DFIR

[SEC]

Identifies the causes and consequences of suspected attacks and security breaches, limiting their consequences

Main benefits

Detect security breaches, reduce their impacts and understand their causes

The Digital Forensics and Incident Response (DFIR) service is the right service to verify security breaches, such as data leaks and other fraudulent activities, allowing the company to gain awareness of the quality and quantity of information and assets that have been compromised, and to avoid extending the perimeter.

Scope

Companies that have been affected by breaches and/or fraudulent activities, or suspect that they have been affected, need to acquire information through investigation and implement timely remediation actions.
The analysis of the causes of the compromise and the impacted area, as well as the isolation of compromised assets, are key activities for the containment of the damage the company has been subjected to.

Challenges facing companies

Whenever a cyber-attack is occurring- or suspected of occurring- the company needs extremely qualified personnel capable of carrying out thorough and exhaustive investigations to answer questions that often have not only an economic, but also a legal retaliation, capable of jeopardising the very existence of the company. Even large companies in almost all cases do not have specialist resources that can carry out the tasks independently.

The advantages offered

The company management gains expert resources to limit the economic, reputational and legal impacts of IT breaches. The IT manager obtains expert support to respond to situations for which he/she is unlikely to have the resources to deal with, especially when the IT department, as well as the entire company, is under extreme pressure.

S2E: approach and proposed methodology

We offer a team of highly specialised experts who combine expertise in Digital Forensics and Incident Response to quickly address and resolve cyber threats. Digital Forensics experts are able to capture information from devices and networks to gather digital evidence of assets that are suspected to have been compromised. Incident Responders reconstruct the chain of events, defining a strategy to contain and mitigate the incident while minimising damage. Our strength lies in being fast, efficient and specialised in both disciplines, in order to support the company in limiting exposure effectively. We collaborate with the company in the preparation of strategies and documentation to respond to requests from regulators following fraudulent activity.

Future development benefits

The main advantages of DFIR are:

1. Specialised and experienced support in situations requiring speed and expertise to safeguard business continuity.
2. Qualified and comprehensive service, capable of responding to the most advanced and complex risk exposures and fraudulent activities.
3. Managerial and technical support in the preparation of documents, analyses and strategies in response to regulatory audits.
4. Timely damage limitation.

Offer model

DFIR is provided as a service. Based on the analysis of the impacted area and the quantity and type of resources involved, the proposal is developed according to the type of support required, between analysis activities and implementation of remediation and response initiatives. In order to make the interventions timely, a feature that makes the difference in situations of exposure of IT resources, we propose activities pre-approved by the company management so that contact can be made immediately with the company technicians to start the activities.