

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva



Monitorización de la red:

- Webinar
- Target profiler
- Dark web monitor

Selva Orejón



Selva Orejón



@selvaorejon



Directora ejecutiva de onBRANDING y CELEBrandSEC

- ✓ Perito judicial especializada en Identidad y Reputación digital y Ciberinvestigación.
- ✓ Licenciada en Ciencias de la Comunicación por la Universitat Ramon Llull.
- ✓ Diplomada en Business Organization and Environment, University of Cambridge.
- ✓ Diplomada en Inteligencia al Servicio del Estado y la Empresa, UIA.
- ✓ Profesora en la Universidad de Barcelona UB en el Máster de Ciberseguridad, impartiendo Ciberinteligencia – OSINT, y en la Escuela de Policía de Catalunya, (Ciberinvestigación y Protección de la identidad digital).

selva@onbranding.es





Índice

1. Briefing y Keywords
2. Namechk y acciones posteriores
3. Herramientas SONDA
4. Análisis del punto cero
5. Alertas tempranas
6. Casos de estudio
 - a. Ultras en Final de un evento deportivo
 - b. Identificación de un reclutador de ISIS
 - c. Predicción del tiroteo de Alexandria
 - d. DarkWeb monitor



1) Briefing y keywords



Briefing y keywords

La monitorización tiene un doble uso, reputacional, de seguridad y privacidad para la empresa, los empleados y para evitar espionaje industrial.

1. 1) Escoger palabras clave
 - 5 familias de palabras clave
 - Diferencia entre:
 - Monitoring de la persona y su entorno
 - Monitoring de la empresa.
 - Incluye múltiples personas y entornos



2) Namechk y acciones posteriores



Namechck

- Hacer búsqueda por nombres de usuario para proteger la marca (personal o corporativa), para evitar usurpaciones, suplantaciones de identidad y estafas.

Legend: ● Available ● Unavailable ● Error ● Invalid

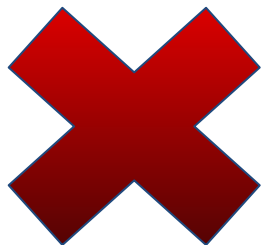
Please share Namechk! [f](#) [t](#)

Names: [Sort By: Rank](#) [Download Results \(CSV\)](#)

Facebook	YouTube ✓	Twitter ⚠
Instagram ✓	Blogger	GooglePlus ✓
Reddit ✓	eBay ✓	Wordpress ✓
Pinterest ✓	Yelp ✓	PayPal ✓
Slack ✓	Github ✓	Vine ⚠

Identificación de contenido potencialmente de riesgo

Eliminación de contenido



Reclamación de contenido



Reservar usuarios y dominios de riesgo potencial





Identificación de contenido potencialmente de riesgo

- Eliminación de contenido



Google

Search Console

Panel de control

Mensajes

► Apariencia en el buscador

► Tráfico de búsqueda

▼ Índice de Google

Estado de indexación

Recursos bloqueados

Eliminación de URL

► Rastreo

Problemas de seguridad

Otros recursos

Eliminación de URL

Elimina **temporalmente** tus URL de los resultados de búsqueda. Para eliminar el contenido de forma [información](#)

Ocultar temporalmente

Introduce la URL de tu sitio web que quieras ocultar (se distingue entre mayúsculas y minúsculas)

Continuar

[DMCA \(Copyright\) Complaint to Google](#)

October 15, 2015 *Walt Disney Company* on behalf of *Disney Enterprises, Inc.* → *Google Inc.*

Walt Disney Company

Disney Enterprises, Inc.: Once Upon A Time

Disney Enterprises, Inc.: Once Upon A Time

Disney Enterprises, Inc.: Once Upon A Time

Disney Enterprises, Inc.: Once Upon A Time

Disney Enterprises, Inc.: Quantico

DMCA NOTICES, COPYRIGHT

[DMCA \(Copyright\) Complaint to Google](#)

April 07, 2015 *Walt Disney Company* on behalf of *Disney Enterprises, Inc.* → *Google, Inc.*

Walt Disney Company

Disney Enterprises, Inc.: Grey's Anatomy

Disney Enterprises, Inc.: Revenge

Disney Enterprises, Inc.: Maleficent

Disney Enterprises, Inc.: Cinderella (2015)

Disney Enterprises, Inc.: Castle

Identificación de contenido potencialmente de riesgo

- Reclamación de contenido, usuarios y dominios





Identificación de contenido potencialmente de riesgo

- Reservar usuarios y dominios de riesgo potencial





3) Herramientas SONDA



Identificación de contenido potencialmente de riesgo

- Estableceremos diferentes tipos de monitorización para estar siempre alerta del riesgo potencial del contenido publicado sobre: organizaciones, marcas comerciales, personas, instalaciones y edificios, y temáticas sensibles.



INSTITUCIONES



MARCAS COMERCIALES



MARCAS PERSONALES



INSTALACIONES Y EDIFICIOS



TEMÁTICAS SENSIBLES



Identificación de contenido potencialmente de riesgo

- Tipos de monitorización:



TARGET PROFILER

1. Crear perfiles target
2. Tracking de dispositivos
3. Identificar conexiones sociales



PERSON OF INTEREST

1. Watch list (eventos, temas)
2. Alertas temáticas y de fuentes



GEO TARGET MONITOR

1. Mapping de usuarios
2. Reconocimiento facial de usuarios determinados



WEBINT PROFILER

1. Focused Data
2. Textos
3. Crawler
4. Extracción De Fuentes



Identificación de contenido potencialmente de riesgo

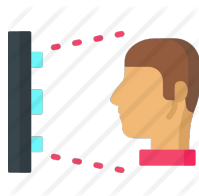
- Tipos de monitorización:



DARKWEB MONITOR



DARKNET INTELLIGENCE



FACE ANALYTICS



4) Análisis de punto cero



Identificación de contenido potencialmente de riesgo

- Informe que Incluye
 - De qué se habla (temas)
 - Temas críticos
 - Temas recurrentes
 - Dónde se habla (espacios)
 - Webs
 - Blogs
 - Redes
 - Foros
 - Audios...
 - Con qué CONTENIDO
 - Texto e Imágenes
 - Videos y Audio
 - En qué tono (famoso sentiment)
 - Quién lo dice (AUTORES)
 - Cuándo dicen (CADENCIA)



INFORME DE MONITORIZACIÓN PARA DEPARTAMENTOS INTERNOS (Reputación online)

El informe de monitorización es un documento muy importante, como bien se sabe la reputación es una disciplina absolutamente transversal para la compañía por tanto debe ser tratada con suma habilidad.

La **monitorización** sólo nos va a aportar **datos**, el **analista** es quien nos va a ayudar a convertirla en información y en **inteligencia para la compañía**, ésta debe ser transmitida de forma **digerible** y **útil** para las personas que la vayan a recibir, por tanto se tendrá que hacer la pregunta previa **¿qué necesitan saber? ¿qué queremos que sepan?**

Mi propuesta es preguntarse:

- Cadencia del informe
- Tipo de informe (tema concreto, crisis, punto 0, status conversación diaria...)
- Largada
- Textual y visual
- Lectores (nivel de conocimiento del medio 2.0 y de la compañía)

La idea es que aún comunicando la información no les dejemos con la idea de que hay un problema y ya, si lo identificamos, pensemos en soluciones planteables.

Informe tipo:

- Breve introducción de la conversación detectada, 3 ítems de información, 4 máximo.
- Espacios online donde se haya detectado mayor conversación, por ejemplo, en la blogosfera es donde más de habla de... los usuarios de foros por lo general... *(Saber dónde hay más conversación nos ayudará a saber dónde desarrollar la estrategia, detectar cuantos recursos serán necesario y sobre todo pensaremos si tiene sentido o no tener activos allí).*
- **Mapping de comunidades aliadas y detractoras:** Identificar influencia del medio (lectores, antigüedad dominio, autor, suscriptores, viralidad "ej. eco 2.0 de 20minutos.com"...
- **Mapping de influencers,** fruto de la escucha identificaremos aquellos usuarios que sea influenciadores (conocer su grado de influencia)



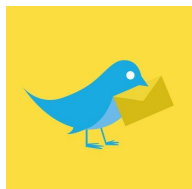
5) Alertas tempranas



Alertas tempranas

Sobre nuestro objetivo de investigación o para proteger un bien (empresa, VIP, idea...)

- Google alerts, Twilert, Tweetdeck, Websays, oteara, mention, alerti...
- Niveles de alerta y notificaciones de éstas (SMS, llamada inmediata, email...)



Ejemplo de clasificación de alerta de contenido

RASTREO - Palabras clave	ACTUACIÓN RESULTANTE en base al riesgo para: 1.Integridad personal / 2. reputación personal 3.Reputación profesional	
Nombre y Apellidos (1 nombre + 1 apellido) (1 nombre + 2 apellidos) (2 nombres + 2 apellidos)	Integridad personal/ compañeros * URL	Reputación personal / profesional * URL
	Reputación profesional * URL	Reputación del cuerpo * URL
Pseudónimo/Nick / Id		ACTUACIÓN A REALIZAR SOBRE EL CONTENIDO RASTREADO Mantener Desposicionar Retirar (inminente)
DNI		
TIP / TIM		
Teléfonos (móvil, casa)		
Emails (actuales y pasados) (personal y profesional)		



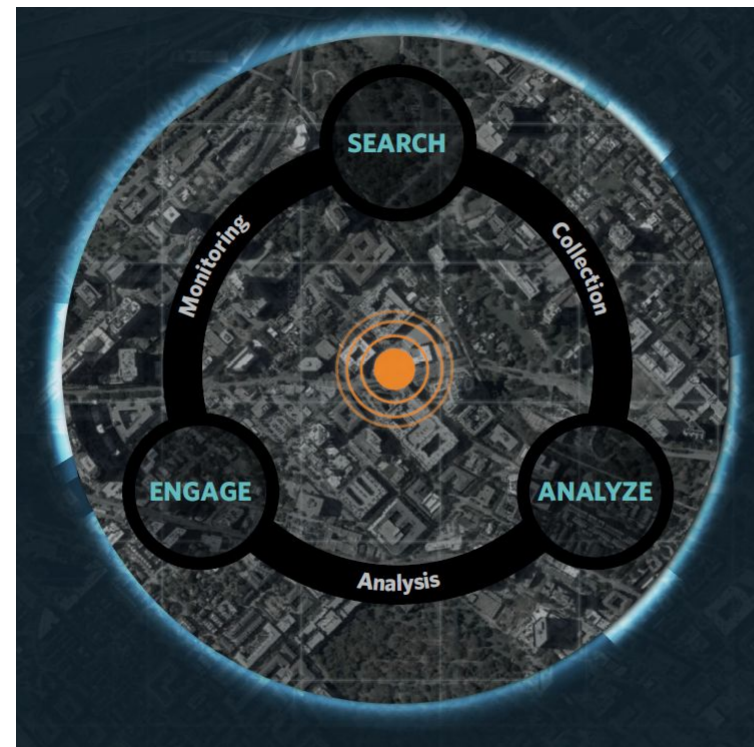
6) Casos de Estudio



Casos de estudio

La monitorización en el ámbito de seguridad recalca el valor de la proactividad en contra de la reactividad.

1. Final de un evento deportivo de gran magnitud.
2. Identificación de un reclutador del ISIS en el de Europa.
3. Predicción del tiroteo de Alexandria, Louisiana.





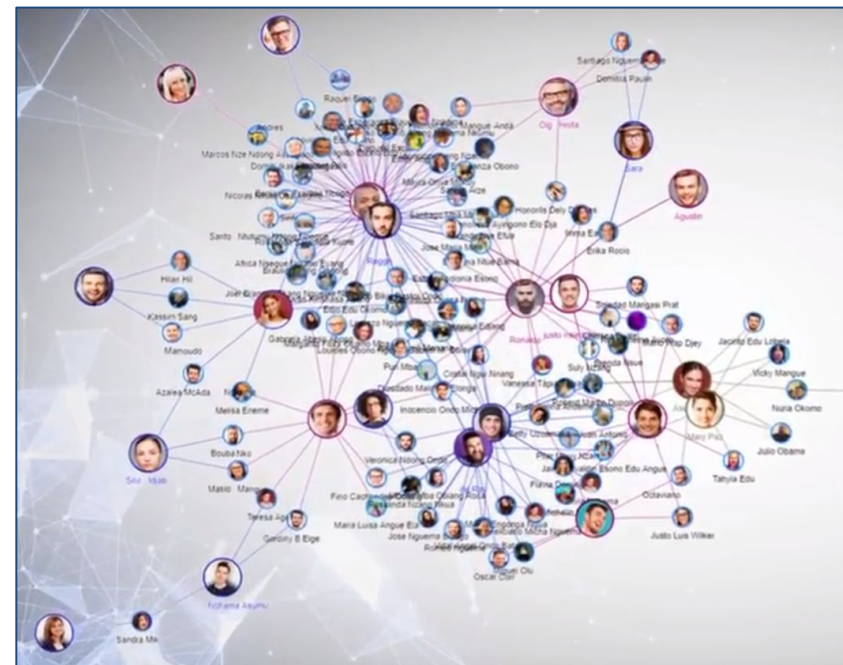
Casos de estudio

Final de un evento deportivo internacional.

Se realizó una investigación de perfiles con historial de violencia de ambos clubs.

Se añaden hashtags y palabras clave con sus alertas para poder identificar los actores que movilizan los colectivos violentos.

Una vez identificados, se monitoriza su actividad en la red en tiempo real





Casos de estudio

Final de un evento deportivo internacional.

La monitorización sigue hasta los días previos al partido, para poder entender si se está planeando algún acto violento.

La monitorización es simultánea en redes sociales, canales de mensajería como telegram y deepweb.



Algunas de las capturas de pantalla de esta presentación están pixeladas por motivos de privacidad.

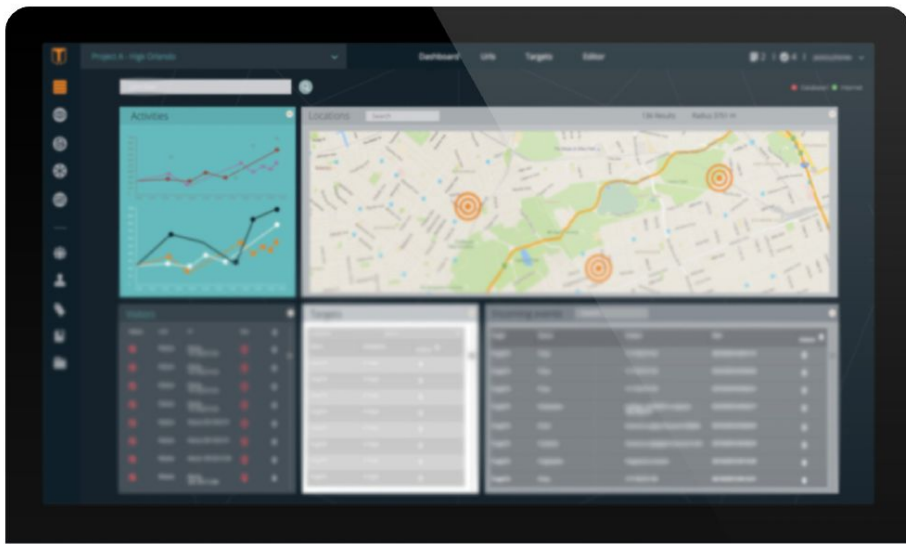


Casos de estudio

Identificación de ultras en la final de un evento deportivo internacional.

Se identifica un actor potencialmente peligroso que pueda provocar actos violentos.

Se realiza un seguimiento de su ubicación antes del inicio del partido, a través de fotografías, etiquetas en RRSS, geoetiquetas del actor y de otros usuarios.





Casos de estudio

Descubriendo un reclutador del ISIS en el sudeste de Europa.

Una agencia de inteligencia alerta sobre dos terroristas que fueron a combatir a Siria, se conocen sus perfiles en RRSS.

Se quiere conocer el resto de la célula que aún se encuentra en el país.

Las cuentas no tenían prácticamente publicaciones, ni fotografías y muy pocos amigos. Además de ello llevan inactivas mucho tiempo.



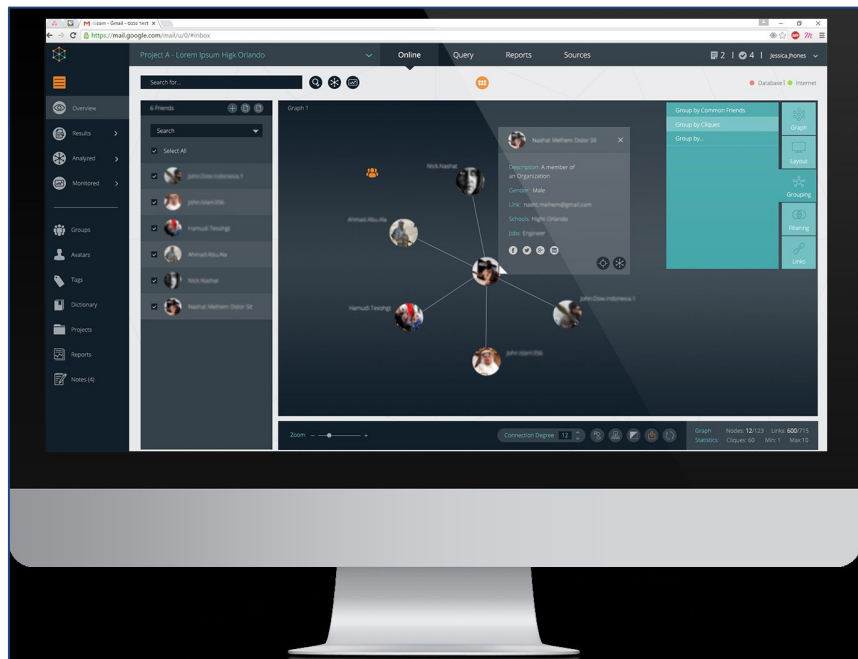


Casos de estudio

Descubriendo un reclutador del ISIS en el sudeste de Europa.

Con el uso de IA se analizaron las distintas interacciones entre perfiles, se fueron descubriendo más perfiles afines al grupo terrorista.

En medio de toda esa maraña se encontró un perfil muy activo, con más de 2000 “amigos”, muchos de ellos residentes en el país dónde se realizaba la investigación.





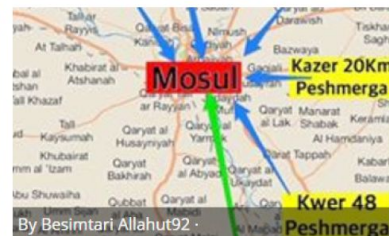
Casos de estudio

Descubriendo un reclutador del ISIS en el sudeste de Europa.

El perfil descubierto resultó ser un gran promotor de la causa del ISIS en la red.

Se trataba muy posiblemente de un reclutador que enviaba ayudaba a radicalizar a través de internet y facilitaba rutas de llegada a territorio del ISIS.

Toda la información fue puesta en conocimiento de la agencia de inteligencia y al poco tiempo el perfil fue cerrado.





Casos de estudio

Predicción de los actos terroristas.

Caso del tiroteo de Alexandria, Louisiana.

La generación de información en la red es tan grande que un analista no puede ejecutar su labor sin un buen sistema que analice y priorize los datos.

En este caso, el atacante, James T. Hodgkinson preparó con esmero su plan. Estuvo dos meses viviendo en una furgoneta en la calle para preparar su objetivo.





Casos de estudio

Predicción del tiroteo de Alexandria, Louisiana.

Hodgkinson a pesar de dormir en la calle era muy activo en las redes sociales y demostraba un gran odio hacia el partido republicano.

Con el uso de sistemas como el procesamiento de lenguaje natural, no solo podemos captar palabras claves, también las emociones hacia un sujeto o idea.



Casos de estudio

Predicción del tiroteo de Alexandria, Louisiana.

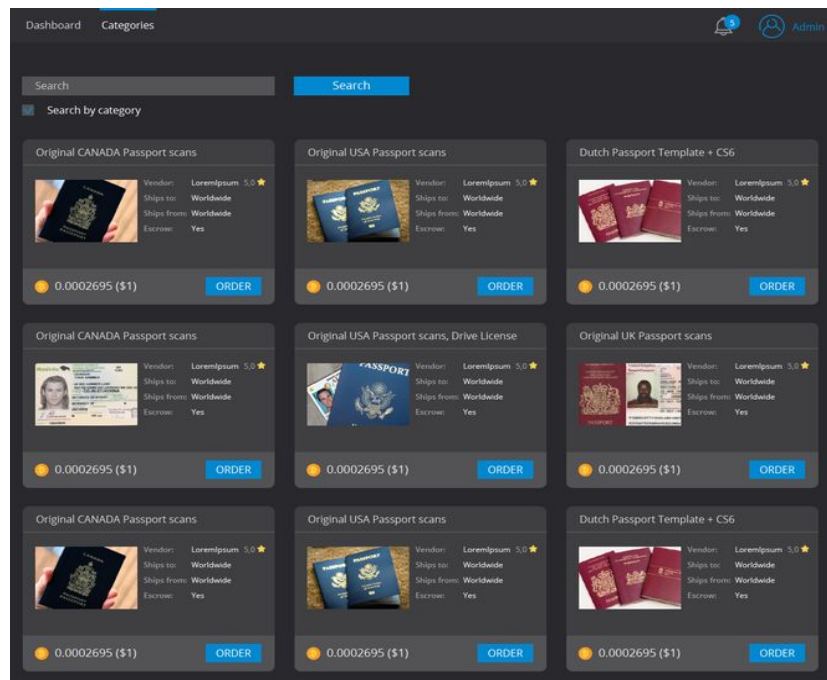
Si combinamos con el procesamiento de lenguaje natural, análisis de imágenes así como un sistema de alerta por cambios de rutina podemos obtener un sistema de alertas para la prevención de crímenes.





Dark web monitor

- Falsificaciones
- Electrónica
- Joyas
- Suministros de laboratorio
- Defensa
- Bienes digitales
- Drogas
- Servicios:
 - Hacking
 - Identidades falsas
 - Divisas
 - Retiradas de dinero



GRACIAS POR LA ATENCIÓN ¿Dudas y preguntas?

@selvaorejon

selva@onbranding.es

@selvaorejon

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva



E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- oc.ccn.cni.es

Síguenos en

