CYBREYE™

WORLD CLASS CYBER SECURITY

- Infrastructure Penetration Testing
- Application Security Testing
- Remote Access Security Testing

Standard Cyber Security defenses could be leaving your organization unprotected. CYBREYE tests for all exploitable vulnerabilities that could allow unauthorized access to key information assets. Through the application of automated scanning, with customized proprietary scripts and manual techniques, we offer a complete roadmap to security and peace of mind.

A FALSE SENSE OF SECURITY... THE GREATEST THREAT TO YOUR ORGANIZATION

Many organizations rely on Intrusion Prevention Systems, often built into firewalls, monitored by a Secure Operation Centre (SOC), together with periodic penetration testing, to protect their networks from attack.

With this line of defense, which is based on testing against known attacks, a well-configured firewall can typically identify and block up to c.60,000 attacks per IP and commercial penetration tests will typically only carry out c. 80,000 attacks.

With these measures in place, you might be confident that your organization is protected. It is not!

Firewalls as well as commercial penetration tests do not cover the entire threat landscape, and are only as good as the number of known threats they can detect or test for. The firewall cannot see, let alone protect against, unknown attacks for which no pattern or signature is publicly available. Further, a SOC can only report the threats that the firewall detects, meaning that while you might believe your network is safe, thousands of successful attacks may be happening.

CYBREYE TESTS AGAINST ALL EXPLOITABLE VULNERABILITIES

A Cybreye Penetration Test utilizes 154,000+ attack vectors per IP

Cybreye's capability is way beyond commercial grade penetration testing and gives complete visibility of the threat landscape,exposing verified exploitable vulnerabilities. With 154,000+ attack vectors per IP this is over c.70,000 more attacks than even the best commercial penetration testing will expose. With Cybreye you can obtain hundreds of successful attack results even in a network where the IPS is set to BLOCK ALL.

THE CYBREYE PENETRATION TEST:

- Exposes your full threat landscape
- Delivers a clear remediation roadmap and support
- Measure and enforces your security policies

CYBREYE SECURITY STANDARDS AUDIT

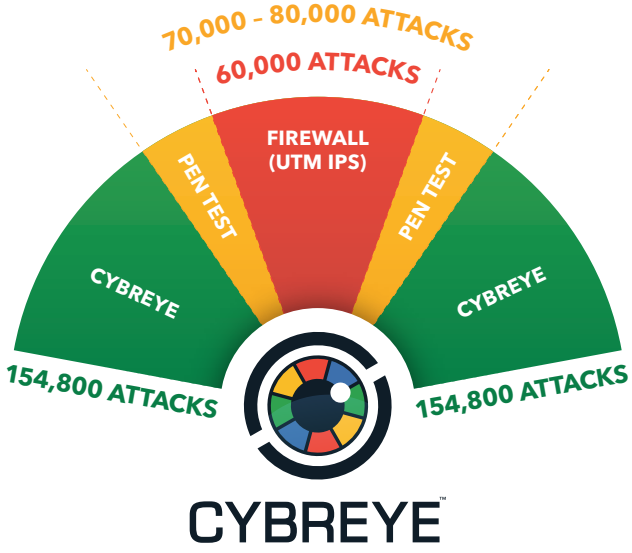
The Cybreye Penetration Test offers the best possible defense by checking against 154,000+ attack vectors, while the Cybreye Security Standards Audit demonstrates compliance with any relevant vendor/industry standards.

SECURITY STANDARDS AUDITS

- **HIPPA**
- **PCI-DSS**
- **ISO 27001**
- **Internal IT Security Policy**

Cybreye's Penetration Test exceeds the level of all, standard vendor and industry compliance requirements. The Cybreye Security Standards Audit will measure compliance to specific standards, filtering out any weaknesses that do not have a direct bearing on those standards. This allows organizations to both demonstrate compliance while gaining a complete private overview of your vulnerabilities.

Any applicable weaknesses will be highlighted with a clear path to remediation, which is the Cybreye Purple Team approach, an alliance between the traditional Red and Blue teams.

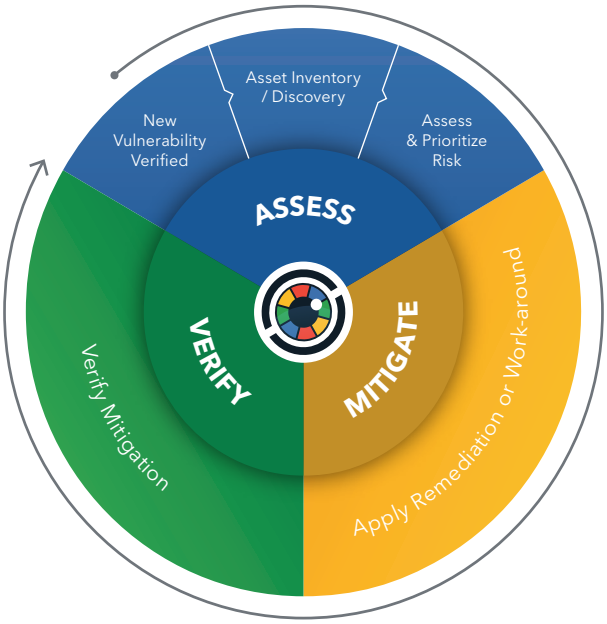


CYBREYE™

CYBER SECURITY AUDITING | GOOGLE SUPPORT | SECURE MOBILE COMMUNICATIONS

Take control and eliminate risk with **CYBREYE**

- Cybreye services can be delivered **anywhere in the world, from anywhere in the world**
- We continually lower your risk with **measurable deliverables** at an affordable price
- We take the **responsibility for actions required** to deliver a security policy that is measured and **enforceable**
- We are enabling IT to **deliver wins** and enable them to provide tangible value
- We remove IT Security from the critical path in respect of business process implementation and improvement and **shorten time to market**
- Integrate with existing security products that results in **investment protection**



THE CYBREYE METHOD

1. **PLANNING**
   Identification of rules, management approval finalized and documented, and testing goals are set. The planning phase sets the groundwork for a successful penetration test.

2. **DISCOVERY**
   Phase 1: Testing commences with information gathering and scanning. Network port and service identification is conducted to identify potential targets.
   Phase 2: Vulnerability analysis, comparing the services, applications, and operating systems of scanned hosts against vulnerability databases (automated vulnerability scanner process) and the testers' knowledge of vulnerabilities.

3. **ATTACK**
   Cybreye specialists execute a staged attack. If an attack is successful, the vulnerability is verified and safeguards are identified to mitigate the associated security exposure.

4. **REPORTING**
   Cybreye's clear, easy to understand reports detail all the security vulnerabilities within an infrastructure that can be exploited and how to resolve all threats found in testing.

In many cases, up to 80% of the risks to an IT environment can be mitigated by resolving a much smaller number of key vulnerabilities. Cybreye's Remediation Report will identify these and prioritize a remediation strategy accordingly.

CYBREYE TEST EXAMPLES:

- SQL Database Attacks
  - (SQL Injections)
- Database Configuration Audited against:
  - Oracle, MSSQL, etc. configuration standards
- Webserver Attacks:
  - WebDAV
    - Flaw Exploit analysis
    - Backdoor identification
    - Payload offload via mechanisms such as Meterpeter – Cross Site Scripting Attacks against Web Applications
- Perimeter security bypass exploitation
- Full Operating System Security Audits

Many organizations are operating in the dark with regards to the risks to their IT environment.

- With regular government–grade penetration testing from CYBREYE, you can be certain that you are aware of and can protect against every threat.
- At the same time, CYBREYE can ensure that you optimize your IT Security costs by not fixing problems that you don't have.

CYBREYE™
SEE CLEARLY

www.cybreye.com