

Forum ICT Security 2025 – Due giornate di evento per ridefinire il futuro della sicurezza digitale in Italia



Il Forum ICT Security 2025 riunisce il 19 e 20 novembre a Roma i principali protagonisti della cybersecurity italiana ed europea per affrontare le sfide più urgenti della trasformazione digitale: dall'intelligenza artificiale alla crittografia quantistica, dalla compliance NIS2 alla resilienza operativa.

PRIMA GIORNATA – 19 NOVEMBRE 2025

Innovazione, AI Security e Tecnologie Emergenti

La giornata si aprirà con la tavola rotonda istituzionale **“Cybersecurity, Innovazione, Governance e Scenari Futuri”**, moderata da **Matteo Lucchetti** (Cyber 4.0), che vedrà confrontarsi i vertici delle istituzioni italiane ed europee: **Luca Tagliaretti** (European Cybersecurity Competence Center), **Alessio Butti*** (Sottosegretario con delega all'Innovazione tecnologica), **Luca Nicoletti** (ACN), **Mario Nobile** (AgID), insieme ai leader dell'industria come **Cristiano Alborè** (Telsy).

AI Security: explainability, edge computing e governance dei dati tra innovazione e rischi

La sessione dedicata all'intelligenza artificiale e sicurezza rappresenta il cuore tecnologico della giornata. **Luca Viganò** (King's College London) introdurrà l'Explainable Security, paradigma emergente che pone sfide superiori alla stessa

Explainable AI. **Simone Scardapane** (Sapienza) svelerà i meccanismi interni dei modelli AI attraverso la mechanistic interpretability, mentre **Dario Sabella** (NEXT G CLOUD, Chairman ETSI MEC) affronterà le sfide del continuum edge-to-cloud nell'era dell'IA, presentando standard ETSI, GSMA e 3GPP per la protezione di applicazioni critiche. **Andrea Virgilio** (Beliven) chiuderà la sessione AI con un focus pragmatico su rischi GDPR e protezione dei dati, smontando la narrazione eccessivamente ottimistica delle AI generative.

Strategie, minacce e difesa operativa

La sessione “Difesa operativa e resilienza” porterà una prospettiva concreta. **Manlio Longinotti** (SANS Institute) presenterà i risultati del 2025 Cybersecurity Workforce Survey su 3.400 manager, dimostrando che il vero gap non è di numeri ma di competenze. **Luca Salvatori** (HiSolution) analizzerà l'evoluzione delle minacce attraverso un caso reale di furto di token, mentre **Pierpaolo Alì** (OpenText) e **Jean-Pierre Carlin** (Corelight) mostreranno come AI e Network Detection and Response stanno trasformando i SOC da centri reattivi a piattaforme predittive.

Crittografia e Quantum: prepararsi al futuro

Il pomeriggio sarà dedicato alla rivoluzione quantistica. **Marco Baldi** (Università Politecnica delle Marche) illustrerà la transizione alla crittografia post-quantum, **Daniele Venturi** (Sapienza, Direttore Lab SCRYPT0) esplorerà gli standard NIST e le applicazioni futuristiche come le monete quantistiche, mentre **Fabio Antonio Bovino** (Sapienza) racconterà 25 anni di storia quantistica italiana dal laboratorio al mercato, con il Q-KeyMaker® come esempio di eccellenza europea nella competizione con USA e Cina.

SECONDA GIORNATA – 20 NOVEMBRE 2025

NIS2, Supply Chain e Resilienza Operativa

La seconda giornata si concentrerà sulla messa a terra della compliance e sulla difesa concreta. Si aprirà con la tavola rotonda **“NIS2 & Beyond”**, moderata da **Laura Liguori** (Portolano Cavallo), che riunirà **Daniela Mazzarone** (NTT DATA), **Nicolò Rivetti di Val Cervo** (ACN – Capo Divisione NIS), **Elsa Catalano** (Engineering – DP0) e **Ilaria Curti** (Portolano Cavallo) per esplorare governance, supply chain risk management e convergenza CISO-DP0 nell’era del Cyber Resilience Act.

Supply Chain sotto attacco: vulnerabilità, impianti hardware e strategie di resilienza

Fabrizio Baiardi (Università di Pisa) approfondirà NIS2 e Software Bill of Materials (SBOM), spiegando come la resilienza sia proprietà dell’ecosistema informativo, non dei singoli sistemi. **Luca Bongiorno** (ZTE Italia) porterà la discussione nel mondo reale con USBsamurai: un cavo USB da meno di 15€ capace di compromettere sistemi air-gapped da remoto, dimostrando come gli impianti hardware siano minacce concrete da Stuxnet a oggi. **Roberta Pellegrino** (Politecnico di Bari) concluderà con una ricerca empirica su come l’Economia Circolare diventi driver di resilienza per le imprese italiane.

Resilienza operativa: IT/OT, cyber operations e convergenza fisica-digitale

Nicola Mugnato (Gyala) presenterà architetture di difesa distribuita per ambienti IT/OT critici, isolati e legacy, con automazione della detection conforme a IEC 62443. **Francesco Arruzzoli** (Cerbeyra) introdurrà le cyber operations in ambito civile: approccio intelligence-driven ispirato al modello militare, con playbook codificati e procedure scalabili che superano i tradizionali SOC. **Marco Bavazzano** (Axitea) affronterà la Security Convergence per le PMI, dove metà delle imprese italiane è in filiere strategiche e la sicurezza

fisica-digitale diventa vantaggio competitivo. **Emiliano Massa** (Proofpoint) e **Massimiliano Graziani** con **Claudio Tosi** (Cybera/Threatdown) chiuderanno con soluzioni Human Centric e tecnologie anti-ransomware basate su AI e ransomware rollback.

Intelligent Detection & Response: l'AI al servizio della difesa

La sessione finale vedrà **Marco Mellia** (Politecnico di Torino) esplorare potenzialità e limiti di LLM e agenti AI autonomi per cybersecurity e digital forensics. **Giorgio Giacinto** (Università di Cagliari) analizzerà come il Machine Learning possa individuare componenti malevoli senza ampliare la superficie di attacco, mentre **Mirco Marchetti** (Università di Modena e Reggio Emilia) concluderà con l'intelligent detection per veicoli connessi, reti V2X e ecosistemi IoT automotive.

Forum ICT Security 2025: le priorità strategiche per la cybersecurity italiana

La 23a edizione del Forum ICT Security che si terrà a Roma il 19 e 20 novembre 2025 rappresenterà un momento di sintesi strategica per comprendere dove si colloca l'Italia nel panorama globale della sicurezza informatica.

Tre direttrici strategiche guideranno le due giornate:

Le sessioni sull'**intelligenza artificiale** affronteranno il nodo critico dell'explainability nei sistemi di sicurezza. Quando i modelli AI prendono decisioni in tempo reale su minacce critiche, la loro opacità diventa rischio operativo. Il confronto tra ricerca accademica e implementazioni industriali metterà in luce il gap tra potenziale tecnologico e applicabilità concreta in contesti regolamentati.

La **minaccia quantistica** uscirà dalla dimensione teorica: il

Summit offrirà una valutazione realistica delle tempistiche di transizione crittografica e delle priorità per infrastrutture critiche. L'Italia potrà posizionarsi nella competizione europea per standard e tecnologie quantum-safe, valorizzando le proprie competenze di ricerca.

Il dibattito su **NIS2** supererà la retorica della compliance per entrare nel merito operativo: come proteggere concretamente supply chain complesse, sistemi OT legacy, PMI con risorse limitate. Gli interventi accademici su SBOM ed ecosistemi informativi dialogheranno con casi d'uso reali di attacco e difesa, dalle dimostrazioni hardware alle architetture di difesa distribuita.

L'elemento trasversale sarà la consapevolezza che la sicurezza non si acquista con singole tecnologie ma si costruisce attraverso competenze, governance integrata e visione sistemica. Il confronto tra istituzioni, università e industria permetterà di identificare priorità condivise e roadmap concrete.

Il Forum ICT Security 2025 ambisce a offrire non solo aggiornamento tecnologico, ma strumenti per ripensare l'approccio alla cybersecurity in un contesto di complessità crescente e minacce in rapida evoluzione.

La partecipazione all'evento è gratuita previa iscrizione online: <https://www.ictsecuritymagazine.com/eventi/register>

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/forum-ict-security-2025-evento-sicurezza-digitale-in-italia/>