DIGITAL FORENSICS AND INVESTIGATIONS

Identify root cause and timeline of a cyber security incident by analysing digital evidence

Improsec offers computer forensic investigation services of malicious outbreaks or cybercrimes, such as intellectual property theft, scams, or vandalism. We can furthermore acquire and zanalyze digital evidence to be used in criminal or civil court.

Our team of cyber forensics experts has vast experience (i.e., law enforcement experience) in providing forensic analysis services and leveraging the latest tools and technologies to carry out detailed computer forensic investigations.

Digital forensics is often performed in connection with Incident Response, but can also be utilized as an individual, reactive task following an incident response e.g. IR carried out by the customer itself or other 3rd party Incident Response Team.

Value

- Identify root cause and timeline of a cyber security incident by analysing digital evidence
- Acquisition of digital evidence to be used in criminal or civil court
- Identify insider or unknown party's malicious intents or actions
- Establish the consequences of the cyber security incident, such as stolen user credentials or intellectual property

Product

The deliverable of the analysis is a written report containing the following:

- A non-technical section with an Executive Summary for management and decision makers
- A technical section describing the performed analysis and the outcome of it
- Recommendations and next steps (if applicable)

Method

The process consists of three stages – acquisition, analysis and reporting:

- During the acquisition stage, we perform forensically sound images of e.g. hard drives by utilizing tools such as hardware write blockers to preserve the state of the original evidence. Memory dumps, network and other logs are also obtained if available (and applicable).
- During the analysis phase, we perform digital investigation on a physical drive, or an image of such, to recover deleted files, identify suspicious files and discover what actions took place (e.g. if data was stolen) by analysing various forensic system artefacts. Furthermore, we can analyse memory dumps to detect advanced malware that leave no traces elsewhere, as well as analyse network traffic to identify potentially suspicious behaviour and detect other intrusions
- All our findings will be documented and reported. After the report presentation, all acquired data and evidence will be handed over to you, after which we will permanently destroy our copy of the data and evidences.

Involvement

The delivery requires minimal involvement of your technical staff.

Improsec A/S
www.improsec.com
Telephone: (+45) 5357 5337
Email: info@improsec.com