Threat Intelligence Generation
Index

01
Threat Intelligence, what for?

02
Generation of Threat Intelligence

03
Quality metrics of our Threat Intelligence
It is about providing context and reliable indicators to improve prevention, detection and response.
Generation of threat intelligence

We are based on the classic cycle of intelligence

1. **Direction**
   - The needs of our customers are determined in all the verticals and regions where Telefónica has a presence

2. **Collection**
   - Alliances
   - Public sources
   - Private sources
   - Telefónica Products and Services

3. **Processing/Analysis**
   - Processing and analysis of the intelligence obtained to enrich it and make it actionable

4. **Dissemination**
   - Storage, visualization and hunting
   - We deliver the technical/tactical, operational and strategic intelligence to the different products and services that our clients consume

Feedback ➔ Solve Gaps
## Dinoflux Evolution

### Processing technique
- Queries in public sources
- Queries in private sources
- Queries in own sources
- Analysis in Sandbox
- Analysis private AV
- Analysis ML
- Yara rules
- Genetic Analysis

### Capabilities
- Maliciousness verdict
- Extraction of indicators
- Behavioral Telemetry
- Malware family identification
- Threat Attribution
- Aggregated background information such as region or industry affected

### Differential characteristics
- Different angles of analysis provide an accurate and rich view of a threat
- We maintain privacy by not sending files to non-private environments
- Our privileged position as a telco + footprint in 14 countries + mss/mdr services provide very rich context information

The resulting intelligence is of very **high quality** as it includes layers of **technical, tactical, operational and strategic** information.
Quality metrics of our threat intelligence

The Cyber Threat Alliance (CTA) is a non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field.
Quality metrics of our threat intelligence

Our threat intelligence positioned at the top of the industry
Demo time

Dinolux

Storage, visualization and hunting