CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

INNOVATION ROADMAP

Webinar tematici: INTELLIGENZA ARTIFICIALE

CYBERSECURITY PER L' AI E LA FABBRICA CONNESSA

L'importanza della I.A. e di avere un S.O.C. per le Aziende soggette alla direttiva NIS 2

Lorenzo Celussi – CISO (Tinet srl)

16 Giugno 2026

Lorenzo Celussi

CISO
Cyber Security Project Manager
Responsabile ISO 27001- 27017 - 9001

INTRODUZIONE

La NIS 2: Oltre la Compliance

La Direttiva NIS 2 nasce dall'esigenza di aumentare il livello di sicurezza e resilienza delle organizzazioni che operano in settori critici o strategici. Ma **la compliance, da sola, non basta**: serve capacità operativa, visibilità e tempestività.

Non si tratta solo di installare tecnologie di sicurezza, ma di costruire un'organizzazione capace di **identificare i rischi, monitorare gli eventi, rispondere agli incidenti** e documentare le decisioni prese. Serve un modello in grado di trasformare un allarme in una decisione aziendale corretta.

IL PRESIDIO OPERATIVO

Come Opera un S.O.C.

Un S.O.C. ben strutturato raccoglie segnali da firewall, endpoint, server e cloud, individua comportamenti anomali, correla eventi apparentemente scollegati e determina se un'anomalia rappresenta un rischio reale.

Sorveglianza Continua

Monitoraggio H24 di tutti gli asset di rete e rilevamento tempestivo di eventi anomali.

Correlazione degli Eventi

Analisi e correlazione di segnali apparentemente scollegati per identificare minacce reali.

Gestione Strutturata

Processo coerente di rilevamento, qualificazione, gestione e notifica degli incidenti.

Per i soggetti NIS 2, il S.O.C. è essenziale: l'organizzazione deve dimostrare non solo di aver subito un incidente, ma di averlo **rilevato, qualificato, gestito e notificato** secondo un processo coerente.

S.O.C. e Referente CSIRT: Componenti Complementari

Il S.O.C.

È il presidio che **vede l'incidente nascere**: rileva gli alert, analizza i log, identifica gli indicatori tecnici e fornisce il quadro operativo completo.

Fornisce una vista operativa continua sul rischio cyber, consentendo all'azienda di passare dalla teoria della compliance alla pratica della reale sicurezza.

Il Referente CSIRT

Ha il compito di **coordinare la risposta**: coinvolgere le funzioni aziendali, supportare le decisioni, gestire la comunicazione interna ed eventualmente supportare il processo di notifica verso le autorità competenti.

S.O.C. e Referente CSIRT non sono strutture alternative:
sono componenti complementari dello stesso modello di difesa.

L'ACCELLERATORE COGNITIVO

Il Ruolo dell'Intelligenza Artificiale

Nei primi momenti dopo un incidente, il problema principale è l'incertezza: molti segnali, informazioni incomplete, poco tempo per decidere. L'I.A. può aiutare proprio in questa fase critica.

Analisi Massiva

Analizza grandi volumi di log e individua indicatori anomali in pochi secondi.

Correlazione Avanzata

Correla eventi distanti, suggerisce scenari di attacco e propone azioni coerenti.

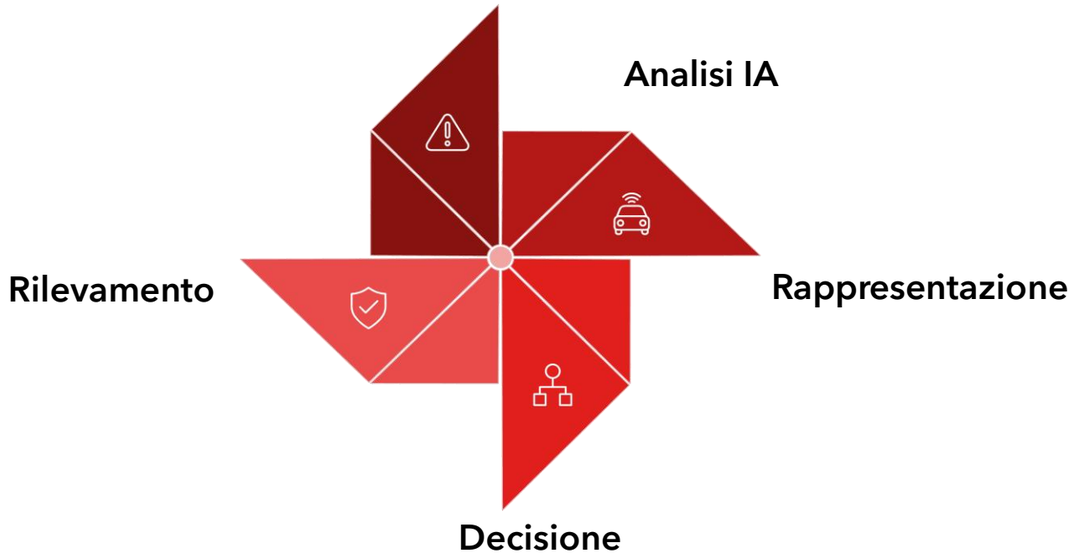
Acceleratore Operativo

Non sostituisce il giudizio umano: potenzia il S.O.C. e supporta il Referente CSIRT, accelerando le decisioni.

I PRIMI 60 MINUTI

Dall'Incidente alla Decisione Corretta

Nei primi 60 minuti, l'obiettivo non è sapere tutto. **L'obiettivo è sapere abbastanza per prendere decisioni corrette.**



L'**I.A**. consente di passare rapidamente da una situazione caotica a una rappresentazione ordinate dell'incidente, permettendo al **S.O.C. e al Referente CSIRT** di concentrarsi sulle decisioni ad alto valore: contenere l'attacco, proteggere i servizi critici e attivare le escalation corrette.

IL PARTNER STRATEGICO

L'Importanza del Service Provider

Molte aziende soggette a NIS 2 non dispongono internamente di tutte le competenze, risorse e tecnologie necessarie per gestire un presidio cyber continuativo. Un service provider qualificato consente di colmare questo gap.

Capacità Operativa Completa

Persone competenti, processi maturi, tecnologie adeguate e procedure di escalation strutturate.

Doppio Linguaggio

Capace di parlare sia il linguaggio tecnico del S.O.C. sia il linguaggio manageriale della governance.

Garanzie Misurabili

Tempi di risposta chiari, tracciabilità delle attività, report comprensibili e supporto nelle fasi critiche.

IL MODELLO INTEGRATO

Quattro Pilastri della Cyber Resilienza

S.O.C.

Il presidio che consente di **vedere ciò che accade** in tempo reale.

Referente CSIRT

Il referente che **coordina la risposta** e gestisce la comunicazione.

Intelligenza Artificiale

L'acceleratore che aiuta a **comprendere e agire** più rapidamente.

Service Provider

Il partner che rende tutto questo **sostenibile, scalabile e misurabile**.

CONCLUSIONE

Il Tempo è il Fattore Decisivo

> Chi rileva prima, capisce prima. Chi capisce prima, contiene meglio. Chi contiene meglio, protegge business, reputazione e continuità operativa.

La NIS 2 rappresenta una grande opportunità: non solo adeguarsi a un obbligo normativo, ma **rafforzare la propria capacità di resistere, reagire e recuperare** da un incidente cyber. Nella cybersecurity moderna, il tempo è il fattore decisivo.

Per informazioni:
ricercainnovazione@confindustriavenest.it

Grazie per l’attenzione.