vicomtech
visual interaction & communication technologies

IK4
Research Alliance

“Aplicación del Big Data a la Ciberseguridad"

Octubre 2017

IK4
Research Alliance

AZTERLAN | CEIT | CIDETEC | GAIKER | IDEKO | IKERLAN | LORTEK | TEKNIKER | VICOMTECH

vicomtech
visual interaction & communication technologies

- **Datos relevantes** www.vicomtech.org
  - 119
  - 42
  - 8,2 M€
- **Ubicación**

  Parque Científico-Tecnológico en Donostia-San Sebastian

- **Especialización**
  - Advanced Interaction
  - Computer Vision
  - Data Analytics
  - Computer Graphics
  - Language Technologies

Contexto

- Larga trayectoria en el programa de I+D en seguridad de la UE
- Centro tecnológico con mayor retorno de investigación en España en H2020 seguridad 2014-2016(1)
- Miembros de las principales asociaciones a nivel EU:
  - EARTO, participando activamente en el grupo de seguridad
  - ECSO - CyberSecurity PPP(2)
- Proyectos en curso
  - Suceso / hazitek estratégico / 8 socios / 2017-2019 / ciberseguridad
  - Titanium / h2020 / fct / 15 socios (5 lea; incluidos interpol y policía nacional) / 2017-2020 / dark net y criptomonedas / eu_restricted
  - Asgard / h2020 fct / 33 socios (12 lea) + importantes stakeholders: europol + enfsi + interpol + ertzaintza / 2016-2020 / eu_restricted / tech for lea (digital forensics, intelligence, foresigh) / vicom coordinator
  - Sekutek / elkartek / 8 socios / 2017-2019 / ciberseguridad
  - haziteks competitivos …

(1) http://eshorizonte2020.cdti.es/recursos/doc/Programas/Cooperacion_internacional/HORIZONTE%202020/43596_235235201716543.pdf
(2) https://www.ecs-org.eu/ *(via IK4 research alliance)*

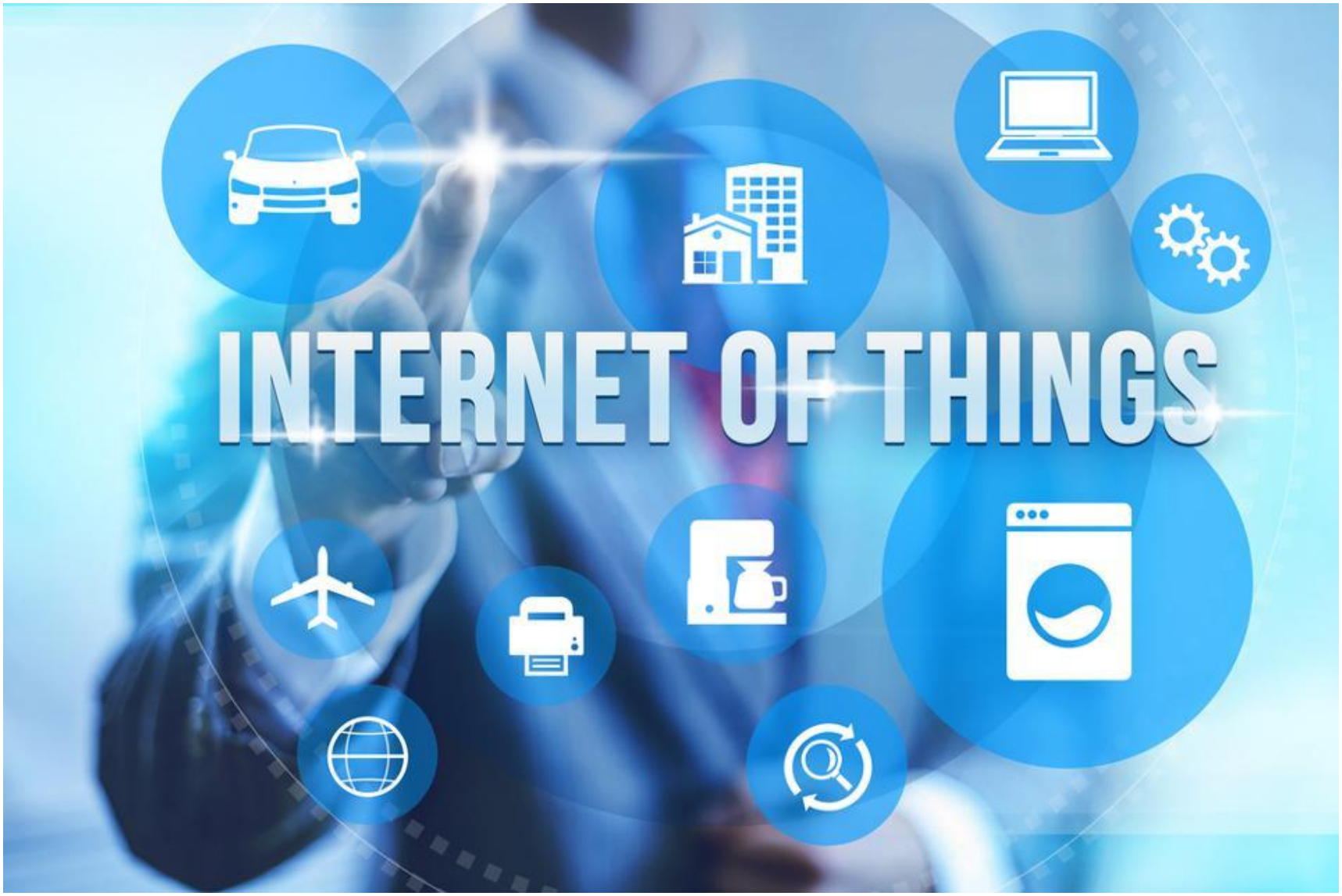
vicomtech
visual interaction & communication technologies

Nuestros socios hablan por nosotros

Aplicación del Big Data a la ciberseguridad

vicomtech
visual interaction & communication technologies

Vivimos en un mundo hiperconectado



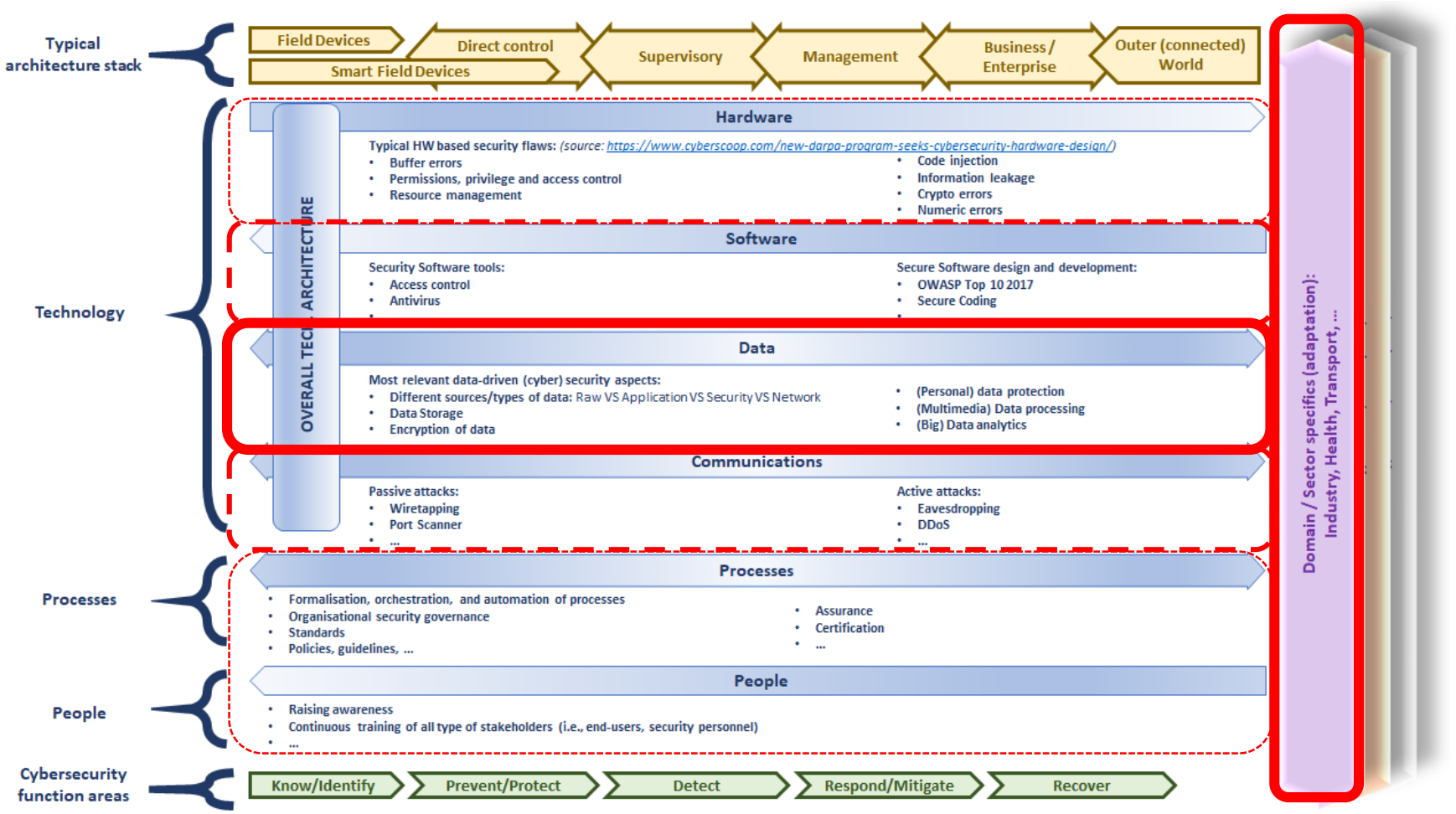
Posibles fuentes de riesgo

DDoS
Ransomware
Vulnerabilidades
BYOD (bring your own device)
Equipos obsoletos
SW & HW no autorizado
Visitas, subcontratas, personal externo
Fuga de información
Ingeniería social
Fraude al CEO
Empleados descontentos, ex-empleados
Dispositivos móviles
…

5 funciones de ciberseguridad

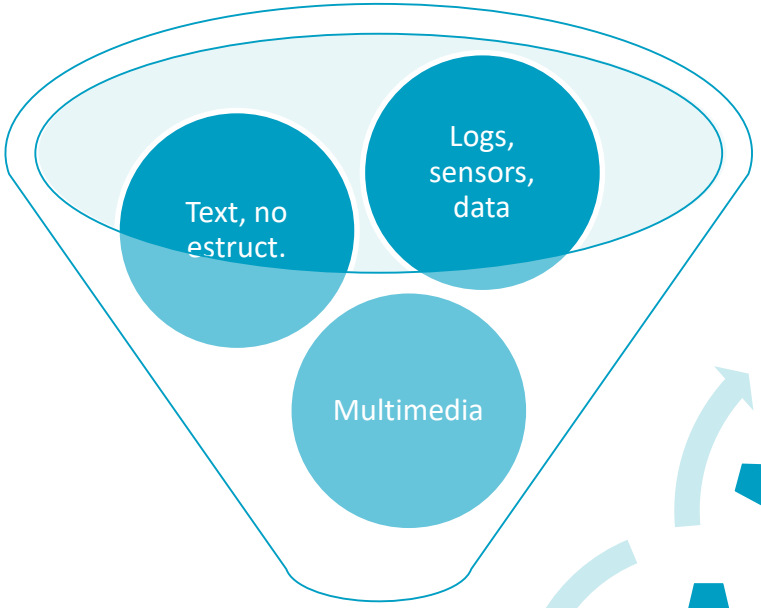
Identificar	Proteger	Detectar	Responder	Recuperar
•Comprender el contexto. Conocer los activos y riesgos	•Aplicar controles para mitigar riesgos	•Control y monitoreo	•Reducir el impacto de un potencial incidente	•Resilencia y recuperación ante incidentes

Visión desde Vicomtech



vicomtech
visual interaction & communication technologies

Analítica de datos



Real time, heterogeneos, grandes volumenes. no estructurados, multimedia

Indicadores de compromiso

"… consiste en definir las características técnicas de una amenaza por medio de las evidencias existentes en un equipo comprometido, de manera que puedan servir para identificar otros ordenadores afectados por la misma amenaza o prevenirlos de la misma."

Claves para su detección:

- Patrones de tráfico inusuales
- Anomalías en la actividad de la cuenta de usuario con privilegios
- Irregularidades geográficas
- Banderas rojas (errores repetidos de autenticación)
- Incremento de accesos de lectura a bases de datos
- Tamaño del HTML de respuesta más grande del habitual
- Un gran número de solicitudes para el mismo archivo
- Utilización de puertos de acceso inusuales
- Modificaciones en el sistema de archivos
- …

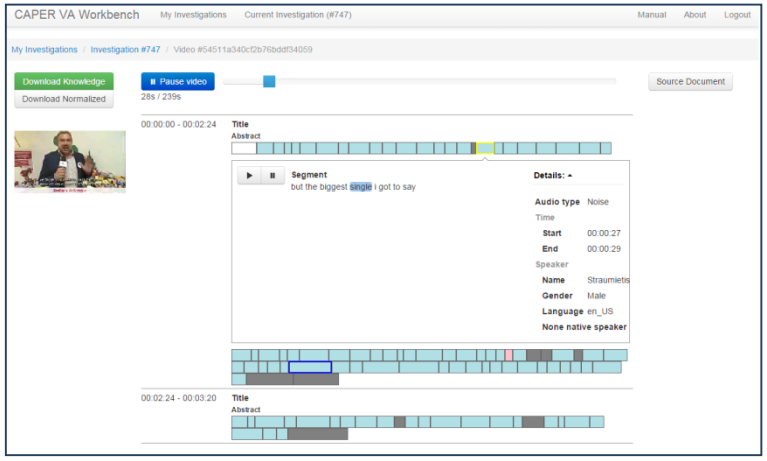
vicomtech
visual interaction & communication technologies

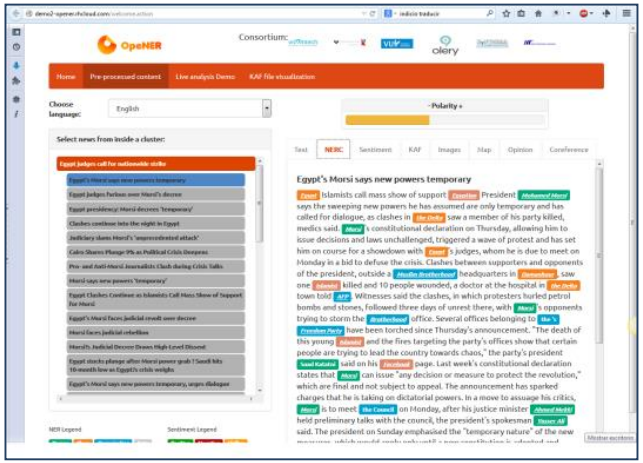
Ejemplos de actividades de Vicomtech:

	2011	2012	2013	2014	2015	2016	2017
Security	CAPER	SAVASA	P-REACT	INSPECT	asgard	Ti H2020	EWISA Early Warning for Increased Situational Awareness
	• Intelligence • OSINT • Many LEAs	• Forensics & Policing • Video archive, search and analysis	• Policing (Petty crimes) • Low cost intelligent video surveillance	• Policing • Enhanced community policing	• Foresight, Intelligence & Digital Forensics • LEAs' tech autonomy • New collaboration approach	• DarkNet • Crypto-currencies • Criminal activities	• Border Control • Computer vision
Related		OpeNER	SAVAS		Cloud-LSVA		TransSec
		• Natural Language Processing • 6 languages • Easy to adapt and integrate tools	• Subtitling • 7 languages • Transcriptions and respeaking system		• Large scale (Big Data) video analysis • Automotive industry		• Transport security • Autonomous emergency manoeuvring and movement monitoring

Open Source Intelligence:

- Video analysis > audio analysis > text analysis
  - **Scene** segmentation
  - **People** detection, tracking, and identification
  - **Complex events** detection
  - …
  - **Multilingual**
  - Voice recognition
  - **Speaker** identification
  - Automatic Speech Recognition (**transcripts**)
  - …
  - **Multilingual**
  - Natural language processing
  - **Entity** recognition
  - Entity **relationships**
  - **Machine translation**
  - …





Evolución colectiva

Dirigente de un Banco americano:

- ¿Qué han hecho cuando han tenido algún incidente de seguridad?
- Nunca hemos tenido un incidente de seguridad
- …pero ¿qué harían si lo tuvieran?
- Decir que nunca hemos tenido un incidente de seguridad

Tendencias en ciberseguridad 2017 (McAfee Labs):

El compartir inteligencia de amenazas observará un gran progreso en 2017
Ej: http://www.openioc.org/, https://cyboxproject.github.io/, https://www.iocbucket.com/ …

vicomtech

visual interaction & communication technologies

Xabier García de Kortazar

IK4 Research Alliance

AZTERLAN | CEIT | CIDETEC | GAIKER | IDEKO | IKERLAN | LORTEK | TEKNIKER | VICOMTECH