CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

In collaborazione con

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

"La Strategia Nazionale di Cybersecurity: impatto e prospettive"
Ciclo di webinar a cura del Centro di Competenza Cyber 4.0

INFORMATION SHARING PUBBLICO-PRIVATO

Mercoledì 20 Luglio 2022 ore 16.00

Per info:
comunicazione@cyber40.it
www.cyber40.it

Strategia Nazionale /1
CSIRT Italia

L'ACN, con al suo interno lo CSIRT Italia, il PoC NIS e il NCS, ricopre due dei tre livelli funzionali dell'architettura nazionale per la gestione degli incidenti e delle crisi di cybersicurezza che si incardina perfettamente nella piattaforma definita dalla Raccomandazione UE 2017/1584 (c.d. Blueprint).

Lo CSIRT Italia, che realizza il livello tecnico nella gestione degli incidenti e delle crisi di cybersicurezza, è un tassello centrale della Strategia.

Il monitoraggio e il contrasto delle minacce cyber operato dai CERT sul territorio nazionale ha ora uno snodo incardinato nell'impianto più ampio e organico della cybersicurezza nazionale con l'ACN a coordinare grazie ad un quadro normativo rinnovato e rafforzato.

Strategia Nazionale /2
NCC e ISACS

L'ACN è fondamentale anche perché svolge organicamente molteplici compiti: punto di contatto unico (PoC) per le finalità NIS, elemento centrale del Perimetro di sicurezza nazionale cibernetica (PSNC), Centro Nazionale di Coordinamento (NCC) rispetto al Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC).

Ulteriore impulso al miglioramento delle capacità di cybersicurezza è stato dato orientando i servizi cyber nazionali verso una distinzione tra:

- **SOC**, coordinati da Hyper SOC;
- **CERT**, coordinate dallo CSIRT Italia;
- **ISAC**, coordinate dall'ISAC Centrale interno all'ACN;

In maniera da rendere più adattiva e flessibile l'intera architettura.

Information Sharing - L'esperienza Sogei – *How it started…*

Il CERT Sogei è stato creato nel 2015, applicando standard e best practice di riferimento. L'information sharing era praticata anche se non ancora strutturata e matura quanto oggi, soprattutto in merito a strumenti, paradigmi e standard.

Nel maggio 2017, in occasione dalla campagna Wannacry/WanaCrypt0r tra alcune importanti realtà istituzionali, governative e private si creò sinergia e collaborazione per scambiare informazioni e IoC.

Ne scaturirono alcune iniziative spontanee che portarono a interessanti risultati, tutti all'interno del comparto della cyber security italiana. A dimostrazione dell'interesse per il tema e la centralità che gli veniva riconosciuta per la lotta e il contrasto alle minacce cyber.

2017

2019

IoC Data Model

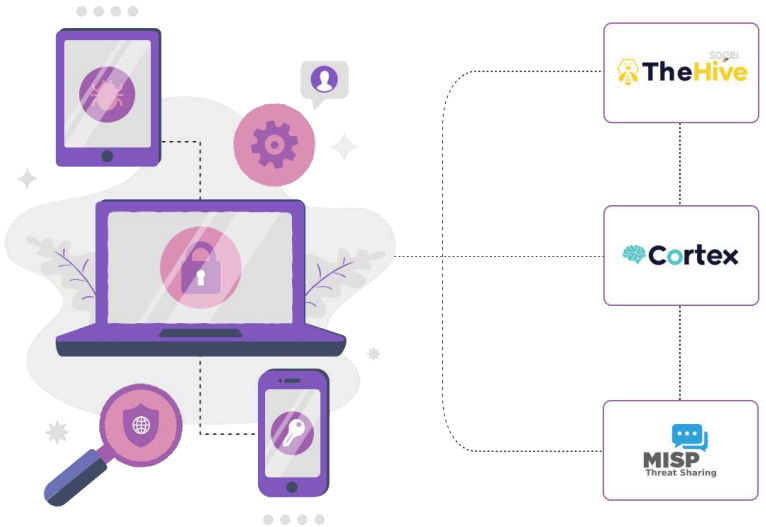
2018

Architettura tecnologica

Information Sharing
L'esperienza Sogei – …*How it goes*

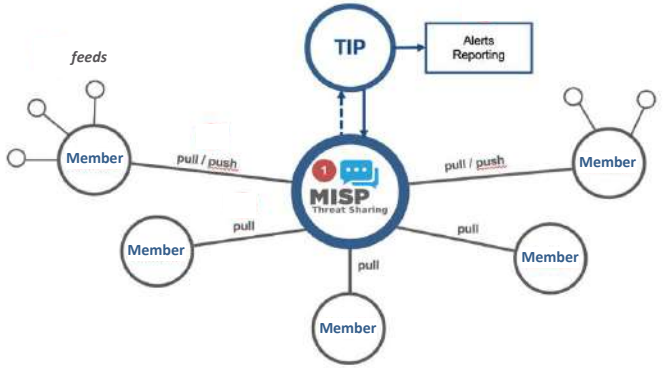
Il CERT Sogei attua l'information sharing, oltre che con le entità che fanno parte della propria *contituency,* con istituzioni e organizzazioni quali fonti autoritative e interlocutori di riferimento, mediante specifici accordi e convenzioni.

Vi sono poi ulteriori entità coinvolte, dall'elevata autorevolezza e affidabilità, nell'information sharing mono e bidirezionale (push/pull) al fine di completare e arricchire ulteriormente gli indicatori e le informazioni in proprio possesso.



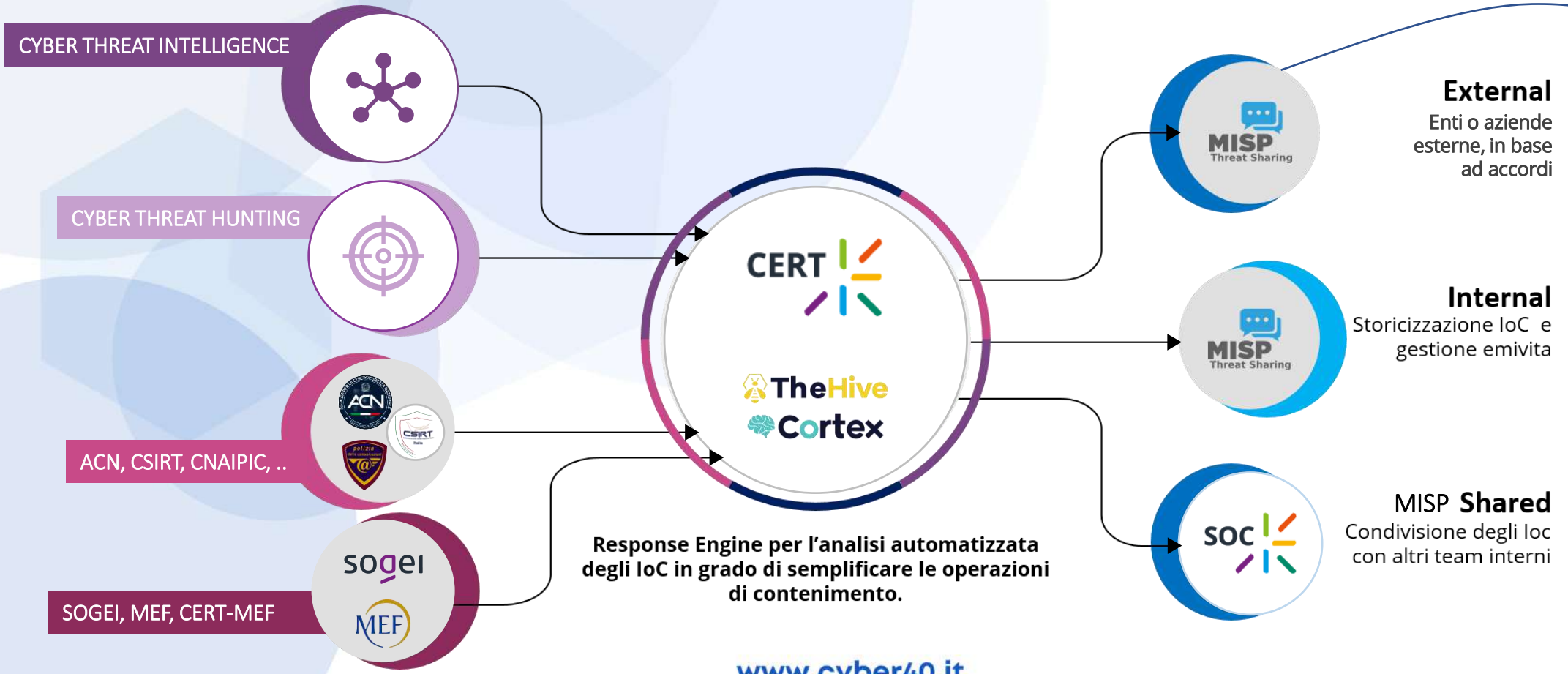
Gli strumenti comprendono MISP, TheHive, Cortex.
Tre strumenti open source e di libero utilizzo assurti a standard *de facto* per la gestione delle minacce e degli attacchi cyber. Hanno robuste community di utenti e sviluppatori; MISP è cofinanziato dall'UE.

Il MISP è utilizzato in una costellazione di istanze collegate o federate, per condividere e gestire gli IoC in maniera coerente con i flussi operativi.



Information Sharing
L'esperienza Sogei – …*How it goes*

Flusso di gestione delle minacce cyber. L'information sharing bidirezionale è parte integrante del flusso.



www.cyber40.it

Information Sharing
Sogei, CSIRT Italia, ACN

Nell'ambito della gestione degli incidenti e delle crisi di cybersicurezza, sono attive una interlocuzione e una collaborazione costanti tra Sogei, con il proprio CERT, e lo CSIRT e l'Agenzia.

Nel rinnovato quadro normativo e organizzativo in materia di cybersicurezza, Sogei si è resa disponibile ad avviare con ACN e lo CSIRT Italia una comunicazione e condivisione che realizzino più compiutamente quanto definito dalla Strategia Nazionale in tema di rete di CERT.

L'integrazione degli attuali servizi cyber nazionali

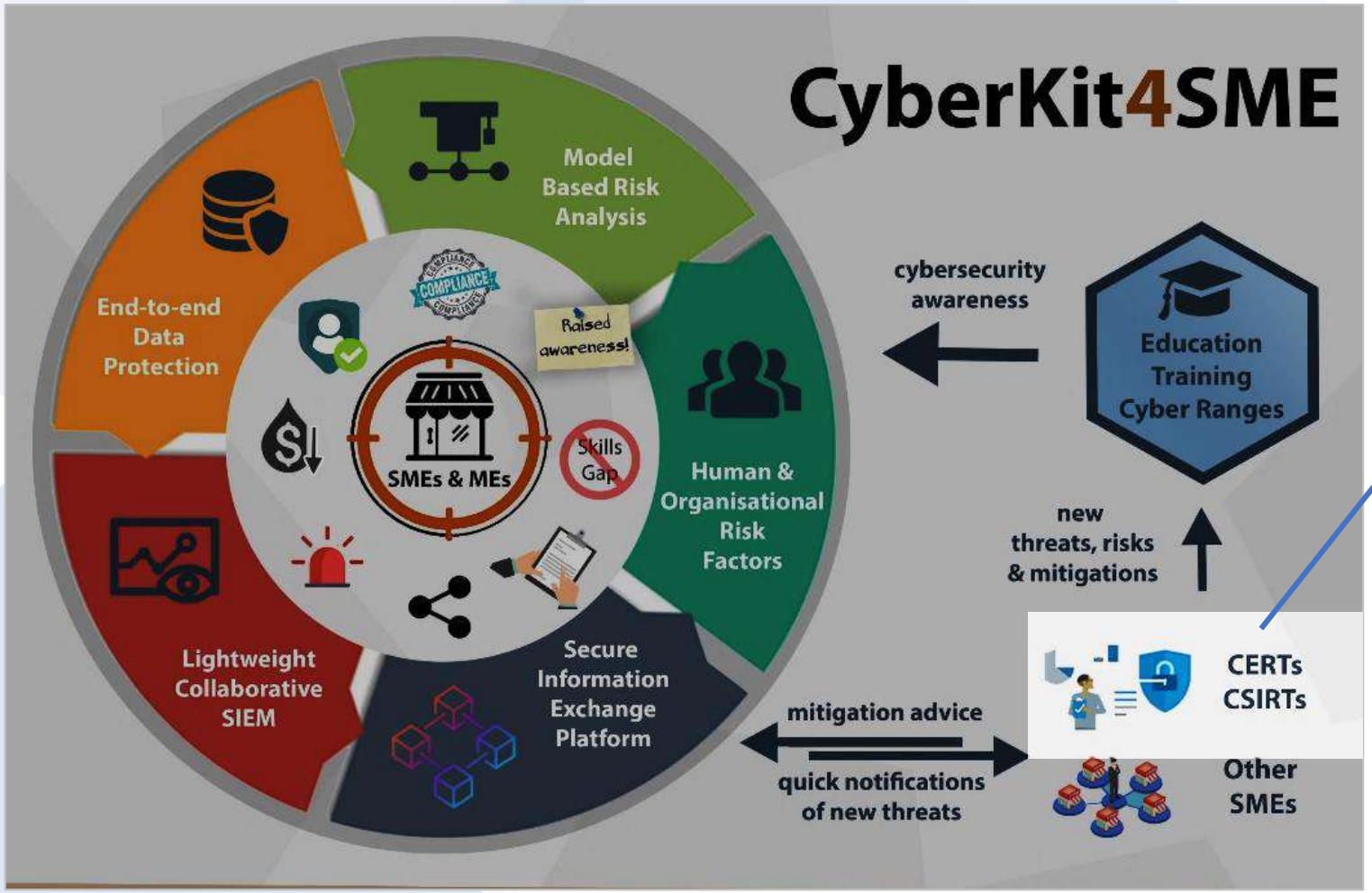
L'information sharing è una delle tematiche considerate in questi scenari.

Il Progetto CyberKit4SME
Caratteristiche e obiettivi

Sogei partecipa al progetto CyberKit4SME, finanziato nell'ambito del programma Horizon 2020, che mira a democratizzare la cyber security, predisponendo un pacchetto di strumenti a protezione delle PMI e micro-imprese contro le minacce cyber, aumentando la cultura sulla sicurezza informatica e la protezione delle informazioni:

- Un tool per l'**Analisi del Rischio** basato sulla ISO 27005 per rilevare fattori di rischio tecnici, organizzativi e umani;
- Un tool per **rappresentare i rischi** umani e organizzativi;
- una **SIEM** (Security Information and Event Management) per la raccolta e la correlazione degli eventi di sicurezza;
- una **piattaforma di condivisione** delle informazioni tra PMI/MI ed CERT/CSIRT;
- un servizio di "**End-to-End Data Protection**" al fine di mantenere l'integrità e la confidenzialità dei dati;

Progetto CyberKit4SME
Ruolo di Sogei



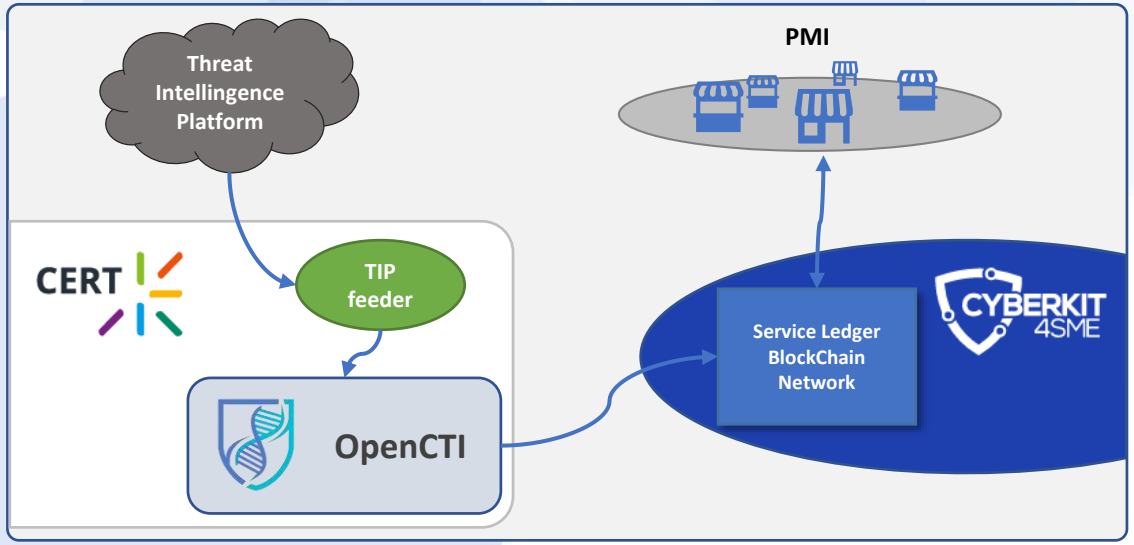
Sogei svolge un ruolo funzionale nella soluzione tecnologica e come responsabile della conduzione di specifiche attività e Work Package.

Nell'ambito della soluzione tecnologica obiettivo del progetto, Sogei con il proprio CERT svolge il ruolo di fonte di informazioni di cyber security che vengono condivise con le PMI e le micro-imprese mediante i tool appositamente sviluppati.

Tale ruolo è previsto venga svolto con strumenti e soluzioni proprie del CERT.

Progetto CyberKit4SME
Architettura proposta

Nell'ambito del progetto è stata messa a punto la modalità di interazione tra CERT Sogei e toolkit CyberKit4SME, cioè l'insieme dei tool previsti dal progetto. In particolare il CERT Sogei alimenta il Service Ledger, sviluppato dall'Università di Southampton.



L'interazione, realizzata con il tool open source OpenCTI e standard consolidati quali STIX/TAXII, permette tramite un connettore custom la condivisione di IoCs e report di cybersecurity secondo uno specifico criterio di selezione.

Information Sharing
Opportunità, sviluppo, collaborazione

La Strategia definisce una nuova architettura di gestione degli incidenti e delle crisi di cybersicurezza più articolata e razionale: declinata su più livelli e in più contesti, garantirà una migliore azione di controllo e contrasto delle minacce cyber.

Nell'impegno Sogei per attuare una efficace ed efficiente information sharing, nell'ambito delle attività del proprio CERT, si inquadra l'obiettivo di dare piena espressione alla Strategia Nazionale in tema di "rete di CERT".

Nel progetto CyberKit4SME, Sogei ha ideato e sperimentato una forma di information sharing diversa dalle modalità istituzionali e consolidate. Una sperimentazione orientata a fornire dati e informazioni a beneficio della cybersicurezza delle PMI.

Potremmo ravvisare quindi spunti per l'eventuale sviluppo di iniziative che possano contribuire alla cybersicurezza così come delineata dalla Strategia: un ISAC per PMI, una fonte IoC per alimentare un ISAC, attività congiunte pubblico-privato orientate alle PMI e micro-imprese, solo per fare qualche esempio.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Grazie

Andrea Pugini
Security Governance e Data Protection