

THE
**NEW
ERA**

SECURITY INNOVATION
DAYS 2020

Threat Intelligence Generation

Index

01

Threat Intelligence,
what for?

02

Generation of
Threat Intelligence

03

Quality metrics of
our **Threat Intelligence**

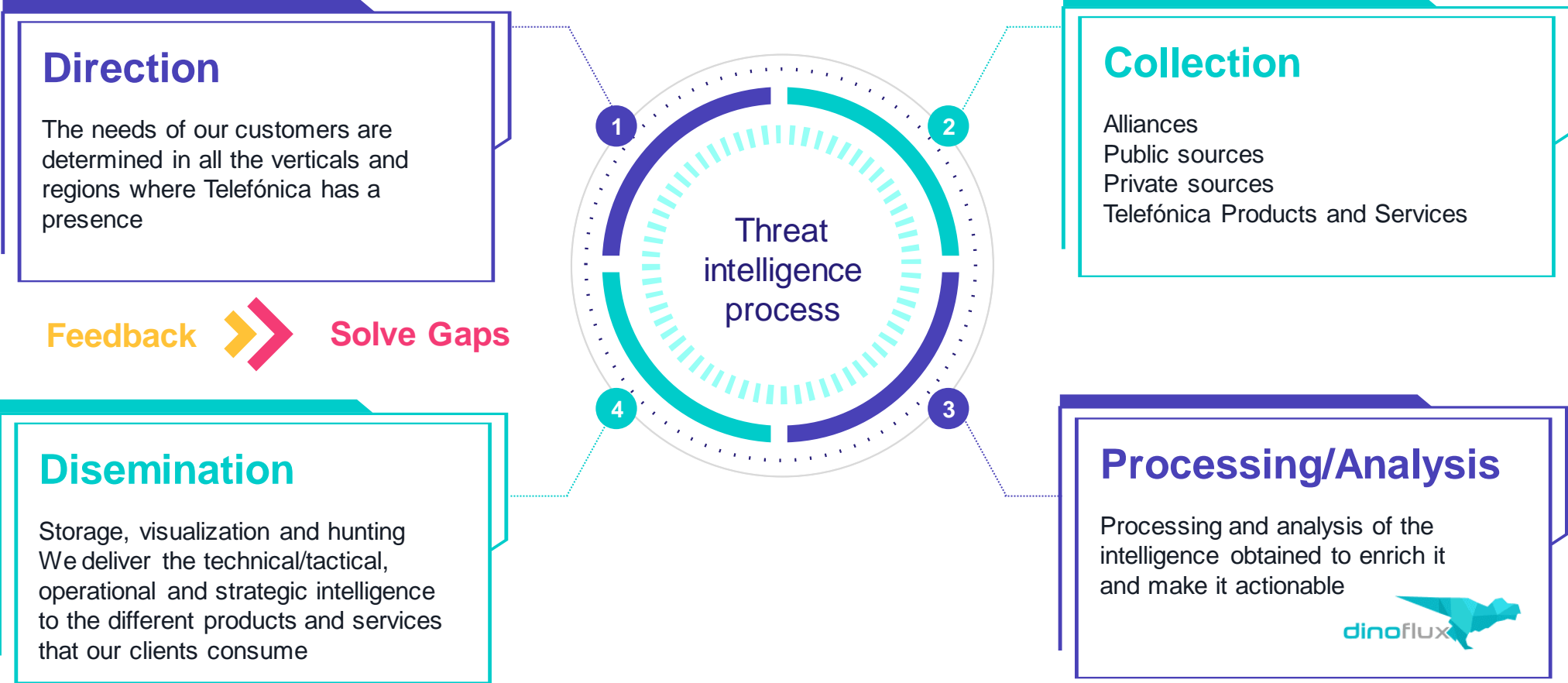


Threat Intelligence, what for?

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



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

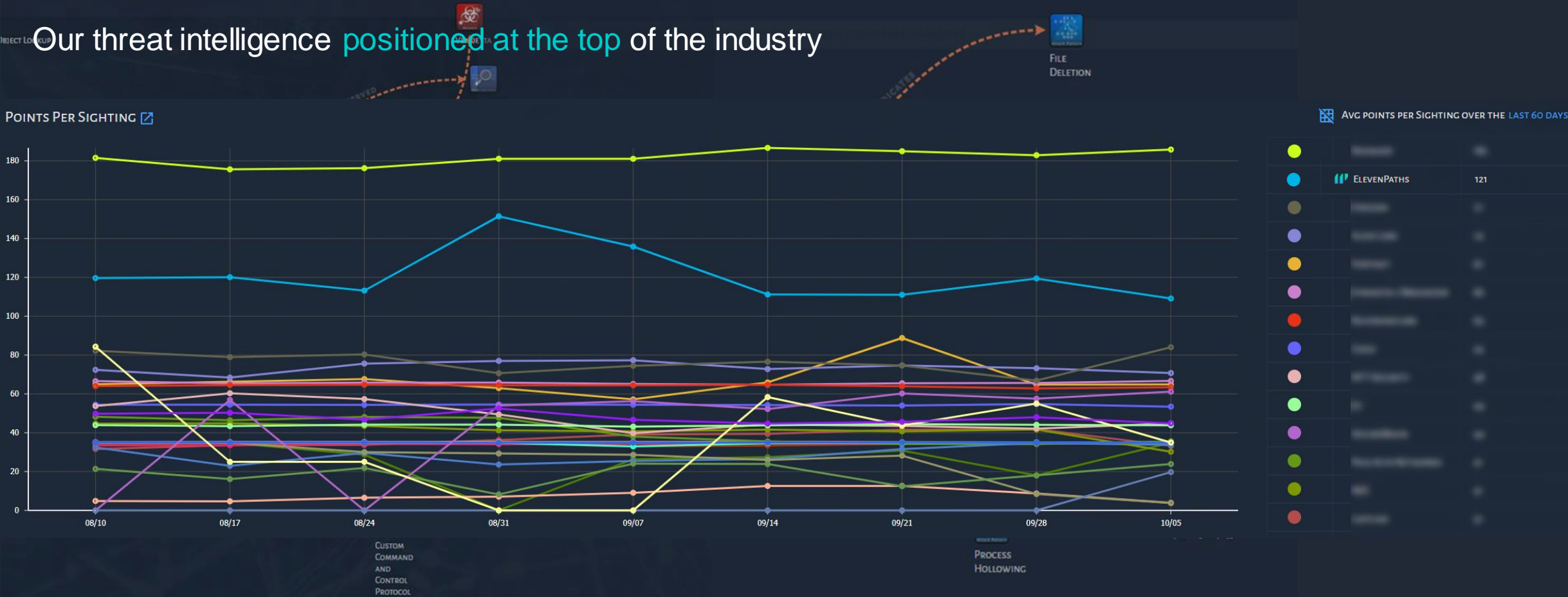
Quality metrics of our threat intelligence



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



Demo time

Dinolux

Storage,
visualization
and hunting





elevenpaths.com

2020 © Telefónica Cybersecurity Tech, S.L.U. Todos los derechos reservados.

La información contenida en el presente documento es propiedad de Telefónica Cybersecurity Tech, S.L.U. ("ElevenPaths") y/o de cualquier otra entidad dentro del Grupo Telefónica o sus licenciantes. ElevenPaths y/o cualquier compañía del Grupo Telefónica o los licenciantes de ElevenPaths se reservan todos los derechos de propiedad industrial e intelectual (incluida cualquier patente o copyright) que se deriven o recaigan sobre este documento, incluidos los derechos de diseño, producción, reproducción, uso y venta del mismo, salvo en el supuesto de que dichos derechos sean expresamente conferidos a terceros por escrito. La información contenida en el presente documento podrá ser objeto de modificación en cualquier momento sin necesidad de previo aviso.

La información contenida en el presente documento no podrá ser ni parcial ni totalmente copiada, distribuida, adaptada o reproducida en ningún soporte sin que medie el previo consentimiento por escrito por parte de ElevenPaths.

El presente documento tiene como único objetivo servir de soporte a su lector en el uso del producto o servicio descrito en el mismo. El lector se compromete y queda obligado a usar la información contenida en el mismo para su propio uso y no para ningún otro.

ElevenPaths no será responsable de ninguna pérdida o daño que se derive del uso de la información contenida en el presente documento o de cualquier error u omisión del documento o por el uso incorrecto del servicio o producto. El uso del producto o servicio descrito en el presente documento se regulará de acuerdo con lo establecido en los términos y condiciones aceptados por el usuario del mismo para su uso.

ElevenPaths y sus marcas (así como cualquier marca perteneciente al Grupo Telefónica) son marcas registradas. ElevenPaths y sus filiales se reservan todos los derechos sobre las mismas.