Servicio de intercambio de ciberamenazas del CERT de INCIBE

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

GOBIERNO DE ESPAÑA

MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

CERT: Público Objetivo

Ciudadanos

Red Académica

Empresas

CERT: Servicios

Detección

Análisis

Respuesta

Notificación

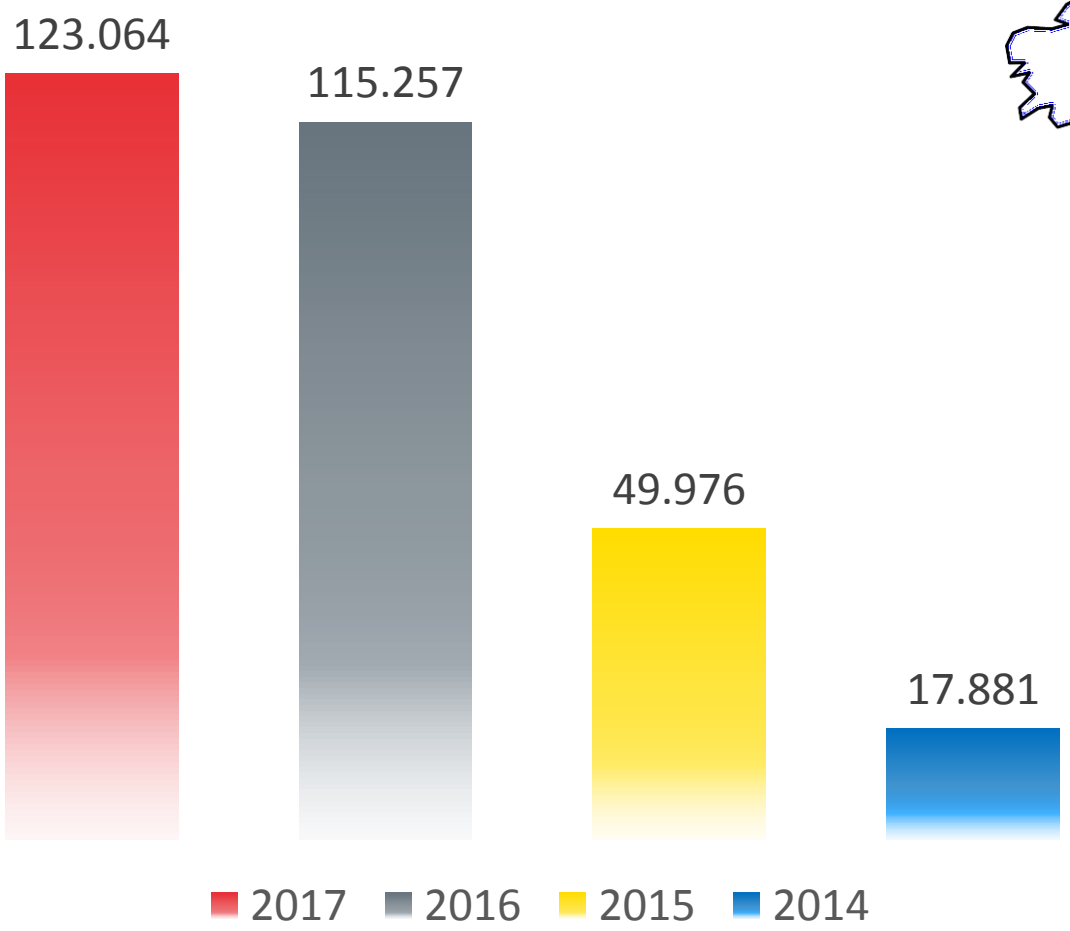
Prevención

Ciberejercicios

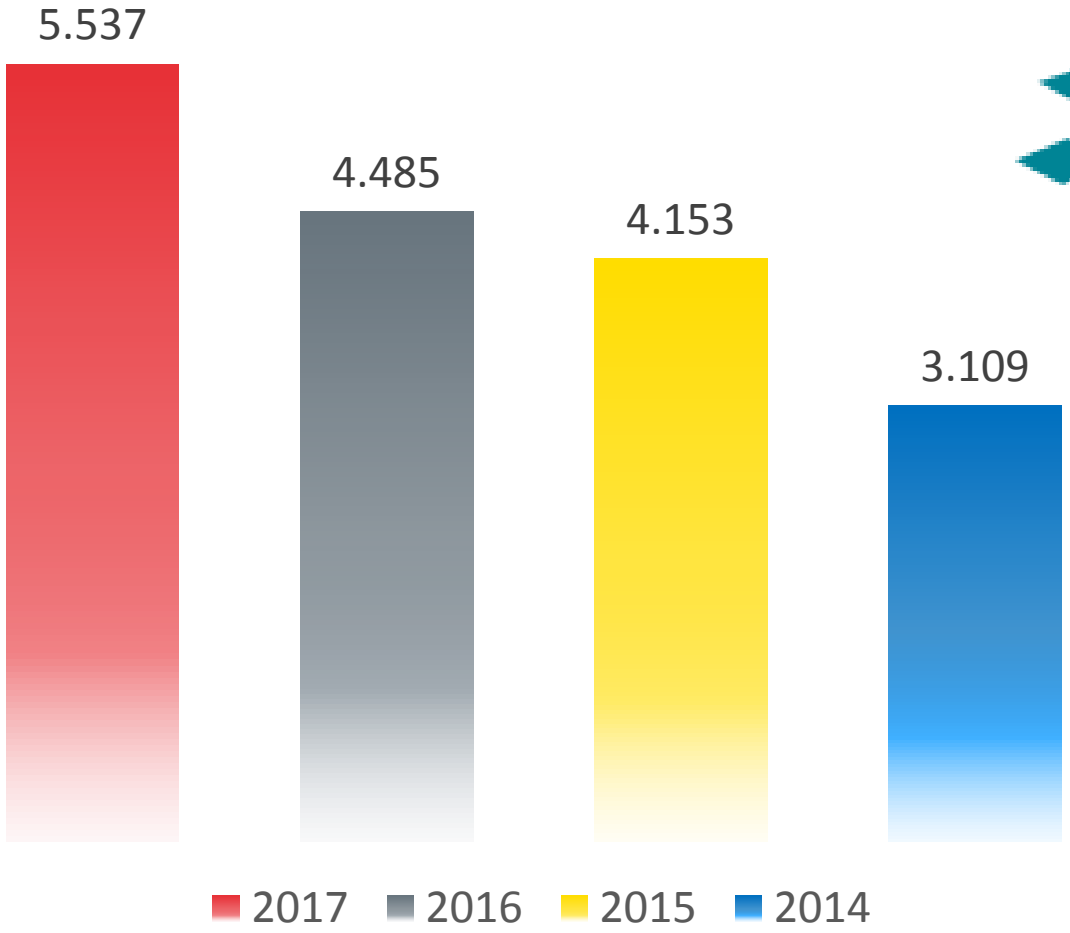
Intercambio de información

Capacitación

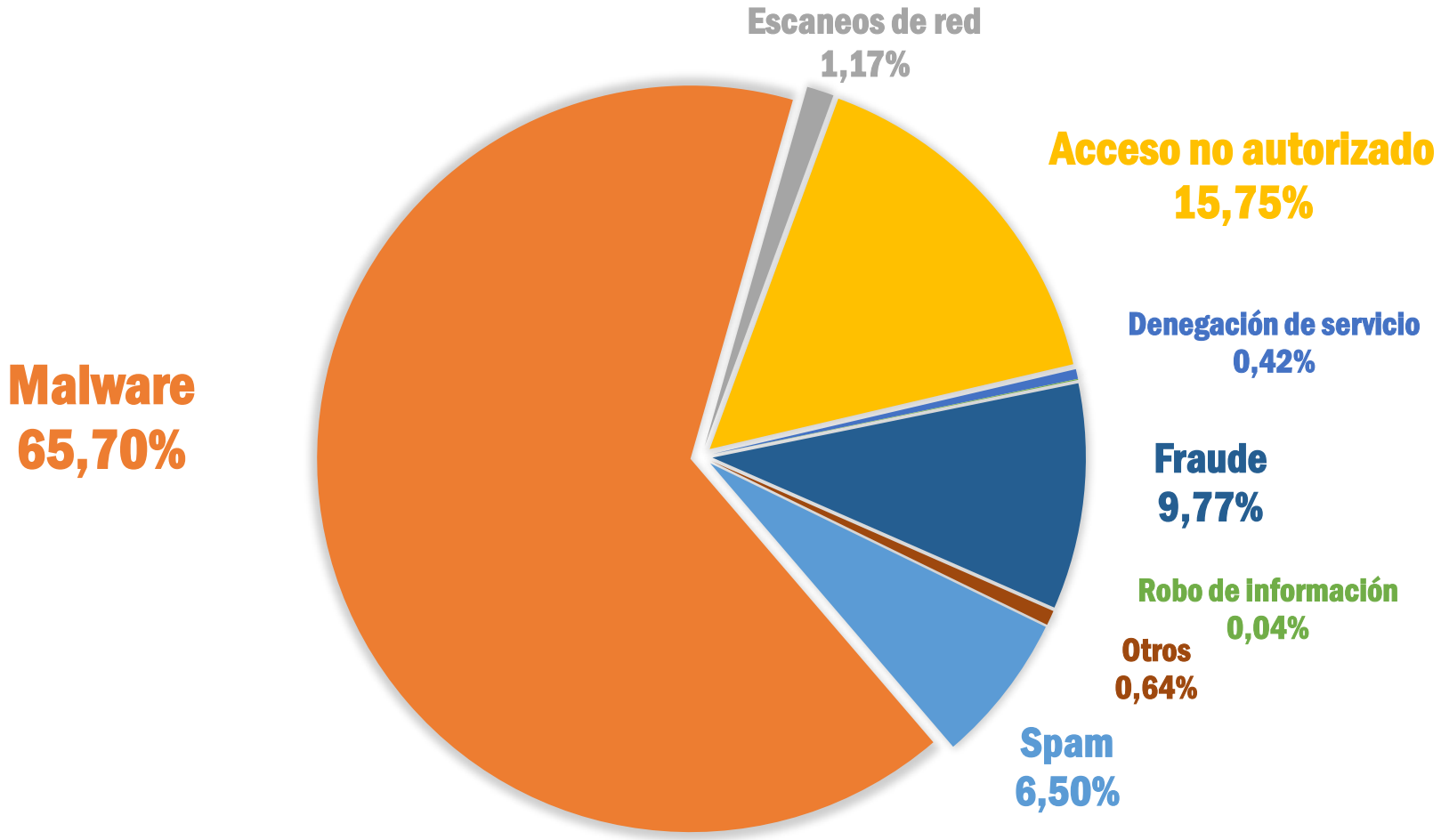
CERT: Incidentes Gestionados



CERT: Incidentes Gestionados II



CERT: Tipos de incidentes



ICARO: Intercambio de información

- Compartir ciberinteligencia entre distintas entidades
- Mejorar el grado de detección en la red de conocimiento
- Establecer un punto neutro nacional
- Facilitar la automatización y la integración

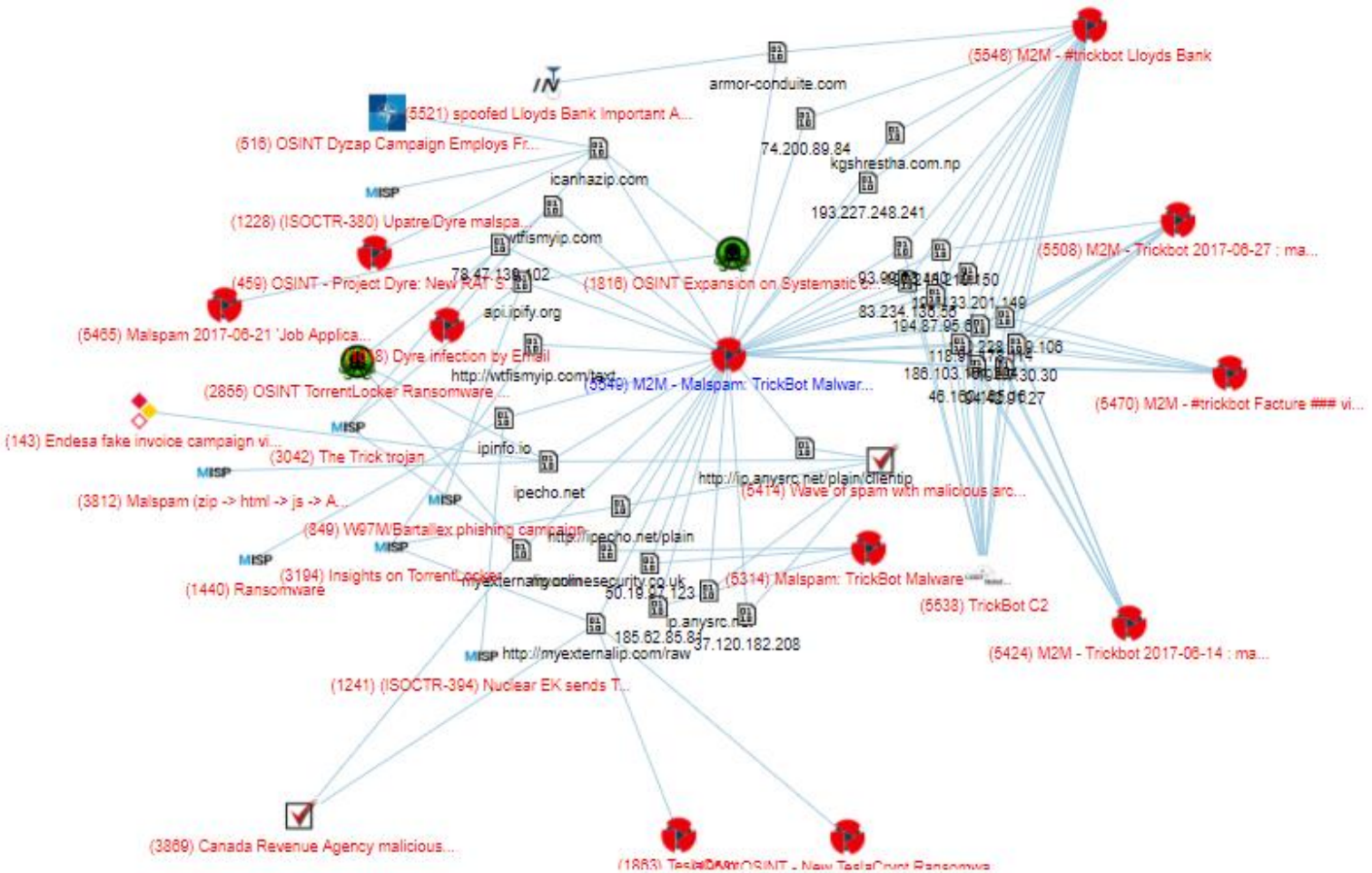
ICARO: Tecnología MISP

Published	Org	Id	Clusters	Tags	#Attr.	Date	Threat Level	Analysis	Info	Distribution	Actions
✔		6761		tlp:green	227	2018-05-02	Low	Completed	CryptoMiner activities - random samples from various misconfigured systems	All	
✔		6760		tlp:green	3	2018-04-30	Low	Completed	Industry targeted phishing	All	
✔	threatbook.cn	6759		APT	59	2018-05-02	Medium	Ongoing	OceanLotus uses office vulnerabilities to launch high-frequency attacks	All	
✔	FINANSCERT.no	6758		tlp:amber	6	2018-05-02	Medium	Ongoing	Threat Hunting: Possible IOC related to Cobalt Group	Organisation	
✔		6762		tlp:green	8	2018-05-02	Low	Completed	Malicious network activity	All	
✔	CERTBw_9014	6757		tlp:white OSINT	31	2018-04-23	Medium	Completed	OSINT: Energetic Bear/Crouching Yeti: attacks on servers	All	
✔	X-ISAC	6755		tlp:white malware very-likely	151	2018-05-01	Low	Completed	OpenDir on compromised server including malware sample	All	
✔		6756		tlp:white technical-report	128	2018-05-01	Low	Completed	OSINT - HOGFISH REDLEAVES CAMPAIGN HOGFISH (APT10) targets Japan with RedLeaves implants in “new battle”	All	
✔		6754		tlp:white very-likely mobile-malware	1505	2018-04-26	Low	Completed	OSINT - HenBox: Inside the Coop	All	

Powered by MISP 2.4.84 and operated by CERTSI

certsi_

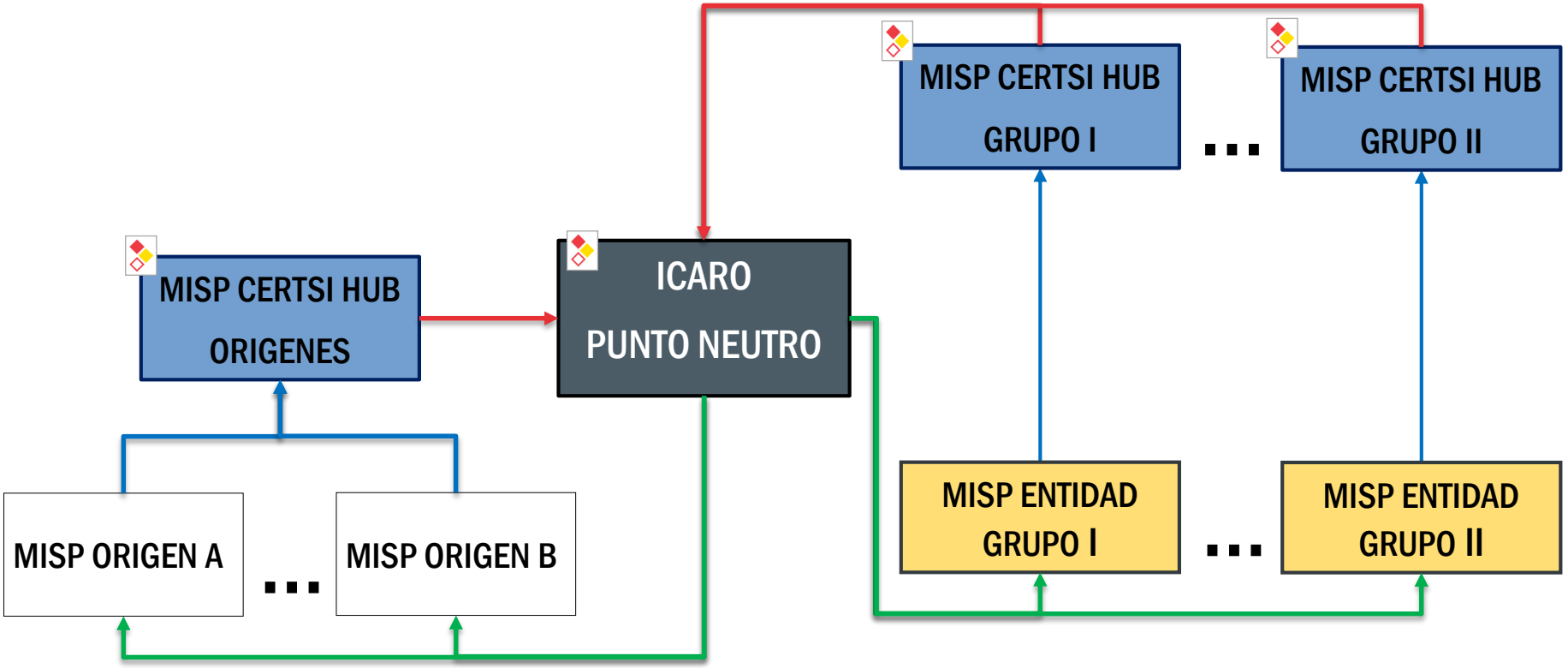
ICARO: Correlación



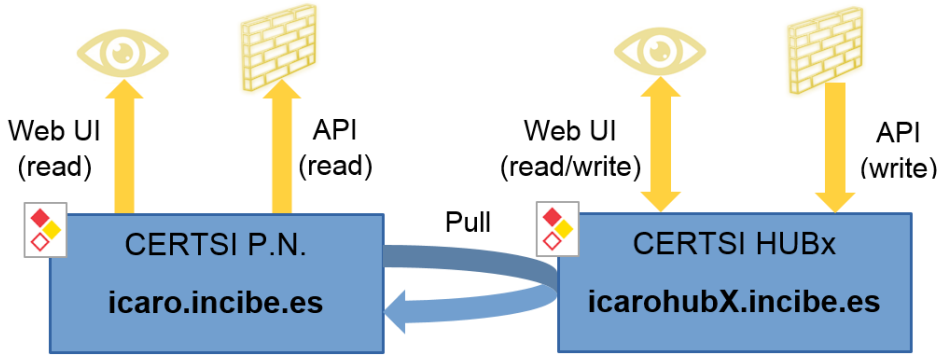
ICARO: Funcionalidades

- Formatos de exportación:
  - NIDS (Snort, Suricata, Bro)
  - OpenIOC
  - CSV
  - STIX
  - RPZ Zone
  - CEF
- Módulos de expansión:
  - passive DNS/SSL
  - countrycode / geoip
  - CVE
  - Virustotal
  - Shodan
- Formatos de importación:
  - OpenIOC
  - GFI sandbox
  - CSV
  - STIX
  - Sandbox (Cuckoo, …)
  - Email metadata
- Feeds
  - Abuse.ch
  - Malwaredomainlist
  - PhishTank
- API REST y librería PyMISP

ICARO: Arquitectura

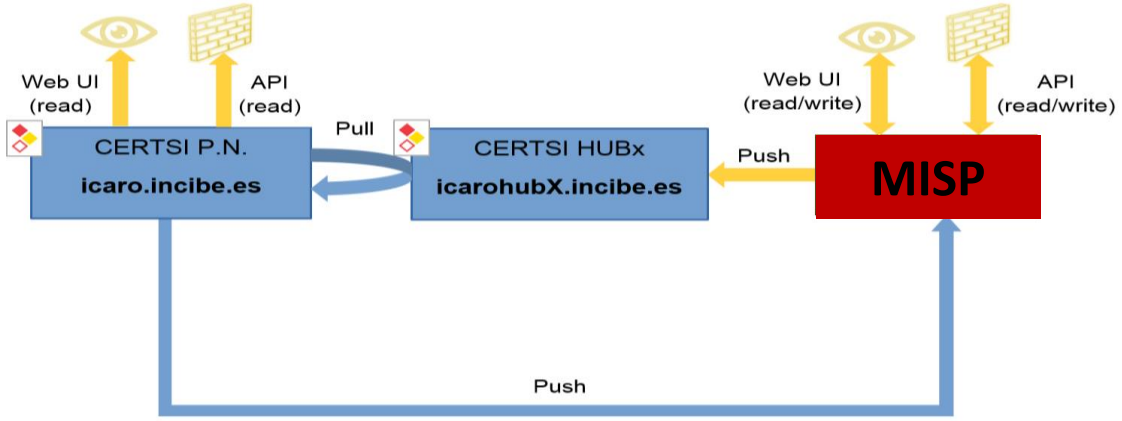


ICARO: Tipos de acceso

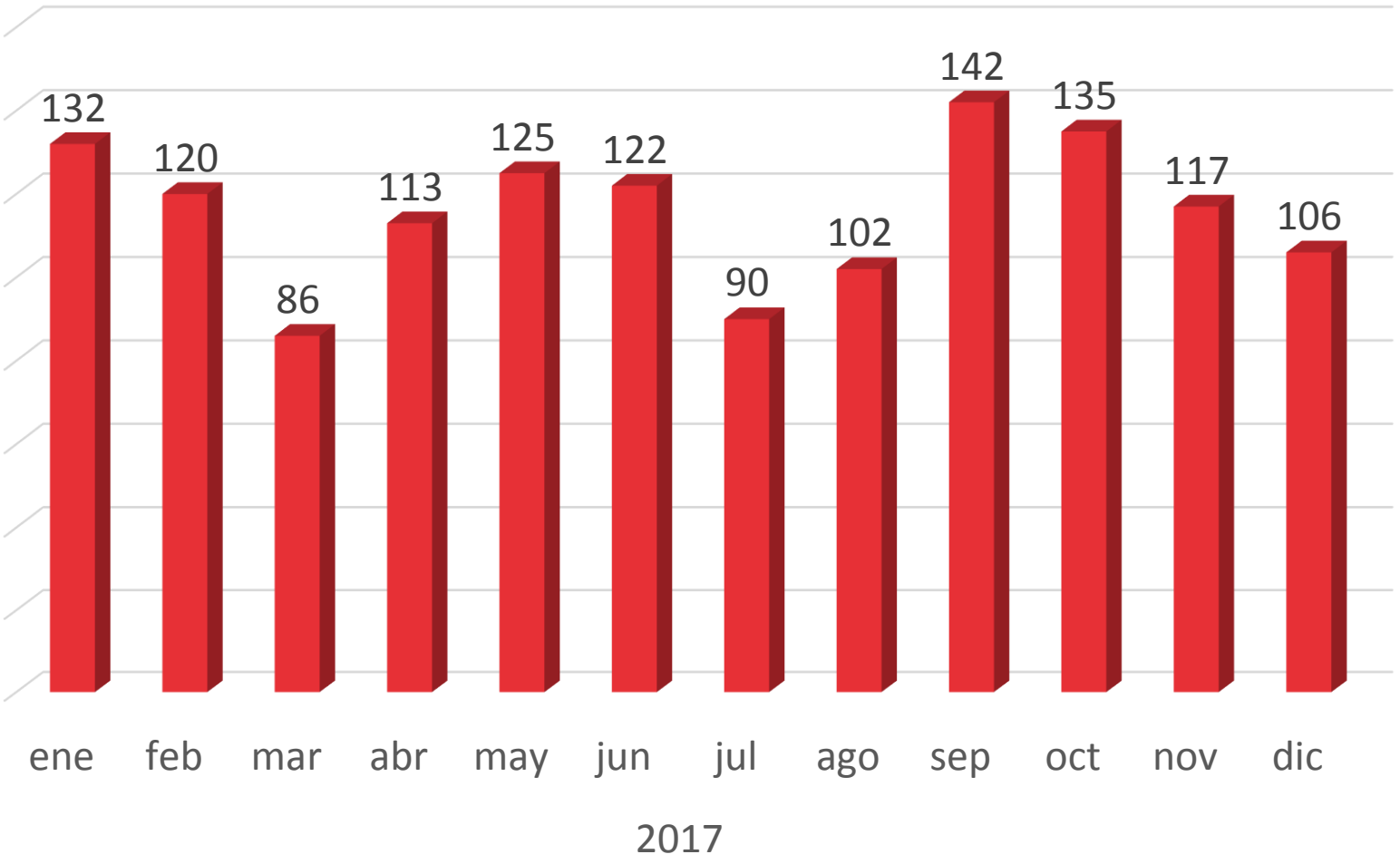


A través de WEB / API

A través de MISP



ICARO: Amenazas



ICARO: Solicitud de acceso

icaro@certsi.es

Gracias por su atención

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD