Broad Security Review

www.zdlgroup.com

Analysing Your Systems from the Attacker’s Perspective

What if you could take your testing to a strategic level where you could take the guesswork out of which systems you need to address next in your security programme?

The ZDL Broad Security Review analyses your company’s security from an attacker’s perspective, giving a **360° view** of the methods and vulnerabilities they would exploit across the business as a whole.

Tailored to your organisation’s unique requirements such as infrastructure, risk profile and its business objectives; the review digs deeper than any off-the-peg security test.

Raising Your Resilience with Advanced Security Testing – Manual Pen Testing

Utilising manual testing, we deploy senior consultants to test your infrastructure, just as a hacker would. They look for all the back doors, not just the known vulnerabilities. As they are a human acting like a human, they get to understand the workflows and infrastructure and where the true weaknesses lie.

A manual ethical hack will also identify patch management requirements and those products or apps added to your systems that are making it insecure.

A Broad Security Review combines advanced hacking with other vectors such as physical security across the business and providing wider online reconnaissance.

A Broad Security Review

- Eliminates false-positives delivered by automated scans allowing you to identify and focus more time on the most critical vulnerabilities.
- Provides a report in a 360° business context to help drive your security program priorities.
- The true criticality of the impact of combinations of individual vulnerabilities is revealed.
- Identify true business risks and establish timelines for remediation.
- Test your organisation's resilience across multiple locations.
- Turns security testing from a tick box exercise to underpinning long-term security strategy and resilience.

> "It has been an absolute pleasure working with ZDL. As an organization Hunt prides itself on excellence in corporate governance, so it has been refreshing to find another company, ZDL, who share our values and commitment to excellence in this area. By engaging with ZDL we are in a much better position, where we now have a deeper and richer understanding of risk in our business. Not only this, we also now have the strategies in place to reduce these risks at pace. The service and quality we received, from first engagement to delivery of the broad security review reports (and beyond) has been excellent. I would happily recommend ZDL as a strategic cyber security partner, and I'm looking forward to continuing our relationship for years to come"
>
> **CISO – Hunt Companies**

Our Methodology

Every business and its risk posture is different. Tailor your Broad Security Review specifically to your organisation's requirements by selecting from a comprehensive list of security tests in four core areas:

- NETWORK SECURITY
- RECONNAISSANCE
- SOFTWARE & SERVICE VULNERABILITIES
- PHYSICAL SECURITY

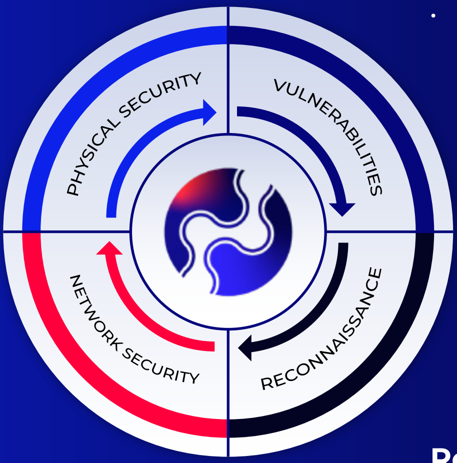
ZDL GROUP

Physical Security

- Insufficient security of the:
  Reception areas or server rooms
  Insecure VOIP Phone systems
  SIP end-points
- Insufficient protection of:
  Network sockets
  Servers
  End-user devices
- Inappropriate protection of sensitive information
- Insufficient access controls
- Unprotected & remotely accessible camera systems
- Weak door access control systems
- Door tailgating

Vulnerabilities

- XSS
- CSRF
- HPP
- XXE
- Integer overflows
- Format string
- Vulnerabilities
- Insecure session implementations
- Insufficient access controls
- Incorrectly implemented authentication mechanisms
- Information disclosure
- Insecure data storage
- Patching weaknesses
- Buffer overflows
- Logic flaws



Network Security

- Insufficient network security controls: MAC filtering, IPS/IDS
- Incorrectly/insecurely configured devices & software default configurations e.g. default usernames & passwords
- Software vulnerabilities in internally accessible services
- Insecure encryption algorithms
- Vulnerable printer installations allowing further network access
- Insecure desktop infrastructure
- Insecure printers allowing access to restricted resources via VLAN hopping
- Insecure server installations/ weak permissions/insecure software
- Pass-the-hash vulnerabilities/ hash description issues
- Firewall ruleset weaknesses
- Weak VPN implementations
- Insufficient network segmentation
- Insecure, unpatched software
- Wireless systems

Reconnaissance

- Email addresses
- Usernames
- Passwords
- Log files
- Back-up files
- Other sensitive information
- Inappropriate disclosure of sensitive information
- Incorrectly configured DNS servers

www.zdlgroup.com
London | Brighton | Manchester | USA

ZDL GROUP

Delivering Excellence in Cyber Security

At ZDL, we believe that effective risk management requires a holistic 360° approach. We take a comprehensive view of our clients' cyber security risks and provide quality services to address those risks.

Our approach to Total Security Management helps make our clients' infrastructure, applications and data more secure in the face of a continually evolving Threat Landscape. Our aim is to build a partnership with our clients, built on a mutual respect and understanding of each other's businesses. We become a part of our clients' team, a valued partner; an intrinsic part of their business.

ZDL's 4 key service areas are designed to focus on our clients' cyber resilience journey. Our unique portfolio of services enables you to build an agile, responsive security infrastructure and strategy.

Our Services

Ethical Hacking

- Broad Security Review
- Red Teaming
- Security Audits
- Penetration Testing
- Cloud Security & Security Ops Testing
- Source Code Review/Coding Standards
- Social Engineering
- Physical Security

Training

- Security Awareness Programmes
- Secure Coding School for Developers
- Bespoke Senior Exec Security Training
- Runbook training/ Scenario Workshops
- Phishing & Resilience Programmes
- Physical Security Awareness
- Online Assessment / CBT Developer Training

Managed Services

- Supplier Evaluation Risk Management (VenDoor)
- Incident Response Preparedness
- Security Training for Developers - Annual Programme
- Managed Detection and Response (MDR)
- Virtual Information Security Manager
- OSINT/Threat Intelligence

Compliance

- Policy Review & Creation
- 360° Assessment
- PCI Remediation Support
- ISO/ NIST/EU GDPR Standards Agreement
- Business Continuity Management
- IR Management Review
- ISO Readiness Programmes
- Office365 Configuration Review

CONTACT US →

www.zdlgroup.com

London | Brighton | Manchester | USA