
SANS DFIR
CYBER THREAT INTELLIGENCE
EN ESPAÑOL
En vivo en línea
Cumbre Libre: 27–28 de enero
Adiestramiento: 31 de enero – 5 de febrero
sans.org/CTI-Summit

CYBER THREAT INTELLIGENCE
EN ESPAÑOL

SANS DFIR

La Evolución del Ransomware: Previsión de Escenarios Posibles para 2022

Stefano De Blasi
Cyber Threat Intelligence Analyst, Digital Shadows

¿Quien soy?

SANS DFIR

- Cyber Threat Intelligence Analyst por Digital Shadows
- Presentador del podcast ShadowTalk (ahora en Español, tambien!)
- Graduado en un Máster internacional en Intelligence, Seguridad y Estudios Estratégicos
- Recién acogido en Tenerife

¡Vamos a conectar!

@stefdeblasi

stefanodeblasii

ShadowTalk

Algunos datos personales de 2021

Ransomware en 2021

SANS DFIR

EL MUNDO

Medios: Colonial Pipeline pagó 5 millones a los hackers para rescatar su sistema

La operadora estadonidense de oleoductos sufrió un ataque informático, tras el que el suministro se recupera lentamente.

El ciberseguro impulsa el aumento repentino de los pagos del ransomware

Aina Pou Rodríguez 03/06/2021 Sin comentarios

CIBERCRIMEN

Kaseya dice que menos de 1.500 empresas fueron afectadas por un ataque de ransomware

CIBERSEGURIDAD >

Biden convoca a 30 países a una reunión para combatir los ciberataques en la que no está Rusia

Estados Unidos asegura que mantiene una vía abierta para tratar las amenazas de ciberseguridad con Moscú

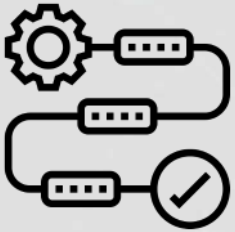
EE.UU. ofrece recompensa de US$ 10 millones por hackers de DarkSide

Washington culpa al grupo con sede en Rusia por el ataque en línea que obligó al cierre del oleoducto más grande en el este de Estados Unidos en mayo.

SANS DFIR

¿Qué Esperar De 2022?

¿Porque utilizamos las TAS?



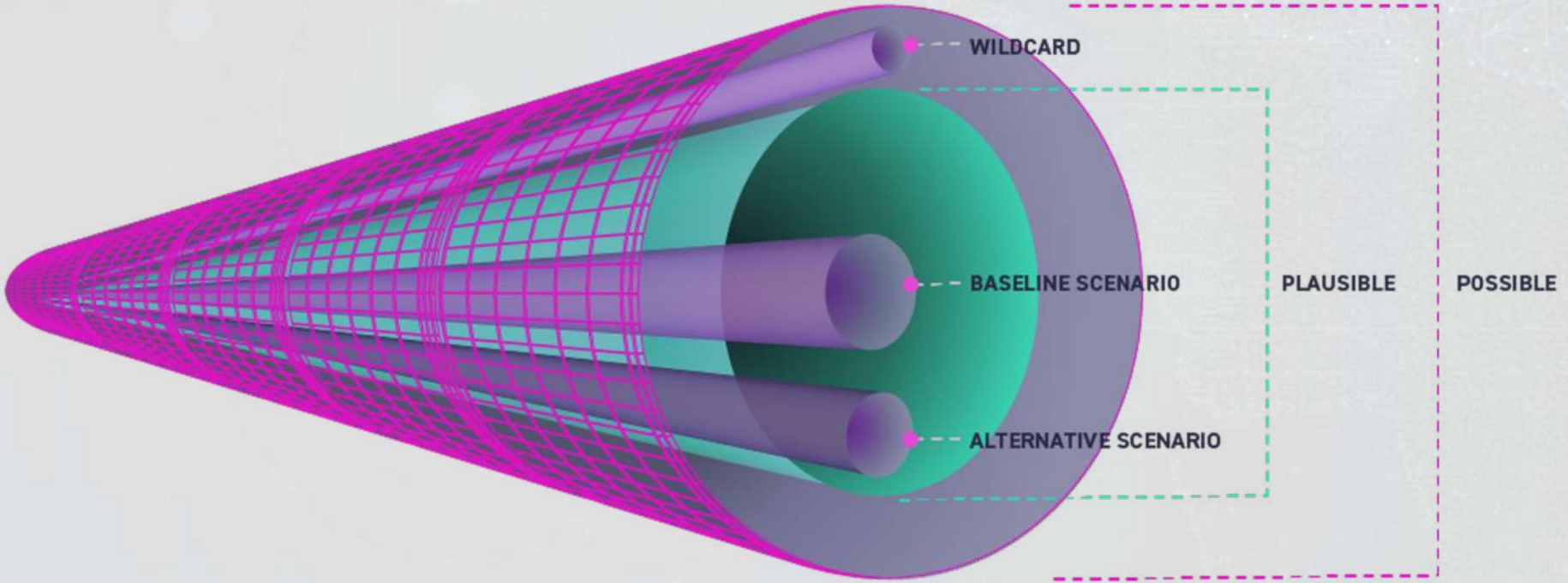
Metodología rigurosa de análisis de inteligencia

Una mayor comprensión de las limitaciones y dificultades cognitivas

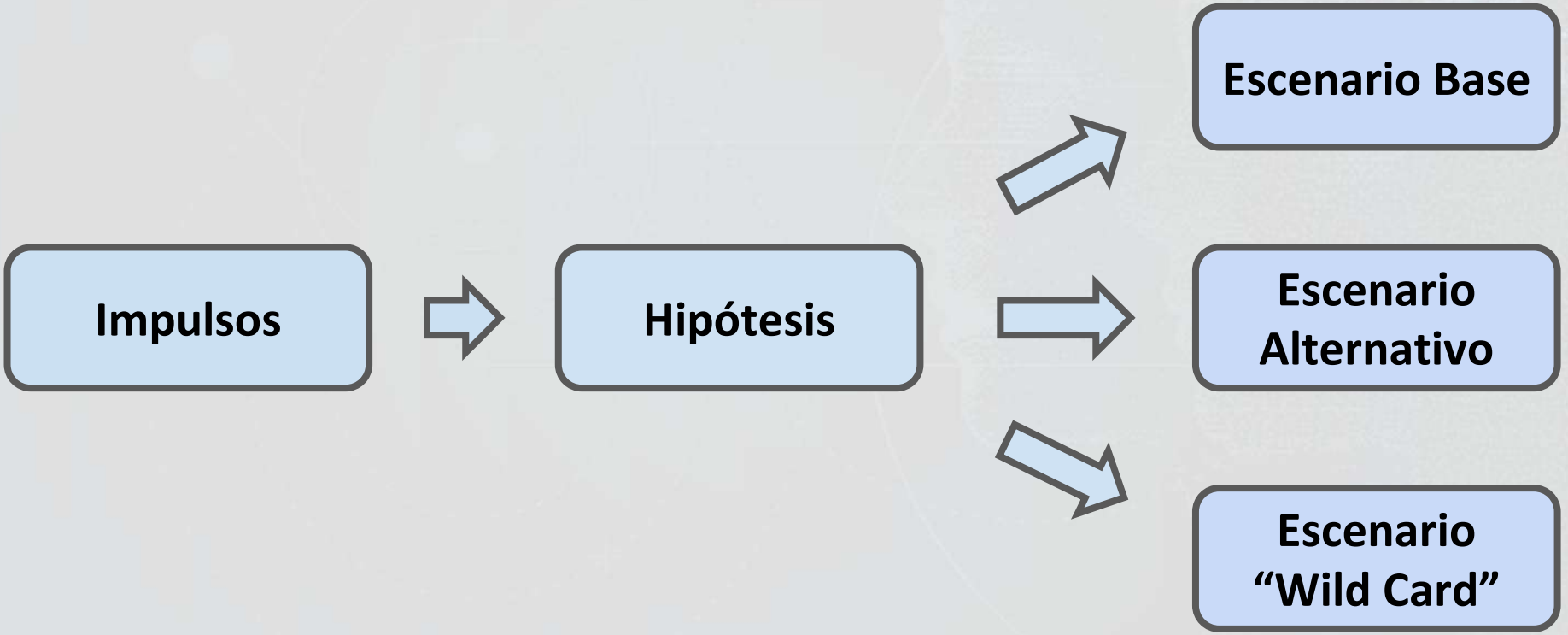
Riesgo de fracaso de la inteligencia es reducido

Para que el razonamiento de los analistas sea más transparente para los consumidores

Cono de Posibilidades



¿Como funciona?



SANS DFIR

Escenario Base

¿Y Si No Cambia Mucho?

SANS DFIR

Escenario Alternativo

¿Y Si Los Pagos de Rescates Fueran Ilegales?

SANS DFIR

Escenario “Wild Card”

¿Y Si Hay Pruebas de Cooperación con el Gobierno Ruso?

¿...Y Ahora Qué?

Cómo Montar su Propio Ejercicio TAS

SANS DFIR

¿Qué necesitas?

Un problema complejo

Un equipo de analistas brillantes y motivados

Un poquito de tiempo

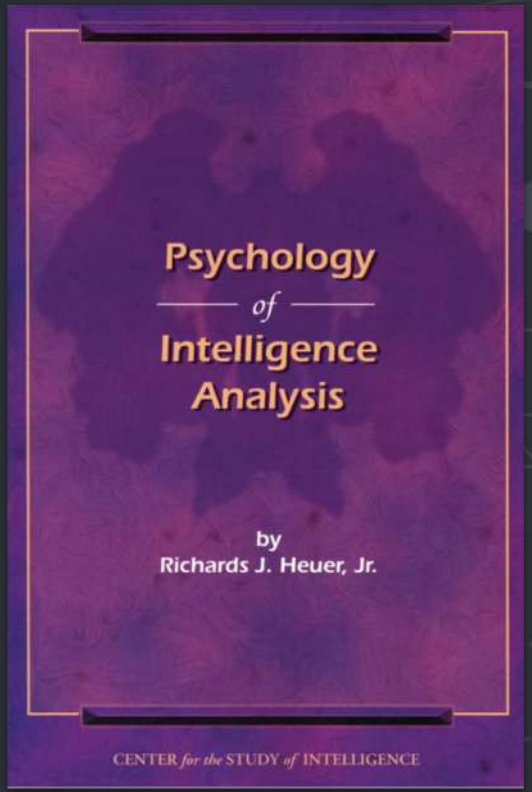
Cómo Elegir La Mejor TAS Para Su Problema

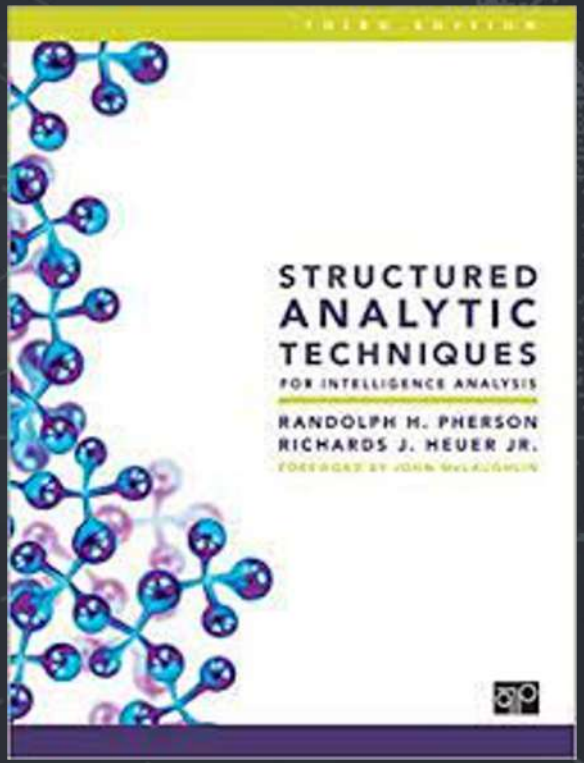
SANS DFIR

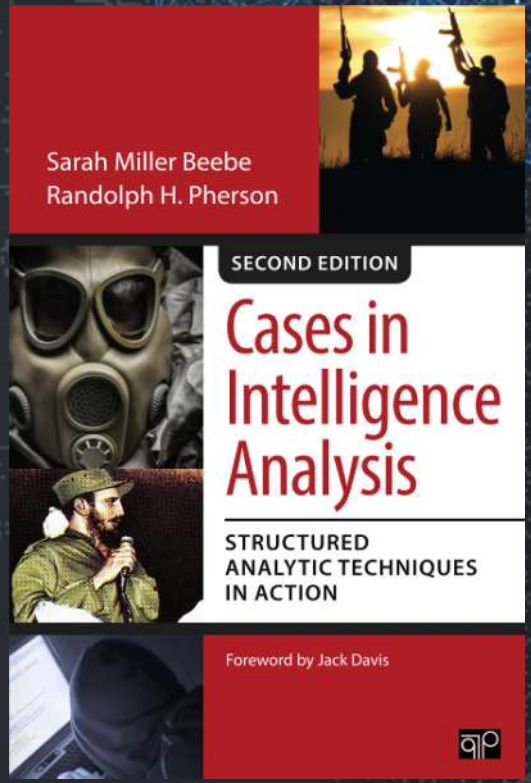
Organización	Exploración	Diagnóstica	Redefinición	Previsión	Tomar Decisiones
Concept Maps Key Assumption Check Circleboarding	Brainstorming Venn Analysis Outside-in-Thinking	Chronologies and Timelines Analysis of Competing Hypotheses Deception Detection	What if? Analysis Red Hat Analysis SWOT Analysis	Multiple Scenario Generation Key Drivers Generation	Decision Matrix Impact Matrix Force Field Analysis

CYBER THREAT INTELLIGENCE
EN ESPAÑOL

SANS DFIR







CYBER THREAT INTELLIGENCE
EN ESPAÑOL

SANS DFIR

Applied Forecasting: Using Forecasting Techniques to Anticipate Cyber Threats

n - 10:50 am ET

Add to Calendar

Gert-Jan Bruggink, Founder, Managing Director & Cyber Threat Cartographer, Venations

Técnicas CTI para la caracterización de un ataque con ransomware

2:20 pm - 2:55 pm ET

Add to Calendar

Nounou Mbeiri, Cybersecurity Engineer and CTI Researcher, GINSEG
Iván Portillo, Cyber Intelligence and Security Analyst, Big4, Co-Founder, GINSEG

Analysis of Competing Hypotheses, WCry and Lazarus (ACH part 2)

Ruegos y Preguntas

shadow talk
DIGITAL SHADOWS

Appendix

- https://isc.sans.edu/forums/diary/Analysis+of+Competing+Hypotheses+WCry+and+Lazarus+ACH+part+2/22470/
- https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf
- https://www.amazon.co.uk/Cases-Intelligence-Analysis-Structured-Techniques/dp/1608716813
- https://www.amazon.co.uk/Structured-Analytic-Techniques-Intelligence-Analysis/dp/150636893X
- https://www.cia.gov/static/955180a45afe3f5013772c313b16face/Tradecraft-Primer-apr09.pdf
- https://www.digitalshadows.com/blog-and-research/forecasting-ransomware-scenarios-in-2022/
- https://www.youtube.com/watch?v=7sGvMPvHLmk
- https://www.youtube.com/watch?v=pJGourOjVVA