

Aftermath Digital Forensics Investigation Service



eWalker Consulting Ltd.

As different services are needed in different IT security stages, we formulated our services into 4 interrelated stages – **Plan, Review, Implement** and **Monitor**. All stages are equally important to the security systems which are worth tackling one by one.

Aftermath Digital Forensics Investigation Service is under the category of **Monitoring Service**. Even for the most sophisticated IT Security systems, there are also chances that the systems may be attacked by worms, malwares or other sources of security incidents. Only with the properly implemented incident handling and investigation procedures, the infected systems could be recovered and backdoors could be identified promptly before affecting other systems. With our wide spectrum of IT system experience, industry domain knowledge and IT security incident handling experience, our consultants would be able to assist you in defining your incident handling and responding procedures. Under certain arrangement, eWalker Consulting team can setup an outsourced incident response and handling services team in annual subscription basis. FORZA framework – a systematic digital forensics investigation framework would be used for our investigation service to identify possible incidents. This can speed up the preparation process in carrying out forensics investigation as well as ensuring the procedures would be forensically sound.

Aims and Objectives

Exploring all tools and designs to minimize external or internal attacks is the basic requirement for security consultants. Through proper handling of security risks, potential issues and attacks could be reduced. However, even though security measures are implemented, there are still chances that the IT systems would be attacked. Nowadays, trojans, spywares, backdoors or botnet could stealthily penetrate and dominate your system. Re-compromise the systems may be resulted in greater negative impact to the organizations. Our consultants would provide advice and support to your team during security incidents according to the pre-requested requirements to identify and verify potential IT incidents. We will also identify and reveal the root cause of the incidents through our tools and our forensics investigation framework. We also preserve the trace for litigation requirement during our investigation process.

Benefits

- eWalker consultants would provide advice and support to your team during security incidents according to the pre-requested requirements to identify and verify potential IT incidents.
- eWalker consultants would conduct post-incident investigation and forensics service to identify the root-cause of the incidents. This reduces the chances of being re-compromised and empower you team to prevent similar attacks.
- Our forensics investigation process followed our FORZA framework which is a widely accepted systematic forensics investigation framework.
- Our consultants preserves evidence in a forensically sound manual

Features

- Following the FORZA framework, the investigation is systematically conducted and performed in a forensically sound manual.
- eWalker consultancy team could reveal and identify the root-cause of the incident and assist your team to rectify the system from the potential issues.
- eWalker forensics specialists with experience in presenting in court could also assist you in the court presentation
- Reports and evidences would be collected and preserved for legal analysis.

Deliverables

As part of the consultation service eWalker's security consultants will deliver:

- In forensics cloning process - cloned and recovered data
- In digital forensics investigation process - digital forensics investigation report

Methodology



Limitation

- The purpose of the reports must be defined prior to the engagement of the project team.
- Unless requested by the client, our consultants would perform standard disk imaging for investigation purpose
- Time event reconstruction and analysis services could be requested as an additional service
- Pre-engagement meeting has to be conducted and deliverables of the project has to be clearly stated during the meeting.

Further details

We have other bundle services and monthly packages, for further details, please contact our **Marketing Team** (marketing@ewalker.com.hk) or logon to www.ewalker.com.hk