Telefónica Tech

CYBER THREAT INTELLIGENCE

Cyber Intelligence is essential for your Cyber Security processes

If Cyber Intelligence is enabled across all existing functional teams, it has the potential to help identify, communicate and reduce risk in your organization.

Prevention

- ↑ Increased number of preventive blocks.
- ↑ Increased number and impact of prioritized patches.

Detection

- ↑ Increased number of true positive detections and alerts.
- ↓ Decreased time spent per alert.
- ↓ Decreased number of false positive alerts.

Response

- ↑ Increased number of incidents discovered.
- ↓ Decreased Mean Time To Detection (MTTD).
- ↓ Decreased Mean Time To Remediation (MTTR).

What challenges do companies face?

Cyber Security is no longer a technical problem, but a business challenge. This makes it necessary to deal with cyber threats in an efficient and cost-effective way.

- TARGETED THREATS
- SOPHISTICATED ATTACKS
- BRAND REPUTATION AND INTELLECTUAL PROPERTY
- REGULATORY COMPLIANCE
- INSIDER THREATS
- SUPPLY CHAIN RISKS

How does Cyber Intelligence help companies?

Proactive threat detection
Detect threats before they cause any significant damage.

Competitive advantage
Prove your commitment to cyber security.

Quicker incident response
Respond quicker and more effectively to security incidents.

Regulatory compliance
Meet compliance requirements for data protection and cybersecurity.

Improved risk management
Understand your risk profile and make informed decisions about how to allocate resources to cyber security.

Our value proposition

We help companies identify and reduce their security risks by taking a proactive approach to defending against emerging threats based on responsive intelligence.

- Shed light on the unknown, gaining a broad view of your company's threat landscape.
- Help threat actors invest wisely, mitigate risk, be more efficient, and make quicker decisions.
- Proactively prepare and protect your business, with visibility into trends, stakeholders, and their motivations and TTPs.
- Access a complete portfolio designed to realign the security mindset to that of an attacker.

Our approach based on the type of customer

ATTACK SURFACE MANAGEMENT

Gain complete visibility of your assets from the outside and identify potential attack vectors.

1. Discovery
2. Contextualization
3. Continuous evaluation
4. Prioritization
5. Remediation

DIGITAL RISK PROTECTION

Find out targeted threats that take place beyond your internal perimeter.

- Protection against brand abuse, account takeover, fraud, and IT infrastructure and VIP protection.
- Takedown of fraudulent content and application of countermeasures to minimize risk (browser, network and mobile lines blocking).

THIRD-PARTY RISKS

Continuously measure and monitor third-party security controls to align with your risk tolerance.

- Vendor assessment.
- Continuous monitoring.
- Effective assurance.

COUNTER-INTELLIGENCE

Go one step ahead in active defense with deception campaigns to detect attacks in their early stages.

1. Detect and divert adversaries.
2. Gather threat intelligence.
3. Monitor adversary behavior.
4. Manage informed decision making to remediate the threat..

THREAT INTELLIGENCE

Obtain data-driven information on emerging threats that may be directed against your company.

- Tactical intelligence.
- Operational intelligence.
- Strategic intelligence.

INTELLIGENCE PROJECTS

A bespoke solution to meet your specific intelligence needs.

- Dedicated team.
- Personalized analyst locations and time coverage.
- Comprehensive risk coverage.
- Personalized deliverables based on your needs.