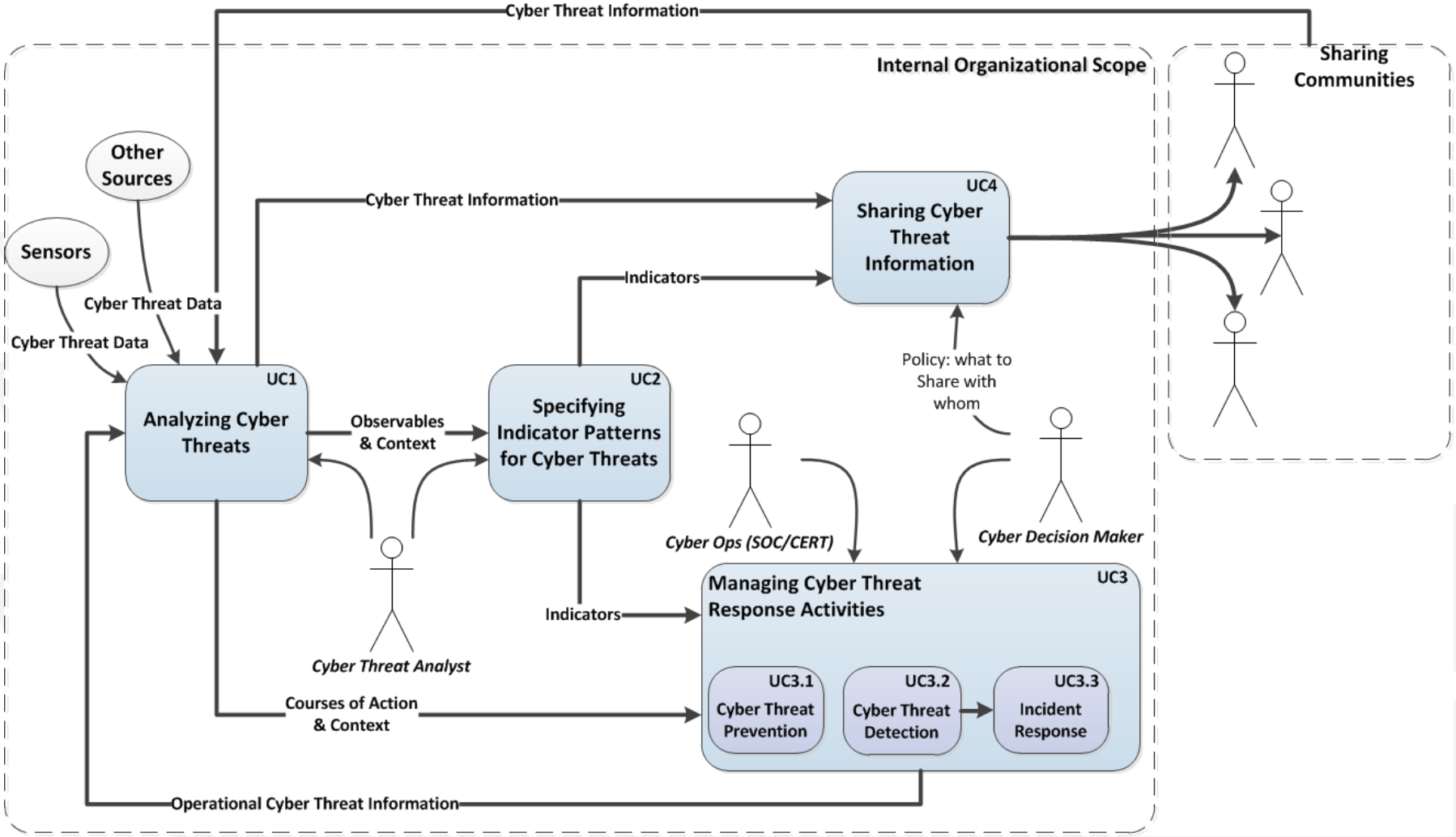
Ciber-Inteligencia

Factor determinante en un CSIRT

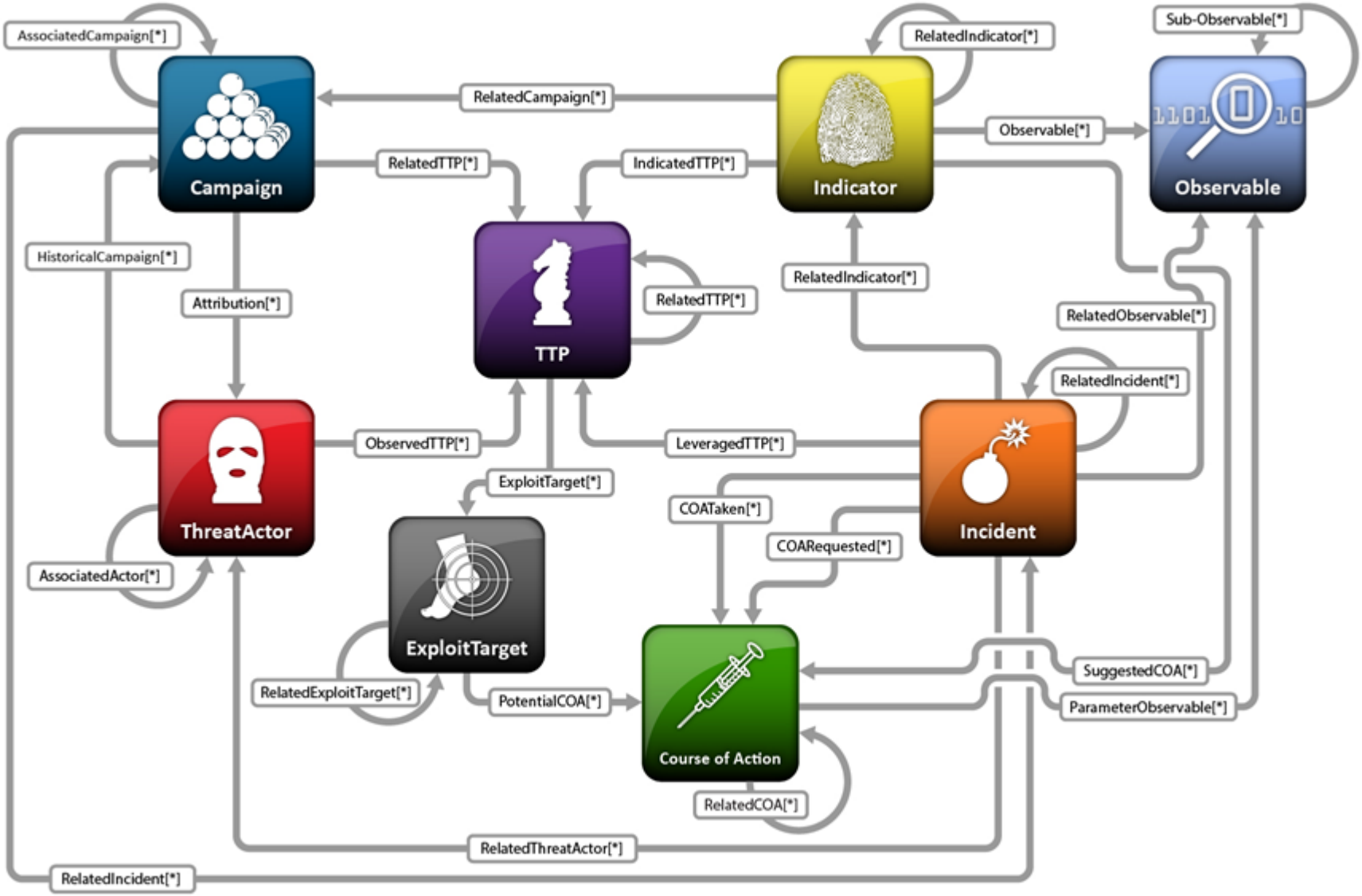
Elihú B. Hernández Hernández

Especialista en Cyber-Seguridad

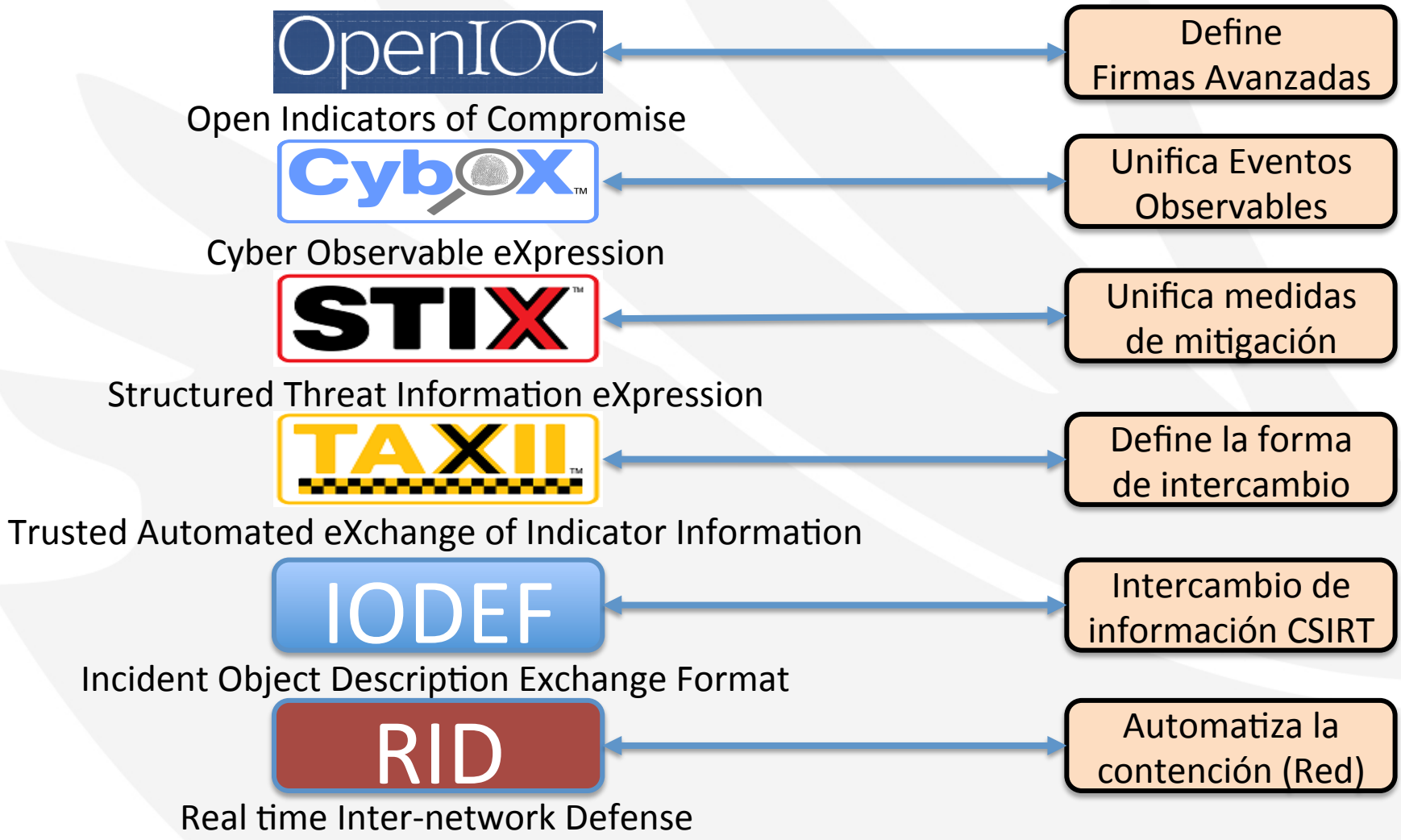
Modelo de Ciber-Inteligencia



Arquitectura de Ciber-Inteligencia



Frameworks de Ciber-Inteligencia



Generando Ciber-Inteligencia

Las fuentes de información OSINT son fuentes de información de acceso libre, gratuitas y desclasificadas

Fuentes de Información OSINT

Web Searching Tools

News

People

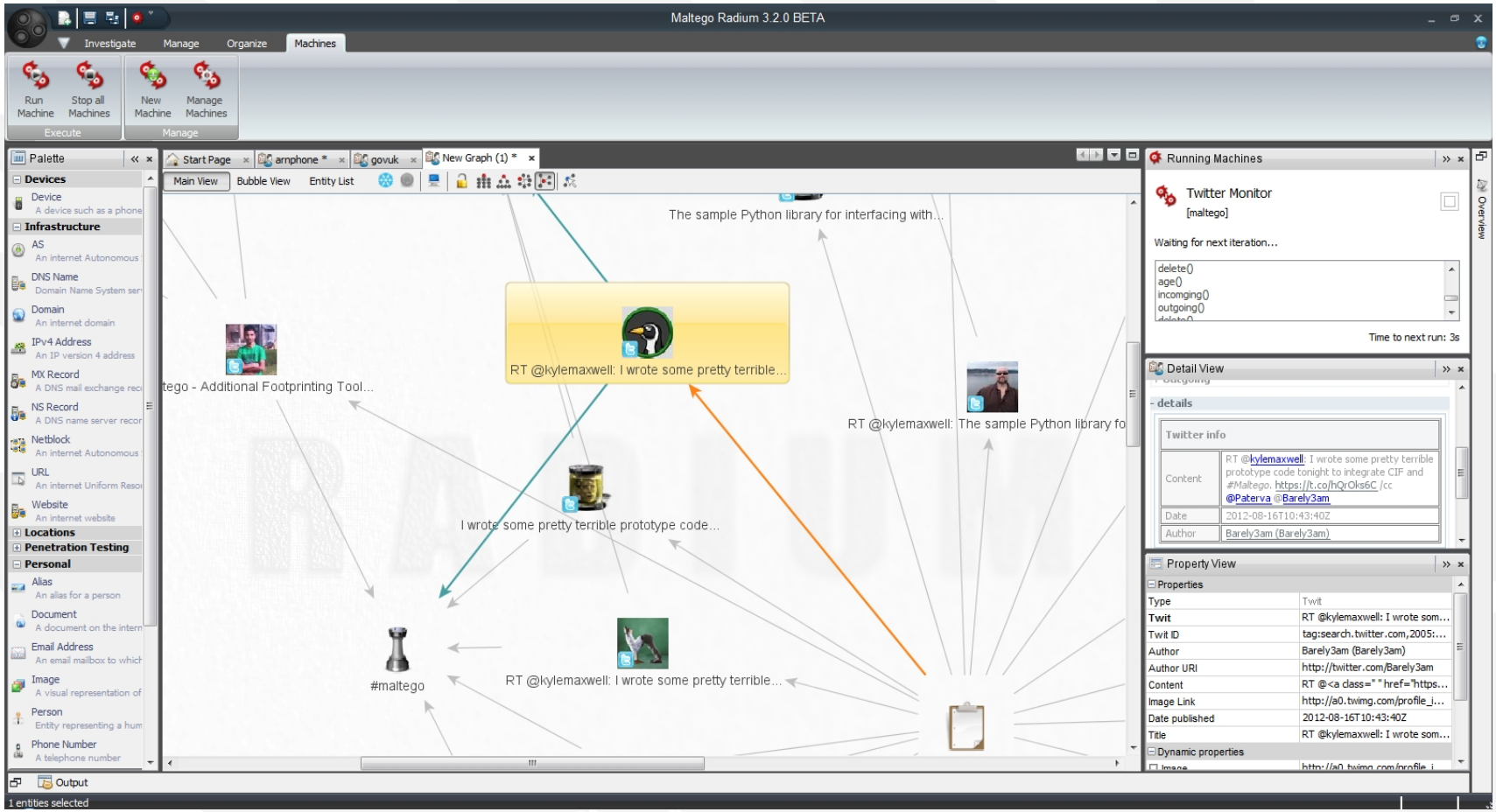
Multimedia

https://inteltechniques.com/links.html

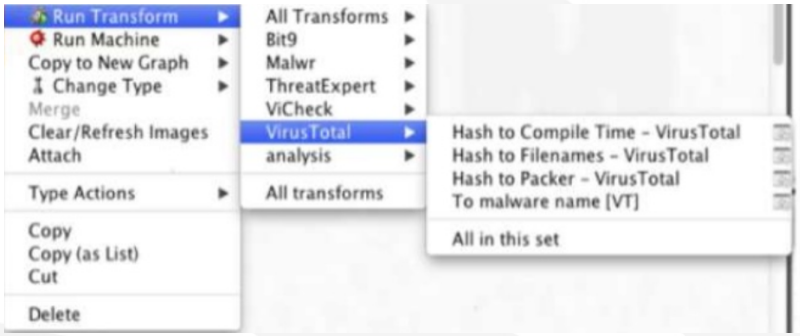
Generando Inteligencia de fuentes no disponibles

INTERNET ARCHIVE
WayBackMachine

MALTEGO



Generando Inteligencia de fuentes no disponibles

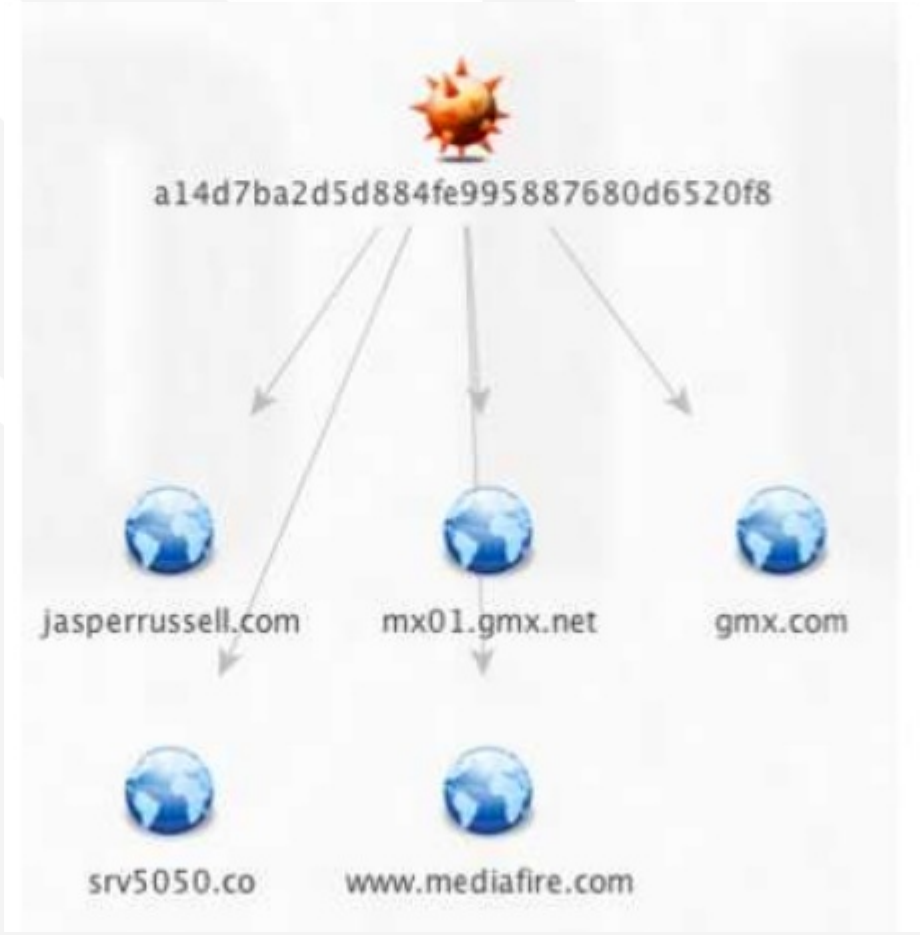


Bit9

malwr

ThreatExpert

VIRUS TOTAL



https://github.com/digital4rensics/Malformity

Utilizando Buscadores Especializados

SHODAN

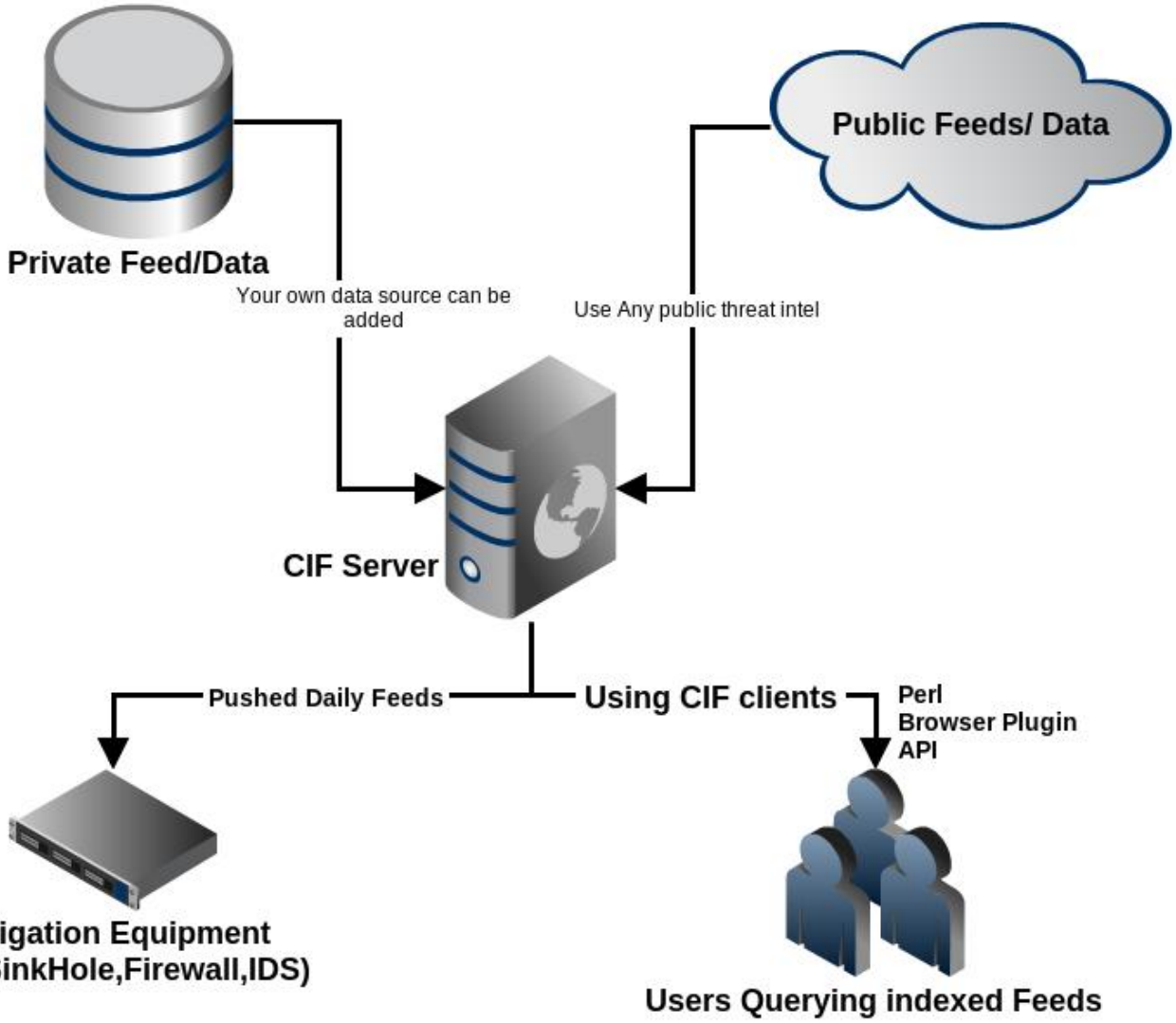
Namech_k

OnionCity

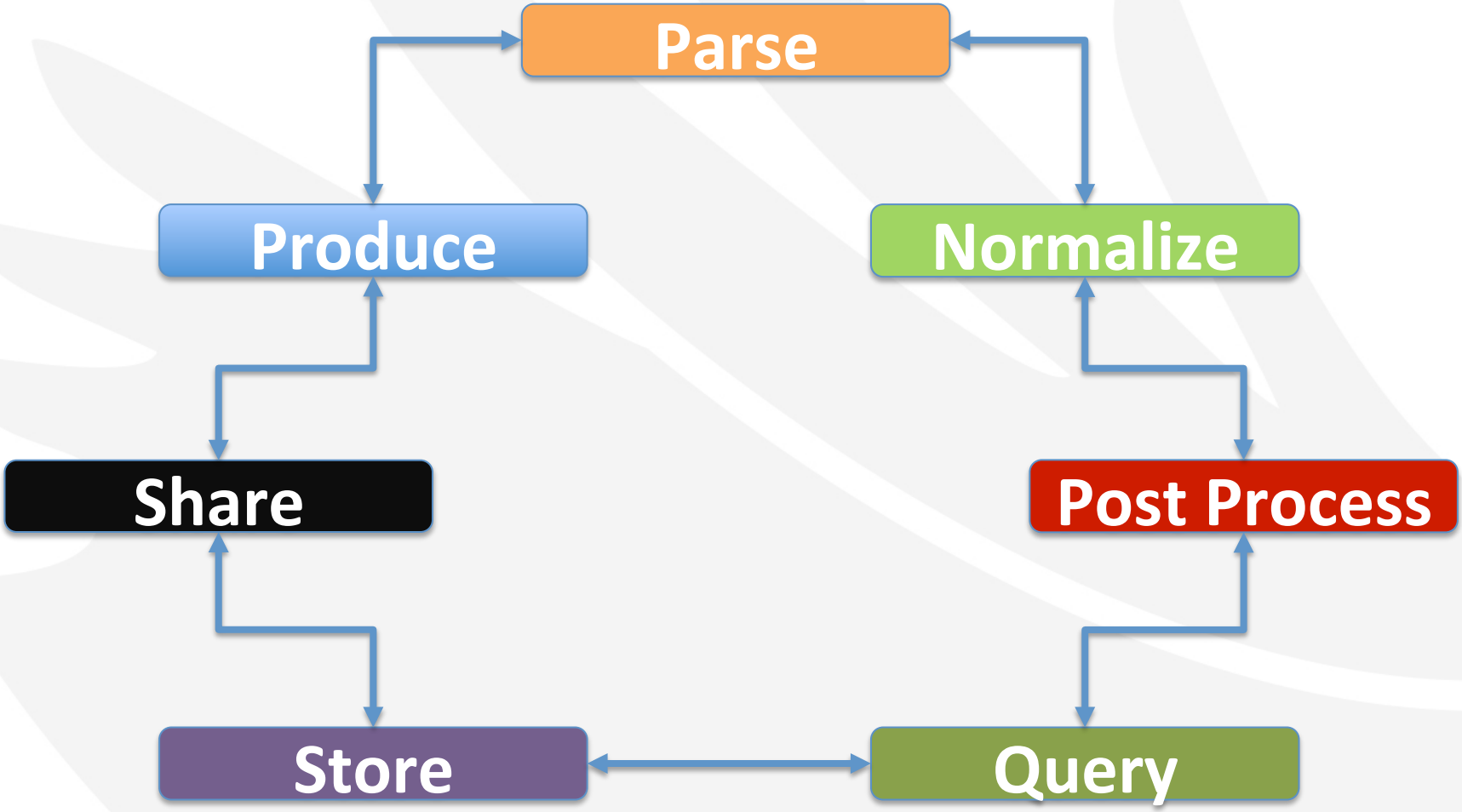
TinEye

Reverse Image Search. Learn more

CIF (collective Intelligence Framework)



CIF (collective Intelligence Framework)



OTX (Open Threat Exchange)

AlienVault Open Threat Exchange

Well known attack methods continue to successfully breach defenses. The adversary is doing something that company security teams are not doing—actively collaborating.

- FRAMEWORK FOR SHARED INTELLIGENCE THAT ENABLES A COLLABORATIVE DEFENSE, IMPROVING SECURITY
- PARTICIPATION FROM MORE THAN 50 COUNTRIES, PROVIDING COMPREHENSIVE IP REPUTATION COVERAGE
- COLLABORATIVE DEFENSE IS FREE FOR EVERYONE
- ALIENVAULT LABS RENOWNED SECURITY EXPERTS ENSURE ACCURACY

Diverse Community

AlienVault's Open Threat Exchange (OTX) enables anonymous sharing of threat intelligence. It is built into OSSIM (Open Source SIEM) and AlienVault products, sharing and receiving threat updates from installations across more than 50 countries. IP Reputation information from a broad range of devices (firewalls, proxies, web servers, anti-virus systems, and intrusion detection/prevention systems) is automatically cleansed, aggregated, validated, and published. Collaborative security intelligence is spread among many industries and countries, composed of organizations of all sizes, limiting the attacker's ability to isolate targets by industry or organization size. It is the most diverse and comprehensive IP Reputation threat feed possible.

Free for Everyone

To participate, download the latest OSSIM update, and simply click to opt-into OTX. The system will automatically begin contributing validated data and will automatically begin receiving and using threat intelligence from the community. Rest assured that no information related to the layout of your network or configuration of any controls or machines in your network will be shared. All data is stored anonymously.

Casos de Estudio OSINT

- Un estudio realizado por investigadores de la Universidad de Cambridge (Reino Unido) en colaboración con Microsoft Research Cambridge advierte que las preferencias mostradas haciendo clic en los “me gusta” son suficientes para trazar un detallado perfil del usuario.

- Investigadores de la Universidad de Pensilvania, en Estados Unidos, tomando con fuente de información las actualizaciones de estado de 75.000 personas en Facebook han conseguido predecir su edad, sexo e incluso el tipo de personalidad basándose únicamente en las palabras que usaron.

- Alessandro Acquisti y Ralph Gross, de la Universidad Carnegie Mellon, realizaron un estudio en el que usaron información de diversas fuentes de carácter público, incluyendo perfiles de redes sociales, informaron que pudieron predecir con precisión el número de afiliado de seguridad social del 8,5% de las personas nacidas en Estados Unidos entre 1989 y 2003, prácticamente cinco millones de personas.

- Las universidades de Sevilla y Alicante están desarrollando una plataforma que analiza las opiniones de la web y de los medios sociales para ayudar a las instituciones o empresas a tomar decisiones estratégicas.

@elihu_hernandez
ehernandezh@produban.com.mx