DHost Enumeration & Vulnerability Scanning.

CATO provides a platform to conduct random and scheduled operations.

- Random and scheduled vulnerability assessments.
- Automated external and internal penetration testing.
- Malware and vulnerability cyber hunt.
- Security control compliance validation.
- Dark Web monitoring of accounts, assets, and brands.
- Performance-based training and education.
- Access to malware analysis and incident reporting.
- Access to risk quantification and mitigation.
- Real-time analysis and reporting.



An example of CATO's Findings.

Current CATO Services

Service	Description
Network IP Space Scanning	Operations in this service are designed to find active hosts on network blocks that you own *(both inside and outside of your boundary protections)*. We don't expect you to know every computer or device, so we can help you find them.
DNS Enumeration & Probing	Operations in this service are designed to query domain name service *(DNS)* servers to find host details for hosts that you own and operate. This activity reveals details about network hosts that were identified by the Network IP Space Scanning service.
Host Enumeration & Vulnerability Scanning	Operations in this service are designed to gain more understanding about active hosts within your infrastructure—typically more than DNS operations can reveal. We will learn which services are active on these hosts, which are publicly accessible, and potentially about the risk *(vulnerability)* that these hosts pose.
Web App Stack Testing	Operations in this service are designed to examine web applications you run or host. We look at every part of the application from the website, through the background servers *(database and messaging)*. We go beyond traditional vulnerability scans and look for risks that application design may pose *(e.g. loss of confidential data)*.
Social Engineering & Phishing	Operations in this service are designed to test your employees *(and yourself)* and their risk for opening or viewing content *(attachments, URLs)* that they should not be trusting. We will send your employees email and active content and test to make sure they do not view or open the content.
Social Media Interaction & Public Info Extraction	Operations in this service are designed to identify details about your business *(e.g. practice, customers, capabilities, IP)* that are publicly accessible even though you may not be aware of them. We examine social media sites and perform search and query of engines that you might not even know about.
Cyber Hunt	Operations in this service are designed to hunt for vulnerabilities and malicious software on internal and external networks that evade traditional security systems.
Web Application Audit	Operations in this service are designed to examine the interactive portions of your web application*(s)*. We look for items such as usability, error handling, and in specific cases, compliance with legal authority or best practices.
Malicious Insider Scenario Execution	Operations in this service are designed to mimic a malicious insider. These operations will attempt to steal trusted files, data and gain access to resources designated as critical. These operations can also include controlled attack scenarios such as cache poisoning.
Wireless Security	Operations in this service are designed to identify and measure the security of any wireless implementation you operate. These operations cover Bluetooth and Wi-Fi only at this time.
Insecure Configuration Identification	Operations in this service are similar to web application stack testing but look at any host that you own or operate. These services are designed to identify mistakes made in the setup or configuration of the host.

About Our Team

CATO operators are well trained and seasoned. They apply their expertise to all facets of testing your environment in the same way that similarly skilled attackers do. They are all capable of testing your network as individuals, but they combine their skill sets and focus to deliver a more effective and repeatable service to CATO customers.

CONTACT US

Email us at info@cyberpointllc.com or call +1 410 779 6700 to learn more about what CATO can do for you.

cato
a CyberPoint product

CyberPoint International
621 East Pratt Street, suite 610
Baltimore MD 21202
phone +1 410 779 6700