Full List of Services

Incident Response Preparedness Programme

25 March 2021

Prepared by: Steve Giachardi, Information Security Manager
Stuart Peck, Director of Cyber Security Strategy
sgiachardi@zerodaylab.com
speck@zerodaylab.com
Tel: +44 (0)207 979 2067

ZeroDayLab Limited
Suite 303
150 Minories
London
EC3N 1LS

Table of Contents

1 ZeroDayLab as your Partner 3
2 Why Choose our Incident Response Preparedness Programme? 4
3 List of Services 6
3.1 IR Management Review- Policy/Plan Creation 6
3.1.1 Cyber Security Incident Response Policy Creation 6
3.1.2 Cyber Security Incident Response Plan Creation 6
3.2 Runbooks Review/Creation and Training 7
3.2.1 IR Runbooks Training 8
3.3 First Responder Training 9
3.4 Digital Forensics Fundamentals Training 10
3.5 Desktop IR Scenario Testing 10
3.6 IR Capability Assessment 11
3.7 Technical IR Simulation 12
3.8 Open Source Intelligence (OSINT)/Cyber Threat Assessment 12
3.8.1 Scope of services to be monitored 13

1 ZeroDayLab as your Partner

ZeroDayLab consultants have a long security pedigree, and as your strategic security partner we bring these advantages to all client engagements:

- **Trusted Authority**

Having developed our own unique toolsets, management reporting methodology, proprietary security training, and an advanced manual testing approach to ethical hacking; ZeroDayLab is uniquely placed as a trusted advisory partner, delivering security projects for many UK & Ireland, USA, and other European & International organisations.

CREST Certified for Penetration Testing, ZeroDayLab's security consultants are not only passionate about what they do, they are certified to the highest standards; CRTP, CRTE, CCT, CRT, OSCP, OSCE, RSE, ISACA, CISSP, CCNA, CCNP, eCRE, eWPTX, eCPPT, eWPT etc.

Our Governance, Risk, and Compliance (GRC) consultants are experts in their field; covering multiple information security standards including ISO 27001, NIST, and PCI DSS amongst many others. The highly-certified team consistently delivers assessment, analysis, and implementation support at an exceptional level for clients of all sectors, sizes, and security postures. What is more, our consultants drive leading-edge thought, speaking at events and conferences in the UK and Europe, as well as publishing whitepapers.

- **Our 360° Approach**

Our ethos is to take a 360° approach to organisational information security, focusing on people, process, and technology. ZeroDayLab champions the concept of an integrated approach that strategically embeds security into an organisation. We conduct our assignments to help organisations improve their security posture in line with their business objectives through a combination of effective risk management, strategic governance, and strong analysis.

- **'Consistency, Quality, On Time, Every Time & In Budget'**

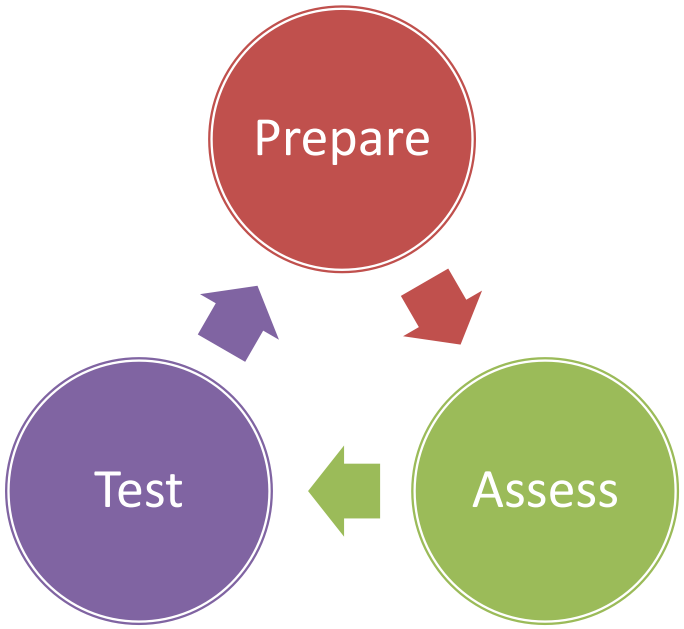
This is ZeroDayLab's mantra, and it is applied to every engagement and every client. CREST certified and aligned to ISO 27001:2013 for Information Security Management and ISO 9001:2015 for Quality Management; ZeroDayLab applies this high standard of internal processes to ensure the effective delivery of all our client projects. We have a full list of client reference sites available on request. We also have several case studies and sample management reports available on request.

- **Award Winning**

ZeroDayLab's high levels of service delivery and thought leadership, not only ensure high client retention but are also reflected in a number of industry award nominations and wins.

2 Why Choose our Incident Response Preparedness Programme?

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.



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.

Incident Response (IR) Preparedness

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.

3 List of Services

The goal of these services is to assist your organisation in developing a robust Cyber Security Incident Response Management programme. To ensure that the programme is comprehensive, all documentation will be aligned with the National Institute of Science and Technology's (NIST) Computer Security Incident Handling Guide (henceforth referred to as NIST 800-61), International Organisation for Standards (henceforth referred to as ISO) ISO 27001 / 27002, ISO 27035 and CREST Incident Response.

3.1 IR Management Review- Policy/Plan Creation

The purpose of the Incident Response Management Review is to establish standards and procedures for Cyber Security Incident Management for systems, servers, networks, and applications. Cyber Security Incident Management standards and procedures protect information assets by establishing protocols and procedures for a standardised method of operation.

3.1.1 Cyber Security Incident Response Policy Creation

The aim of this exercise is to review and update the current version of the Cyber Security Incident Management Policy to be in line NIST 800-61, IS0 27001 / 27002, ISO 27035, and CREST Incident Response. This policy will serve as the foundation for the proposed Cyber Security Incident Response Plan (CSIRP) and associated Runbooks, explained later.

In the absence of an existing Cyber Security Incident Management Policy altogether, one will be created. In lieu of reviewing a legacy document, the ZeroDayLab consultant will interview key IT and security stakeholders to ensure that the policy is tailored appropriately to the organisation's operational model and strategic objectives.

3.1.2 Cyber Security Incident Response Plan Creation

The Cyber Security Incident Response Plan (CSIRP) will be designed to adhere to the previous Policy, and as such be in line with NIST 800-61, IS0 27001 / 27002 and ISO 27035. The plan will be a holistic response to a cyber security incident in that it will not only address the technical aspects of the cyber incident but also the business impact. The CSIRP will address the following areas of concern initially gathered through stakeholder interviews:

- Criteria for identifying a cyber incident and determining potential severity level also known as Triaging
- Composition of the Cyber Security Incident Response Team (CSIRT)
- Composition of Executive Response Team (ERT)
- Roles and responsibilities of each team
- Incident response process milestones e.g.
    - Documentation of incident
    - Assignment of incident to IT Lead
    - Declaration of major security incident
    - Actions of the Cyber Security Incident Response Team (CSIRT)
    - Actions of the Executive Response Team (ERT)

- Communications Plan (Internal and External)
- Mitigation and containment
- Follow up activities
- Post incident reporting
- Training requirements

3.2 Runbooks Review/Creation and Training

The Incident Response Runbooks are the technical response plan of action providing best practice guidance on all stages of a response to a cyber security incident, specifically:

- Prevention and Preparedness
- Detection of an Incident
- Incident Escalation & Containment Actions
- Eradication Actions
- Recover Actions
- Follow Up / Remediation

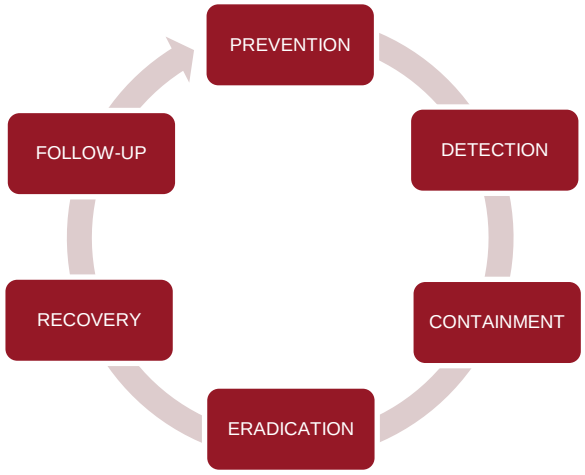


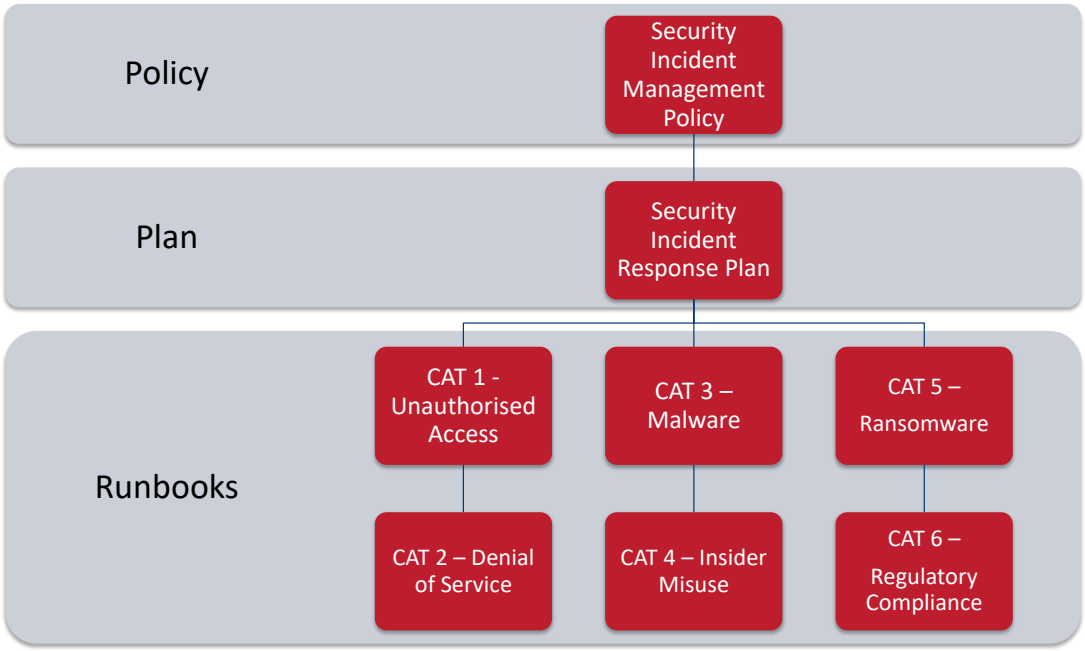
Figure 1: Incident Response Lifecycle.

While the response to cyber security incidents will follow the same general pattern, the Incident Response Runbooks will flag actions that are specific to the following cyber incident scenarios:

- Unauthorised Access
- Denial of Service (DoS)
- Malware
- Insider Misuse
- Ransomware
- Regulatory Compliance
- (Optional) PCI DSS

Once the draft documentation has been completed, the procedures and runbooks will be presented to the appropriate stakeholders, where alterations and adjustments can be made.

Once all the documents have been completed the topology of the documents that have been created will align to the diagram that is produced below:



3.2.1 IR Runbooks Training

It is envisaged the training element for the Runbooks implementation will consist of the following:

- Preparation Time – Tailored training session creation
- Four x 2.5 hours training sessions (delivered over two consecutive days – remote or onsite tbc), including Q&A and mini-scenario testing after each session. If number of attendees is large – additional sessions in some categories will be added.

The topics that are covered as part of this training are:

- Awareness of a Security Incident, how to identify, what to do, documents to read, etc.
- The overall lifecycle of a Cyber Security Incident
- Cyber Security Incident Management Policy
- Awareness of the Cyber Security Incident Response Plan
- Inquiry into any other documentation that may assist in the event of a security incident
- Key teamwork areas, focal points (e.g., effective Crisis Communications and Cooperation)
- 'Walk through, talk through' of response to incident scenarios to stress test the effectiveness of the runbook
- Meeting UK Data Protection 2018 (DPA 2018) & UK General Data Protection Regulation (UK GDPR) 24-hour breach notification requirement and under EU GDPR for cross-border processing if applicable.

The preparatory work will include tailoring of the training package.

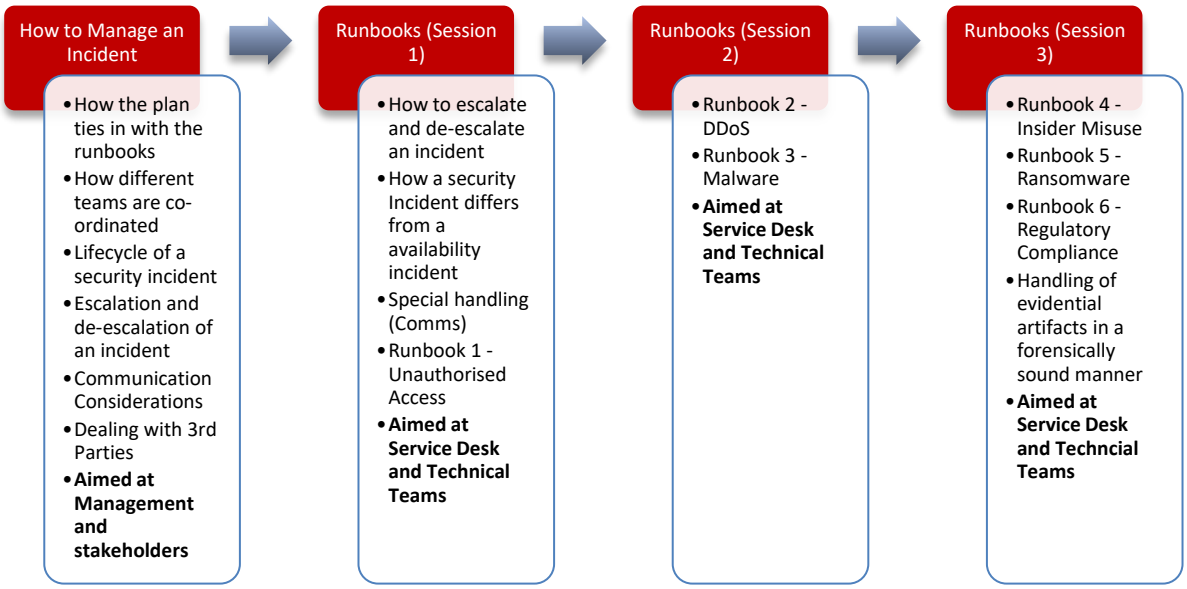
The attendees for this training package should include job roles that are similar to:

- Information Security Manager
- IT Service Desk Manager
- Infrastructure Team members
- First Responders (senior members of the service desk team)

Partial Attendance:

- Business Continuity / Disaster Recovery Manager
- PR / Communications personnel
- Legal team members
- HR staff
- Facilities Team

The following is a schematic diagram of the **4 x 2.5-hour training sessions** that will be delivered



3.3 First Responder Training

The First Responder training focuses on investigation and containment activities to ensure incidents are appropriately triaged, classified and contained. The actions during first hour of an incident being detected are vital and can make or break the organisation's ability to contain.

The expertise and lessons gained from responding to major global breaches will be imparted to the attendees of this training, focusing on the following:

- The Golden Hour of Incident Handling
- First Responder fundamentals
- Effective Incident Triaging
- Investigation and analysis during an incident

- Incident Classification
- Containment vital- techniques that are extremely effective (by incident type)
- Tools/Sources to review during an incident

This course will be delivered to up to 5-8 key attendees on average and will be up to 4 hours including Q&A.

3.4 Digital Forensics Fundamentals Training

The Digital Forensics Fundamentals Training will provide an organisation a hands-on introduction on what to do if there is an identification of an asset that requires forensic analysis as part of an investigation, such as a PC/laptop/mobile phone/Virtual Server etc… This course will build upon the First Responder Training. The aim of this exercise is to train the first responders on what to do against a defined checklist agreed as the best practice for isolating and maintaining evidence in preparation for further investigation. The course will cover:

- Why it is important to maintain a chain of custody
- Evidence Handling
- Artifact collection
- Isolation techniques for Phones, Laptops/devices, servers, virtual machines, and cloud assets
- Tools to aid in evidence preservation and preparation for Forensic collection.
- Example scenarios to stress test the knowledge gained during the training.

The aim of this training course is to maximise an organisation's potential to be prepared for an incident and to effectively handle digital evidence, while minimizing the costs of an investigation for the data to be analysed. This course will be delivered to up to 5-8 key attendees on average and will be up to 4 hours including Q&A.

3.5 Desktop IR Scenario Testing

ZeroDayLab provides the ability for organisations to test their Incident Response Plan and how teams will operate during high profile cyber incidents. The output of this exercise will be a report documenting the actions taken, and any recommendations based upon the ZeroDayLab consultant's observations.

ZeroDayLab's incident scenarios are taken from real world experience of responding to high profile and global attacks and malware / ransomware outbreaks in similar industries.

Examples of ZeroDayLab's previous incident response scenarios include:

- Ransomware smokescreen hiding data exfiltration
- Unauthorised access
- Insider malicious data theft
- Supply chain breach, affecting a company's Personally Identifiable Information (PII) data
- Security researcher discovers critical vulnerability, releases to the press
- Extortion by well-known threat actor group, over theft of personal data

- Sensitive data theft by well know organised criminal gang, with the dump being found on the dark web by a well know security journalist
- Whistleblower of bad practice affecting regulation within a company
- Developer account is hacked, resulting in the hacker having control of critical applications and website and sending malware to customers, BBC news is running with the story

The Incident Scenario Workshop will give ZeroDayLab knowledge of an organisation's ability to respond to a likely cyber-attack and improve the company's understanding of the impact of a successful attack. In addition, the scenario will address the company's regulatory and legislative obligations, including the DPA 2018, UK GDPR, EU GDPR & ISO 27001, PCI DSS etc.

The ZeroDayLab team will consist of two consultants, one to deliver the scenario and one to observe and take notes of all activities and decisions made throughout the 4-hour session.

To close the workshop a debrief will be conducted. The goal of the debrief is to capture issues and items of concern that have been identified as a result of the exercise. This specialist training is a set fee and as part of the exercise the findings will be documented in a report post project and will be supported with actionable and prioritised recommendations.

3.6 IR Capability Assessment

The Incident Response Capability Assessment delivered by ZeroDayLab assesses all of the controls that are in place to detect, react and respond to a potential incident against a range of threat scenarios. The Assessment will deliver the following:

- Assessment of the company's proactive, deterrent, detective, compensating, and application controls
- Technology that supports incident response, logging, monitoring, containment, evidence capture etc.
- High Level Review of existing threat models and risk assessments
- High Level Review of external and internal threat vectors
- Reviewing the potential impact of the threats
- Reviewing the likelihood of the threats
- Modifications required to deal with threats
- Review the capability to detect, react and respond the incident scenarios that have the largest impact
- Estimated time from detection through to recovery, based upon evidence gathered through the assessment

After the evidence gathering has been completed, ZeroDayLab will produce a report, outlining the gaps and recommendations for technical controls, monitoring, and additional policies (outside of the Runbooks, Incident Response Plan, and Policy already created), that should be implemented to increase the overall response capability.

3.7 Technical IR Simulation

ZeroDayLab provides the ability for organisations to technically test how IT and Security teams will operate during high profile cyber incidents, this is a natural evolution to a Desktop Incident Response Simulation. The Technical Incident Response Simulation will start with a technical assessment, after this has been delivered ZeroDayLab will use the results of this to develop the scenario presented to the company.

The output of this exercise will be a report documenting the actions taken, and any recommendations based upon the ZeroDayLab consultant's observations. The following will be performed as part of this exercise:

- Technical Assessment:
  - <Insert scope of test performed such as simulating ransomware activity>
  - Reporting
- Scenario creation and preparation based upon the output of the technical assessment
- Delivery of 4-hour Incident Response Simulation to technical teams to test:
  - Triaging
  - Containment
  - Eradication
  - Recovery
- Reporting and recommendations

The Technical Incident Response Simulation will require days for the assessment, preparation, simulation, and reporting. It is estimated, the Technical Incident Response Simulation will be delivered to a maximum of 25 staff.

3.8 Open-Source Intelligence (OSINT)/Cyber Threat Assessment

The Open-Source Intelligence (OSINT), service attempts to expose the threats currently "in the wild" that could be used to harm the business. To achieve this, ZeroDayLab experienced consultants use recognised real world intelligence techniques to locate any data available within the Deep, Dark, and regular Internet. The objective of the OSINT service is to provide you with visibility into the information that either attackers could utilise to craft attacks and to provide intelligence on threats relevant to the company and its employees. The service will provide the following:

- Workshop and Initial Discovery (2 hour)
  - Setting out the monitoring and alerting over the duration of the assessment
  - Documenting keywords for search
  - Document key threats
- Intelligence gathering and analysis (timeboxed)
- Reporting
- Debrief workshop (up to 2 hours)

3.8.1 Scope of services to be monitored

During the OSINT Exercise ZeroDayLab will monitor the following:

- Domain(s) (Limited to 5 TLD)
  - COMPANY.com
  - COMPANYservices.com
- Key People (Limited to 3)
  - John Smith - CEO
  - Jane Smith -CFO
  - Peter Jones - CIO
- Brands (Limited to 3)
  - COMPANY PLC
  - COMPANY Super-Secret Brand Name
  - COMPANY Super-Secret Service

ZeroDayLab will utilise the following methodology to deliver this assessment

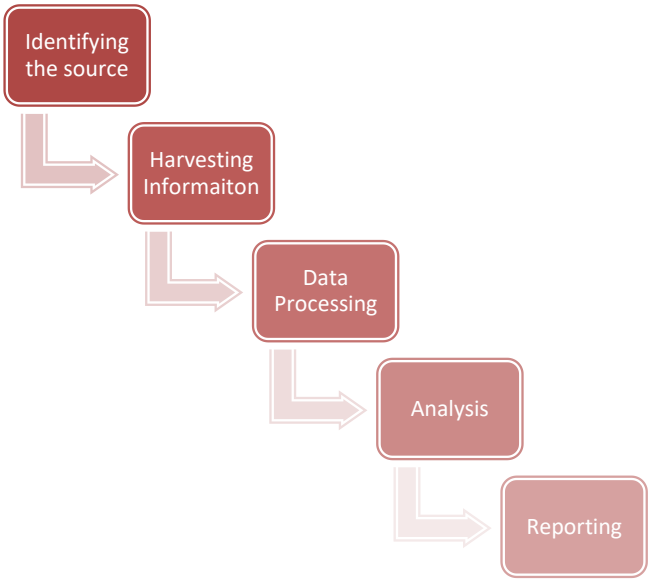


Figure 5: ZeroDayLab intelligence gathering methodology

In addition to the report, a debrief workshop will be held at your offices (or remotely) with the key project stakeholders and key management team members to discuss the findings from the campaign and any recommendations.

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.