

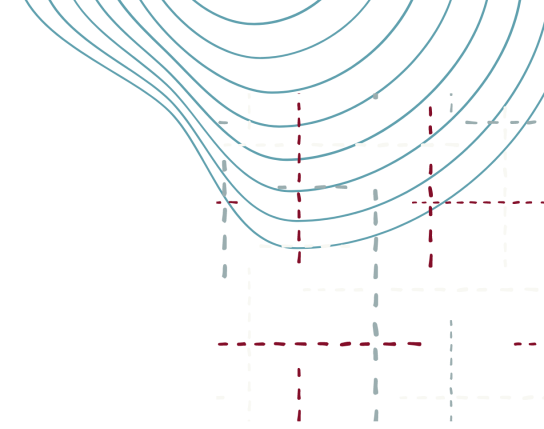
# Progetto ConTI

**Contextual threat intelligence to minimize cost and optimize remediation with **Haruspex Digital Twin****



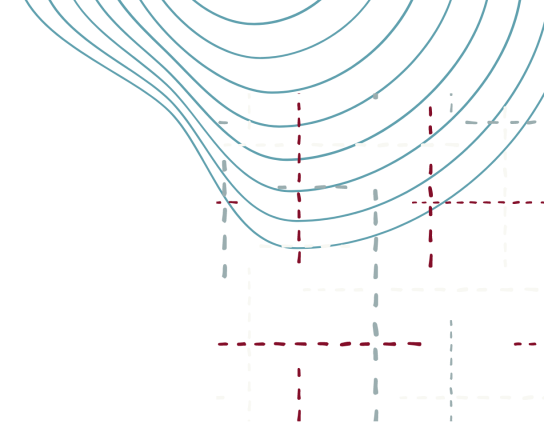
# Partecipanti

- Haruspex
- Leonardo (divisione CyberSecurity)
- Università La Sapienza, Roma
- Centro di Competenza Cyber 4.0



# Haruspex: chi siamo?

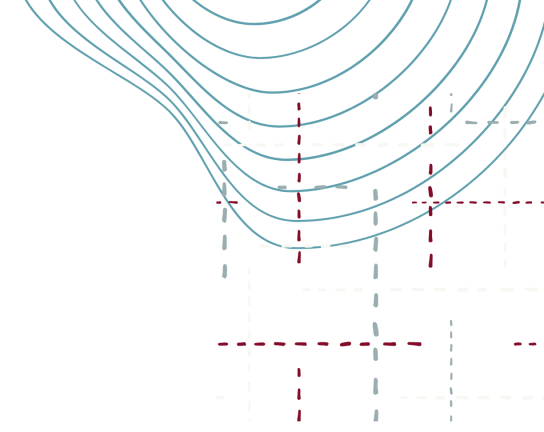
- PMI attiva nella cybersecurity
- **Cybersecurity Decision Support System - Soluzioni per prevedere e neutralizzare attacchi informatici su sistemi IT/OT critici prima che avvengano**
- Adversary Simulation tramite Cybersecurity Digital Twin di sistemi **IT/OT** e possibili attaccanti



# Cyber Threat Intelligence di Leonardo

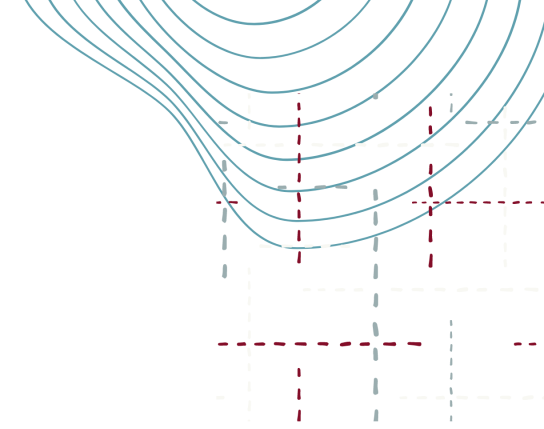
- Raccolta di informazioni su attacchi informatici e cyberminacce
- Fonti molteplici
- Organizzazione delle informazioni
- Supporto ai processi decisionali per difesa infrastrutture critiche

La divisione Cybersecurity di **Leonardo** ha realizzato un database di **CTI**



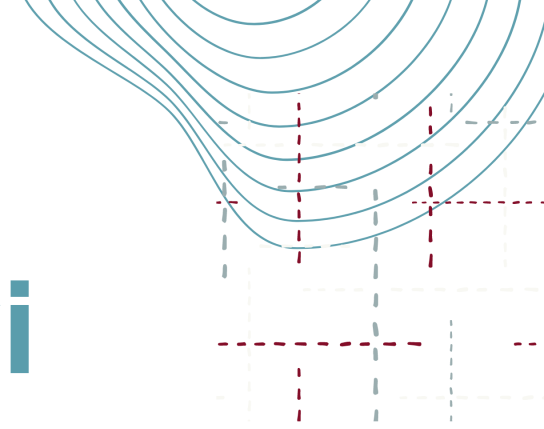
# Progetto ConTI

- **Import automatico** di informazioni di **Threat Intelligence Leonardo** nei **twin Haruspex**
- **Modellazione** di attaccanti di Threat Intelligence su twin Haruspex
- Ogni twin Haruspex avrà a disposizione un insieme di **TTPs da sfruttare** nella simulazione
- **Test** degli attaccanti su twin di reti IT/OT



# Progetto ConTI: obiettivi

**Calcolo automatico**, tramite i **twin** Haruspex, un insieme ottimizzato di contromisure per **mitigare il rischio** generato da attaccanti di **Threat Intelligence** su specifiche infrastrutture **IT/OT**



# Timeline del progetto (1)

Mesi: 0-2

- Definizione delle informazioni utili nel database CTI di Leonardo: attaccanti, malware, TTP

Mesi: 2-3

- Implementazione di un protocollo di comunicazione tra il database Leonardo e la Suite Haruspex tramite API

# Timeline del progetto (2)

Mesi: 3-4

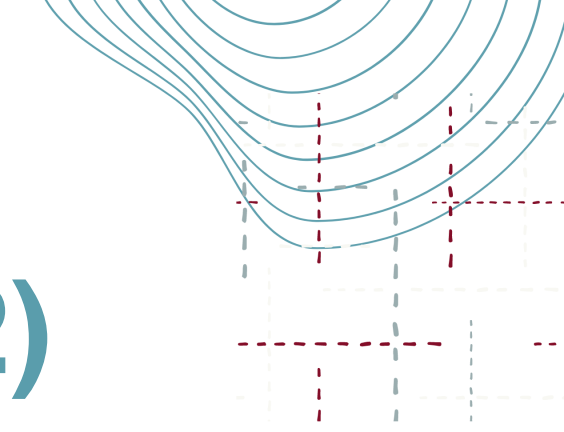
- Creazione di profili di attaccanti da quelli nel database CTI, utilizzabili su ogni Twin Haruspex di reti IT/OT

Mesi: 4-5

- Modellazione del comportamento delle TTPs: dal linguaggio descrittivo ad istruzioni software

Mesi: 5-6

- Modellazione dei comportamenti dei Twin di attaccanti in base alle TTPs che possono sfruttare e alle info in loro possesso





# Timeline del progetto (3)

Mesi: 6-14

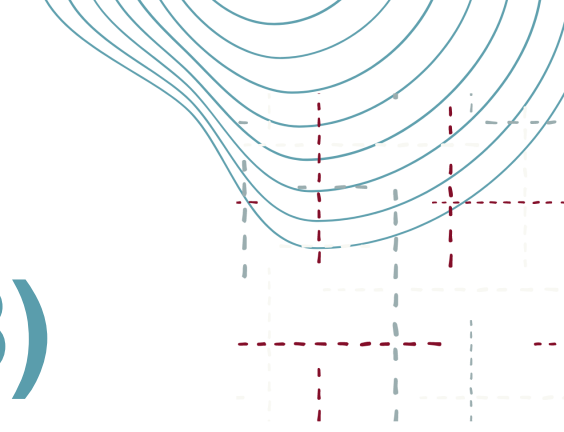
- Implementazione di un simulatore Montecarlo che esegue Twin di attaccanti sui Twin di reti IT/OT

Mesi: 14-15

- Definizione ed implementazione di un report adeguato ai nuovi risultati ottenuti

Mesi: 15-18

- Validazione dei risultati



# Progetto ConTI

Grazie!

[www.haruspex.it](http://www.haruspex.it)

info@haruspex.it