Incident Response Preparedness

Cyber Incident Prevention Training, Planning & Support

Incident Response Preparedness is designed to raise your organisation's resilience in the event of a breach to minimise the impact of an attack. Pre-Breach preparation is key and this is why we focus totally on Pre-Breach only services. Assessing your capacity for managing an incident and setting the processes and training in place to manage them before they happen, are core to the ZeroDayLab approach for Incident Management. From Policy Reviews & Creation to Assessments to Runbook Creation to Training and Desktop Simulations, preparing for the attack before it strikes protects business continuity and reduces the level of monetary damage that could occur.

Only 11% of businesses have invested in Threat Intelligence to identify Cyber Security risks in the last 12 months*

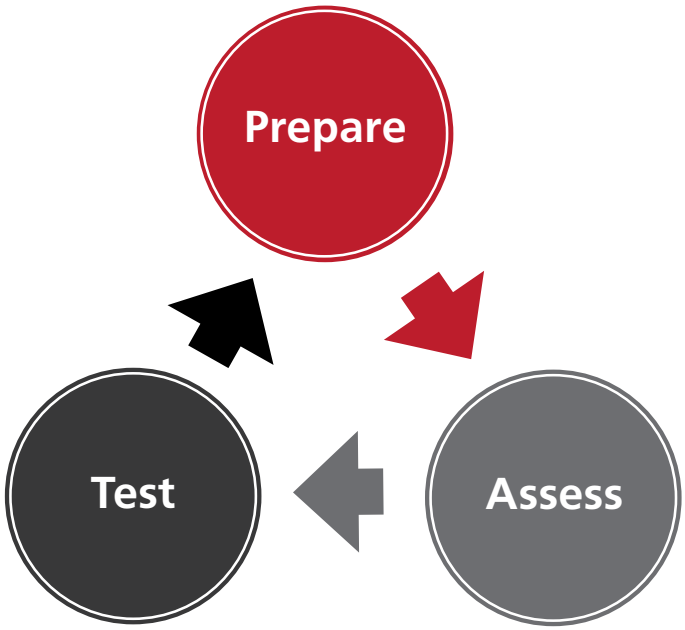
46% of all UK businesses identified at least one breach or attack in the last 12 months.*

Prepare

Reduce the impact of an attack through training and response planning. Identify attack scenarios and define processes for response, tailored to your organisational needs. Train team members from across departments, from Security and IT to the Board & Communications, to work in a cohesive unit to help you protect your customers and financial and reputational position.

Assess

How ready is your organisation for an attack? Get attack-ready by assessing the process and response gaps in your business - before an attack happens. Ideally assessments should take place on an annual basis to accommodate for team and business structure changes.



Test

The most effective way to understand if your organisation is prepared for a significant cyber incident is to regularly test your incident plan, runbooks, controls and how your teams respond through both desktop and technical incident simulations.

**Cyber Security Breaches Survey 2020 - DCMS, Her Majesty's Government*

ZERODAYLAB®

Incident Response (IR) Preparedness Packages

Attackers are evolving tactics constantly and Incident Response Preparedness activities should be conducted every year to ensure you are ready for those perfect storms. For on-going resilience, our annual plans help businesses ensure that their incident planning and preparation stays current with changes in business strategy, departments, teams, and the latest threats.

We suggest three different levels of Packages but can of course create a Bespoke Package as well. Pricing is determined by many factors such as the size of organisation, number of participants in certain activities, the current cyber maturity of the business, existence of policies and/or Incident Response Plan etc...

PLATINUM

The Complete Package of Full Incident Response Preparedness through Reviews, Creation, Training and Desktop as well as Technical IR simulation, and Dark Web Analysis includes:

- IR Management Review – Policy/Plan Creation
- Runbook Review/Creation & Training
- First Responder Training
- Digital Forensics Fundamentals Training
- Desktop IR Scenario Training
- IR Capability Assessment
- Technical IR Simulation
- Open Source Intelligence (OSINT)/Cyber Threat Assessment

GOLD

A Mid-Level Package to ensure more than the basics are covered includes:

- IR Management Review – Policy/Plan Creation
- Runbook Review/Creation & Training
- First Responder Training
- Digital Forensics Fundamentals
- Desktop IR Scenario Testing

SILVER

Entry Level Package to get started with a Review, Policies and Training to include:

- IR Management Review – Policy/Plan Creation
- Runbook Review/Creation & Training

BESPOKE

Maybe your organisation already has certain items in place?
We can create a Bespoke Pre-Breach Package right for you.

ZERODAYLAB®

At **ZeroDayLab**, every day is spent helping make our client's infrastructure, applications, and data more secure through the intelligent combination of services from highly trained consultants and leading edge, complementary security technologies.

At **ZeroDayLab**, we take a holistic approach to Total Security Management. Our skilled and experienced consultants can provide help, advice, training and support on a whole range of IT security solutions such as:

- Vulnerability Assessment of Desktop, Servers, and Infrastructure
- Penetration Testing of all Internal / External Web Applications and Infrastructure
- Broad Security Review (Architecture and Infrastructure)
- Source Code Reviews
- Firewall Audits
- Desktop and Server Build Reviews
- Blockchain Application Security Audits
- Digital Forensic Analysis
- Security Awareness Programmes
- Security Training for Developers – Secure Coding School, CBT, Online Assessment
- Pre-Breach Incident Response & Runbook Training
- Phishing Resilience Programmes
- Bespoke Senior Executive Security Training
- Red Team Testing
- PCI DSS Remediation Support
- Gap Analysis to ISO, PCI DSS, SSAE16(18), GDPR
- 360° Assessment
- Virtual Data Protection Officer
- ISO / NIST / EU GDPR Standards Alignment
- Internal Audits
- SERM Supplier Evaluation Risk Management
- OSINT / Threat Intelligence - Deep & Dark Web
- Protective Monitoring (Managed SOC)
- Security Risk Training for Agile Developers
- IR Preparedness (Full package of pre-breach services)
- Business Continuity Management
- Cloud Security Configuration Review

Our team looks forward to sharing our vision with you and helping you to defend against the malicious attacks that come from both inside and outside of your environment.

Europe Headquarters:

ZeroDayLab Ltd
Suite 303, 150 Minories,
London,
EC3N 1LS, UK
Phone: +44 (0)207 979 2067

North America Headquarters:

ZeroDayLab LLC
3524 Silverside Road, Suite 35B
Wilmington, DE
19810-4929, USA
Phone: 1-614-263-9765

Amsterdam I Manchester I Edinburgh I Dublin I Brighton & Hove

www.zerodaylab.com I info@zerodaylab.com