DISRUPTORS

Penetration Testing Services Overview

Disruptors Cyber

Executive Summary

Proactive Security Testing

Expert penetration testing services designed to identify vulnerabilities before attackers do

Disruptors Cyber provides comprehensive penetration testing services that proactively identify vulnerabilities in your systems, ensuring robust protection against evolving cyber threats.

Our penetration tests expose weaknesses and provide actionable recommendations to fortify your defenses against complex security threats, ensuring protection for your critical data and assets.

Our assessments support organizational compliance with industry regulations and standards including ISO 27001, NIST, and other international standards. Each engagement is tailored to your unique business requirements using proven methodologies and industry best practices.

With Disruptors Cyber, you can confidently secure your operations and maintain trust with customers and stakeholders.

Why Choose Disruptors Cyber?

Our penetration testing services deliver comprehensive security assessments backed by certified expertise and proven methodologies.

Expertise

- Certified Ethical Hackers (OSCP, OSWE, OSEP)
- Deep industry knowledge
- Real-world attack simulation experience

Custom Solutions

- Tailored assessments for your business
- Flexible engagement models
- Aligned with your risk profile

Compliance Assurance

- ISO 27001, NIST, and other international standards guidance
- Regulatory compliance support
- Industry best practices

Proactive Defense

- Identify threats before they materialize
- Actionable remediation guidance
- Continuous security improvement

Team Certifications & Accreditations

Our team holds industry-leading certifications demonstrating deep technical expertise and commitment to professional excellence in penetration testing and cybersecurity.

OSCP - Offensive Security Certified Professional

Industry-standard certification for penetration testing professionals. Demonstrates hands-on expertise in identifying vulnerabilities and exploiting systems in controlled environments.

OSEP - Offensive Security Experienced Penetration Tester

Advanced certification focusing on evasion techniques and complex attack scenarios. Validates expertise in bypassing modern security controls and defenses.

OSWE - Offensive Security Web Expert

Specialized certification in web application security testing. Proves advanced skills in identifying and exploiting web application vulnerabilities including complex authentication bypasses.

OSWA - Offensive Security Wireless Assessor

Expert-level wireless security certification. Demonstrates proficiency in assessing and exploiting wireless network vulnerabilities across multiple protocols.

CPTE - Certified Penetration Testing Expert

Comprehensive penetration testing certification covering methodology, tools, and techniques. Validates practical skills in conducting thorough security assessments.

CISEH - Certified Information Security & Ethical Hacker

Professional certification in ethical hacking and information security. Demonstrates knowledge of security principles, attack vectors, and defensive strategies.

CCPenX-AWS - Certified Cloud Pentesting Expert (AWS)

Specialized cloud security certification for AWS environments. Validates expertise in identifying misconfigurations and vulnerabilities in cloud infrastructure.

CITP MBCS - Chartered IT Professional

Professional membership with the British Computer Society. Demonstrates commitment to professional standards, ethics, and continuous professional development.

BCS Ethical IT Professional

Certification in ethical IT practices and professional conduct. Validates understanding of ethical frameworks and responsible technology use in cybersecurity.

Comprehensive Testing Services

Disruptors Cyber offers a full spectrum of penetration testing and security assessment services to protect your organization from evolving threats.

Web Application Testing

Rigorous testing for vulnerabilities including SQL injection, cross-site scripting (XSS), and IDOR. Ensures robust protection against cyber threats while safeguarding user data and business continuity.

Network Penetration Testing

Internal and external network vulnerability identification, simulating real-world threats to fortify infrastructure against breaches and insider threats.

Mobile Application Security

Security evaluation for iOS and Android applications and APIs. Identifies insecure storage, authentication flaws, and API endpoint vulnerabilities with actionable insights.

Cloud Security Assessment

Examination of public and private cloud infrastructures (AWS, Azure, Spark CCL, Datacom) for misconfigurations, access control flaws, and vulnerabilities with tailored recommendations.

Advanced Security Services

Beyond standard penetration testing, we offer specialized security assessments and collaborative engagements to strengthen your overall security posture.

Purple Team Engagements

Collaborative Red (offensive) and Blue (defensive) team exercises that enhance threat detection, response, and recovery capabilities, boosting overall cybersecurity resilience.

Red Team Operations

Sophisticated real-world attack simulations including social engineering and physical security bypasses, thoroughly testing organizational readiness and defensive capabilities.

Phishing Simulations

Realistic email and SMS simulations to evaluate employee susceptibility, significantly enhancing awareness and response capabilities to minimize attack success rates.

Secure Code Reviews

Detailed software source code reviews detecting vulnerabilities like buffer overflows, SQL injections, and logic flaws, ensuring software security prior to deployment.

Infrastructure & Compliance Services

Comprehensive security assessments covering your entire technology stack and physical environment.

Host Configuration Security & Compliance Reviews

Thorough audits of operating systems, databases, web servers, and firewall configurations. Ensures compliance with NIST and CIS standards, strengthening security posture and reducing risk.

Wireless Penetration Testing

Examination of wireless networks including Wi-Fi and Bluetooth to ensure proper protection is in place and identify potential vulnerabilities.

Security Maturity Assessment

Does your organisation meet international security requirements? Our Security Assessment Maturity Tool—a comprehensive evaluation framework—can provide the answer.

Our framework rigorously evaluates organisations across six critical cybersecurity domains:

- Governance
- Information Security
- Personnel Security
- Physical Security
- Cloud Security
- Threat Intelligence

Aligning with international security standards and industry security frameworks, we use evidence-based methodology that prioritises finding and resolving risks.

Our framework also helps address ISO 27001, NIST, and other international standards requirements for handling government information and contracts, as well as achieving compliance with privacy regulations and data retention requirements.

Transform Your Security With Reporting:

- Detailed Assessment Reports show your compliance levels within security domains
- Executive Summaries provide board-level reporting to your leadership
- Gap Analyses highlight critical vulnerabilities, pinpointing areas that need to be addressed

With Guidance:

- Remediation Roadmaps, organised by risk levels, outline the way forward with actionable steps
- Requirements Guides provide evidence-based practices for each of your security controls
- Compliance Mapping helps to align with specific ISO 27001, NIST, and other international standards requirements

Strategic Consulting Services (vCISO)

Access executive-level cybersecurity expertise without the full-time cost. Our Virtual CISO services provide strategic guidance tailored to your organization's needs and budget.

01

Risk Management & Compliance

Liaison with Risk and Audit Committees and Boards to identify and manage risks. Conduct risk assessments, establish mitigation plans, and ensure compliance with ISO 27001, NIST, and other international standards and other regulations.

02

Security Program Development

Work closely with IT and security teams to align with industry-standard practices. Set up and enhance information security programs including security controls, incident response plans, and business continuity plans.

03

Vendor Management & Third-Party Risk

Assess security practices of vendors and third-party service providers to minimize relationship risks. Establish robust vendor management frameworks including due diligence, contract reviews, and ongoing monitoring.

04

Incident Response & Training

Provide guidance during security incidents for swift and effective response. Offer training programs to educate employees and promote security-conscious culture.

Privacy & Identity Solutions

Implement privacy by design with comprehensive identity management frameworks and data sovereignty controls.

Identity Management Frameworks

Establish robust identity and access management systems that ensure proper authentication, authorization, and accountability across your organization.

Data Sovereignty Controls

Implement controls to ensure data residency requirements are met and sensitive information remains within appropriate jurisdictions.

Privacy by Design

Integrate privacy considerations into system architecture from the ground up, ensuring compliance with privacy regulations and international standards.

Compliance Assurance

Ongoing monitoring and assessment to maintain compliance with evolving privacy regulations and industry requirements.

Privacy Impact Assessments

Systematic evaluation of how your systems and processes affect individual privacy, with recommendations for improvement.

Data Protection Strategy

Comprehensive approach to protecting personal and sensitive information throughout its lifecycle.

Our Engagement Process

A structured, transparent approach to delivering comprehensive penetration testing services that align with your business objectives.

01

Initial Consultation

Understanding your business requirements, risk profile, compliance needs, and specific security concerns. Define scope and objectives.

02

Scoping & Planning

Detailed assessment planning including systems to be tested, testing methodologies, timelines, and success criteria. Establish rules of engagement.

03

Testing Execution

Certified ethical hackers conduct comprehensive testing using industry-standard tools and methodologies. Real-world attack simulation with controlled approach.

04

Analysis & Reporting

Detailed findings documentation including vulnerability severity ratings, potential business impact, and evidence of discovered issues.

05

Remediation Guidance

Actionable recommendations prioritized by risk level. Clear implementation guidance and best practice advice.

06

Executive Briefing

Board-level reporting with executive summaries, compliance mapping, and strategic security recommendations.

> Professional, thorough, and results-focused. Every engagement is tailored to your unique environment and business needs.

DISRUPTORS

Get Started

Ready to strengthen your security posture?

Contact Disruptors Cyber today to discuss your penetration testing needs and schedule a consultation. Our team of certified experts is ready to help protect your organization from evolving cyber threats.

Email

info@disruptorscyber.com

Phone

07775346462