DETECTION & RESPONSE

Digital Forensics & Incident Response

HOW CAN TELEFÓNICA TECH HELP?

Digital Forensics and Incident Response service helps organisations respond effectively to cyber-incidents

The rise and sophistication of today's cyber threats requires organisations to respond quickly and comprehensively with advanced capabilities that reduce the business impact of a security breach.

These threats, such as APTs or ransomware, can have a high economic, reputational, operational or legal impact, requiring an end-to-end response that helps contain, mitigate and recover from them.

Telefónica Tech, through elite technologies, specialised teams and experience, can minimise the impact of incidents on organisations, as well as on their processes, operations and critical services.

WHO IS THIS SERVICE FOR?

Medium to large organisations that require a fast, efficient and comprehensive response capability but **wish to reduce the financial burden of hiring staff and tools** for DFIR activities.

Organisations with an established incident response capability **looking to outsource or expand the volume of security operations,** reducing costs in a flexible manner.

Companies and public bodies that have suffered an incident, security breach or cyber-attack and need support in response and containment through a team with expertise in malware and forensic analysis, incident coordination, threat intelligence and threat hunting, among others.

OUR VALUE PROPOSITION

Our service

Building a skilled and experienced incident response team is a challenge even for the most mature organisations. Telefónica Tech incorporates this capability through the Digital Forensics and Incident Response (DFIR) service.

Our main objective is to provide help, support and guidance to IT and security teams on security breaches, with capabilities designed to address threats such as ransomware, email compromise, denial of service, data breaches, insider attackers or APTs.

What does it allow you to do?

This service will allow you to:

- **Ensure coordination, containment, investigation and mitigation following a security incident** with the support of an expert team based on a robust methodology.
- Enhance your cybersecurity through **advanced malware analysis and forensics capabilities.**
- Obtain a rapid, effective, and comprehensive response to cyber-crisis to reduce response and recovery times.

Benefits

End-to-end support

Full response during and after the incident, providing close guidance on actions to be taken at technical and executive level.

Based on Threat Intelligence

We take a multi-source intelligence-driven approach to effective investigative responses, validating compromise alerts and serving as the basis for in-depth threat searches.

Dedicated Incident Handler

The incident handler provides comprehensive support and coordination to your teams throughout the entire incident lifecycle, including initial triage, evidence collection and containment recommendations, as well as assistance in building an effective eradication, recovery and communication strategy.

Elite team

Specialised team made up of forensic and malware analysts, threat hunters, incident handlers, network experts, threat intelligence analysts and legal specialists available to assist with investigations.

Telefónica Tech's differential value

Global team with local support and 24/7 availability for rapid response and containment.

Customised response to each situation, through a dedicated incident handler in remote or on-site modality.

Response times and trade discounts when pre-purchasing DFIR workdays.

TEAMS & ACHIEVEMENTS

Our team

- **+30** global forensics and malware specialists.
- **+25** ***threat hunting*** experts.
- **+70** threat intelligence analysts.

Achievements

- +40 **ransomware incidents handled in the last 12 months.**
- 30 minutes: **average initial response time to a crisis.**
- **70.100 IoCs researched** annually and **19 million IoCs** stored in our TIP.
- +8.800 **threat hunting processes** per year **on average.**

BUSINESS MODEL

Based on days, our DFIR service adapts in a flexible and personalised way to the needs of customers with **remote or on-site assistance** and with **8/5 or 24/7 availability** to deal with any situation.

Our **DFIR Retainer modality** offers customers the security of incident response with a trusted partner such as Telefónica Tech, through the **annual pre-purchase of workdays** including response times, special pre-agreed prices with volume discounts, conversion of days not consumed by other services and communication and action protocol with customers.

RELATED PARTNERS

CROWDSTRIKE paloalto NETWORKS

RELATED SERVICES

SIEM Management

Monitoring and correlation of security events with 24/7 alert management, providing a solid foundation in security threat detection.

Managed Detection & Response

Comprehensive endpoint security monitoring through 24/7 detection, containment and rapid response to security breaches with continuous Proactive Hunting and expert cyber-crisis support, based on leading EDR and XDR technology.

Contact us to start the digital transformation of your organization.

2023 © Telefónica Cybersecurity & Cloud Tech S.L.U. All rights reserved.