# DFIR

[SEC]

Identifica le cause e conseguenze di sospetti attacchi e violazioni di sicurezza, limitandone le conseguenze

## Principali benefici

### Accerta le violazioni di sicurezza, riducine gli impatti e comprendine le cause

Il servizio di Digital Forensics e Incident Response (DFIR) è il servizio adatto per verificare le violazioni di sicurezza, come fughe di dati e altre attività fraudolente, permettendo all'azienda di acquisire consapevolezza sulla qualità e quantità di informazioni e risorse che sono state compromesse, ed evitarne l'estensione del perimetro.

### Ambito di applicazione

Le aziende che sono state colpite da violazioni e/o attività fraudolente o che sospettano di esserne vittima, necessitano di acquisire informazioni tramite indagini e porre in essere azioni tempestive di remediation.
L'analisi delle cause della compromissione e della superficie impattata, oltre che l'isolamento delle risorse compromesse, sono attività fondamentali per il contenimento del danno a cui l'azienda è stata sottoposta.

### Le sfide che le aziende incontrano

In situazioni di attacco informatico - o sospetto tale - l'azienda necessita di personale estremamente qualificato in grado di portare a termine indagini approfondite ed esaustive per rispondere a domande che spesso hanno una ritorsione non solo economica, ma anche legale, in grado di compromettere l'esistenza stessa dell'azienda. Anche le aziende di grandi dimensioni nella quasi totalità dei casi non dispongono di risorse specialistiche che possono assolvere le attività in autonomia.

### I vantaggi offerti

Il management aziendale acquisisce risorse qualificate per limitare gli impatti economici, reputazionali e legali conseguenti a violazioni informatiche. L'IT manager ottiene un supporto esperto per rispondere a situazioni per le quali difficilmente dispone delle risorse necessarie ad affrontarle, soprattutto in quando il dipartimento IT, così come l'intera azienda, sono posti in condizione di estrema pressione.

# S2E: approccio e metodo proposto

Offriamo un team di esperti altamente specializzati che combinano competenze in Digital Forensics e Incident Response per affrontare velocemente e risolvere le minacce informatiche. Gli esperti in Digital Forensics sono in grado di acquisire le informazioni da dispositivi e reti per raccogliere prove digitali delle risorse che si sospetta siano state compromesse. Gli Incident Responder ricostruiscono la catena di eventi, definendo una strategia per contenere e mitigare l'incidente, minimizzando al massimo i danni. La nostra forza consiste nell'essere veloci, efficienti e specializzati in entrambe le discipline, in modo da supportare l'azienda a limitare l'esposizione in modo efficace. Collaboriamo con l'azienda nella predisposizione di strategie e documentazioni per rispondere alle richieste degli enti regolatori a seguito di attività fraudolente.

## Vantaggi per lo sviluppo futuro

I vantaggi principali di DFIR sono:

1. Supporto specializzato ed esperto in situazioni che richiedono velocità e competenza per salvaguardare la continuità di business.
2. Servizio qualificato e completo, in grado di rispondere alle più evolute e complesse esposizioni al rischio e attività fraudolente.
3. Supporto manageriale e tecnico nella predisposizione di documenti, analisi e strategie in risposta agli audit regolatori.
4. Limitazione tempestiva del danno.

## Modello di offerta

DFIR è erogato come servizio. Sulla base dell'analisi della superficie impattata e della quantità e tipologie di risorse coinvolte la proposta si sviluppa in base alla tipologia di supporto richiesto, tra attività di analisi e implementazione di iniziative di remediation e response. Per rendere tempestivi gli interventi, caratteristica che fa la differenza in situazioni di esposizione delle risorse informatiche, proponiamo attività pre-approvate dal management aziendale in modo da poter immediatamente prendere contatto con i tecnici dell'azienda per l'avvio delle attività.