

29 OTTOBRE 2025

CYBER SECURITY DAY

**LA SICUREZZA ONLINE INIZIA DA UN CLIC
CONSAPEVOLE!**

ated 

PROGRAMMA POMERIDIANO 29 OTTOBRE 2025

Ore 13.30 Check in

Ore 14.00 Inizio evento Luca Mauriello e Cristina Boggia Giotto

Ore 14.15 GdL Cyber , Luca Mauriello e Alan Vananti

Ore 14.20 Sessione 1; 1° Workshop Rocco Sicilia, PATIO

Ore 14.50 Pillole Cyber: AIL

Ore 14.52 Inizio ATED CYBER CHALLENGE LIVE – TRUST THE SIGNAL!, suddivisione in gruppi

Ore 14.55 Sessione 2, Sale

- Paolo Pezzoni SOC/ROC (Security/Risk Operation Center)
- Andrea Cappai e Alessio Loche: Lab Forense
- Andrea Pasin: Hacking Networks 101: La Falsa Sicurezza della Client Isolation
- Lorenzo Ladina: Attack Paths in Active Directory con BloodHound
- Gianni Ricca e Emanuele Bianchi: Microsegmentazione intelligente
- Martino Pozza: Cyber Challenge: Sopravvivi all'attacco!

Ore 15.30 Pillole Cyber: .Cleafy

Ore 15.32 Sessione 3 ; Massimo Bertaccini: CSE – Crypto Search Engine

Ore 16.00 PAUSA

Ore 16.20 Sessione 4, Sale

- Paolo Pezzoni SOC/ROC (Security/Risk Operation Center)
- Andrea Cappai e Alessio Loche: Lab Forense
- Andrea Pasin: Hacking Networks 101: La Falsa Sicurezza della Client Isolation
- Marta Muto e Andrea Roncoroni: AI for Cybersecurity, OSINT e ingegneria sociale
- Alessandro Alampi: Dalle Basi ai Canali Nascosti
- Stefano Bonfanti, Matteo Bordignon, Marco Molinati: AI e Security: Strumenti per attaccanti e difensori

Ore 16.50 Pillole Cyber: Netability

Ore 16.52 Sessione 5, Sale

- Alessandro Alampi: alle Basi ai Canali Nascosti
- Marta Muto e Andrea Roncoroni: AI for Cybersecurity, OSINT e ingegneria sociale
- Andrea Cappai e Alessio Loche: Lab Forense
- Andrea Costantino: Dal lato oscuro del web alla Cyber Threat Intelligence
- Gianni Ricca e Emanuele Bianchi: Microsegmentazione intelligente
- Matteo Moro: Sovranità del dato: capire, valutare, agire

Ore 17.22 Sessione 6 ; Alessandro Oteri, Cyber Persuasion, PATIO

- Ore 17.50 Aperitivo offerto da ated con Betacom

PROGRAMMA SERALE

29 OTTOBRE 2025

Ore 18.00 Apertura Check-in

Ore 18.30 Inizio serata, presentazione di Luca Mauriello

Ore 18.40 Onorevole Norman Gobbi

Ore 18.50 VIP Guest: Greta Cristini - Cyber Geopolitics: strategie, poteri e vulnerabilità nel mondo interconnesso

Ore 19.10 Cyber Pillole a cura di Security Lab

Ore 19.15 Dante Marco Pollini e Michele Rusconi - Infrastrutture critiche

Ore 19.30 Cyber Pillole a cura di Ailanto

Ore 19.35 Nicolas Fasolo- Emergenza e psiche

Ore 19.50 Cyber Pillole a cura di Elmec Suisse

Ore 19.55 Panel finale moderato da Luca Mauriello
Ospiti: Massimo Baioni, Robert Bregy, Greta Cristini, Alessandro Oteri e Marta Muto

Ore 20.25 – Aperò-cena offerto da ated con Threema

ATED CYBER CHALLENGE LIVE - TRUST THE SIGNAL!

LA PRIMA ESPERIENZA INTERATTIVA IN CUI IL PUBBLICO DECIDE
CHI MERITA DI RESTARE SUL PALCO.
ENERGIA, FIDUCIA, RESPONSABILITÀ CONDIVISA.

Non è un evento da guardare, ma da vivere in prima persona.
Tu sei parte del “sistema immunitario” della Cyber Community.

Obiettivo

Trasformare i 13 workshop del pomeriggio in una vera cyber experience partecipata, dove ogni partecipante è parte attiva del giudizio e contribuisce alla qualità dell'evento.

Modalità di Partecipazione

Al check-in ogni partecipante riceverà:

- un layer colorato che lo identificherà nel suo mini gruppo;
- un cartellino giallo numerato personale.
- I partecipanti saranno suddivisi in 6 sessioni da seguire in base al colore assegnato.
- Tutte le sessioni saranno videoregistrate.
- Tutti i partecipanti ated Cyber Security Day 2025 che lo desiderano potranno successivamente acquistare le registrazioni integrali di tutti i workshop del pomeriggio.

Funzionamento dei Gruppi

Ogni gruppo (colore) ruoterà tra le diverse sale secondo la pianificazione prevista.
I facilitatori di sala controlleranno gli ingressi e supporteranno i relatori nella gestione dei tempi.

Il Potere del Cartellino Giallo

I partecipanti sono i guardiani della neutralità.

Se durante un workshop il relatore devia in promozione commerciale o autopubblicità, è possibile alzare il cartellino giallo.

Se due partecipanti (anche di gruppi diversi) alzano contemporaneamente il cartellino:

- il relatore viene segnalato immediatamente al team di coordinamento;
- il workshop viene interrotto e verificato;
- in caso di conferma della segnalazione, il relatore viene escluso dalle sessioni successive e dal programma futuro di ated Cyber Events.

Video e Replay

Ogni sala sarà videoregistrata per garantire trasparenza, qualità e accesso successivo ai contenuti.

I partecipanti potranno accedere (in forma opzionale) al pacchetto completo di 13 workshop on-demand.

Premio “Cyber Credibility”

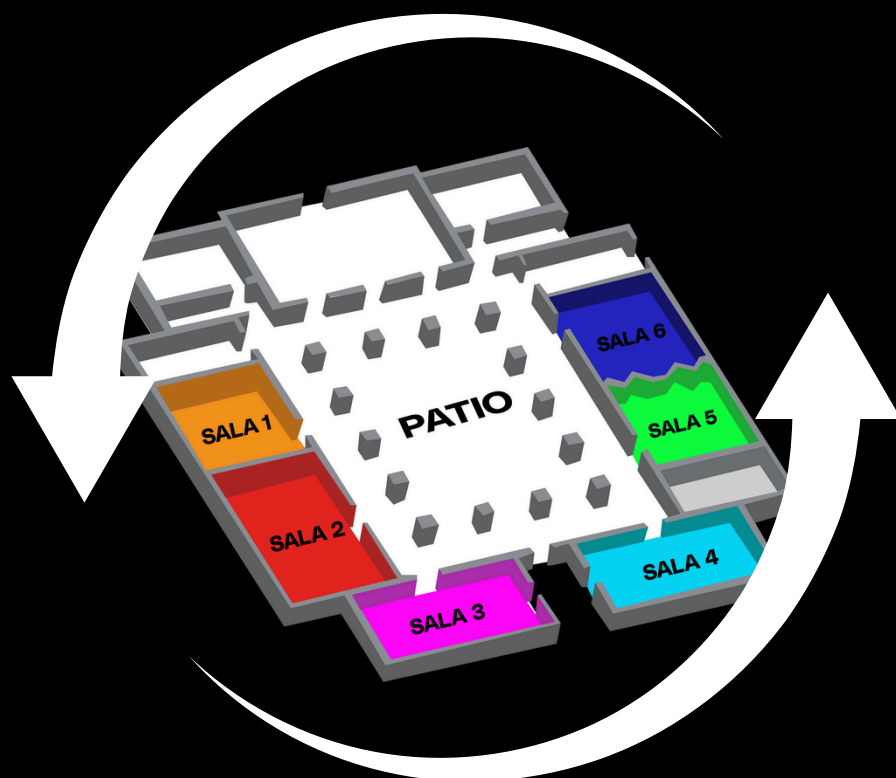
Alla fine dell'evento, il relatore o team più apprezzato (zero cartellini gialli + feedback positivi raccolti) riceverà il riconoscimento ufficiale:

 Cyber Credibility Award – ated 2025

REGOLE IN SINTESI

1	Layer colorato	Determina il gruppo e la sequenza dei workshop
2	Cartellino Giallo	Strumento etico del partecipante
3	Doppio giallo = STOP	Due segnalazioni attivano l'espulsione
4	Nessuna pubblicità	I Workshop devono essere neutri, pratici, dimostrativi e divulgativi
5	Videoregistrazione	tutti i contenuti saranno disponibili in seguito
6	Premio finale	Riconoscimento ufficiale al miglior relatore

Rotazione
ANTIORARIO



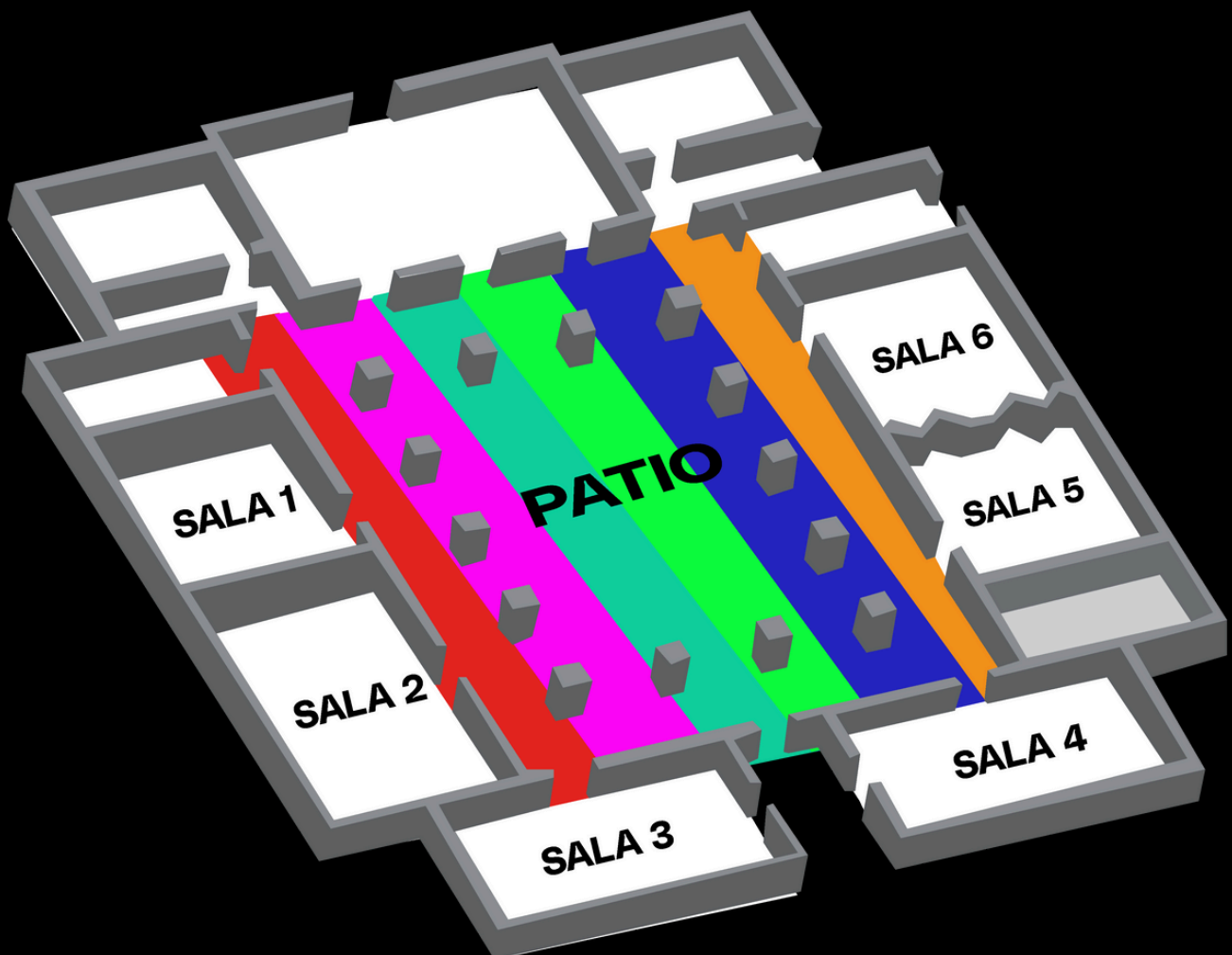
Ogni 30 minuti alla fine di ogni workshop ci sarà la rotazione delle persone nelle sale seguendo il senso antiorario.

PATIO

Ore 14.20 Sessione 1
Workshop Rocco Sicilia

Ore 15.32 Sessione 3
Workshop Massimo Bertaccini: CSE – Crypto Search Engine

Ore 17.22 Sessione 6
Workshop Alessandro Oteri, Cyber Persuasion, PATIO

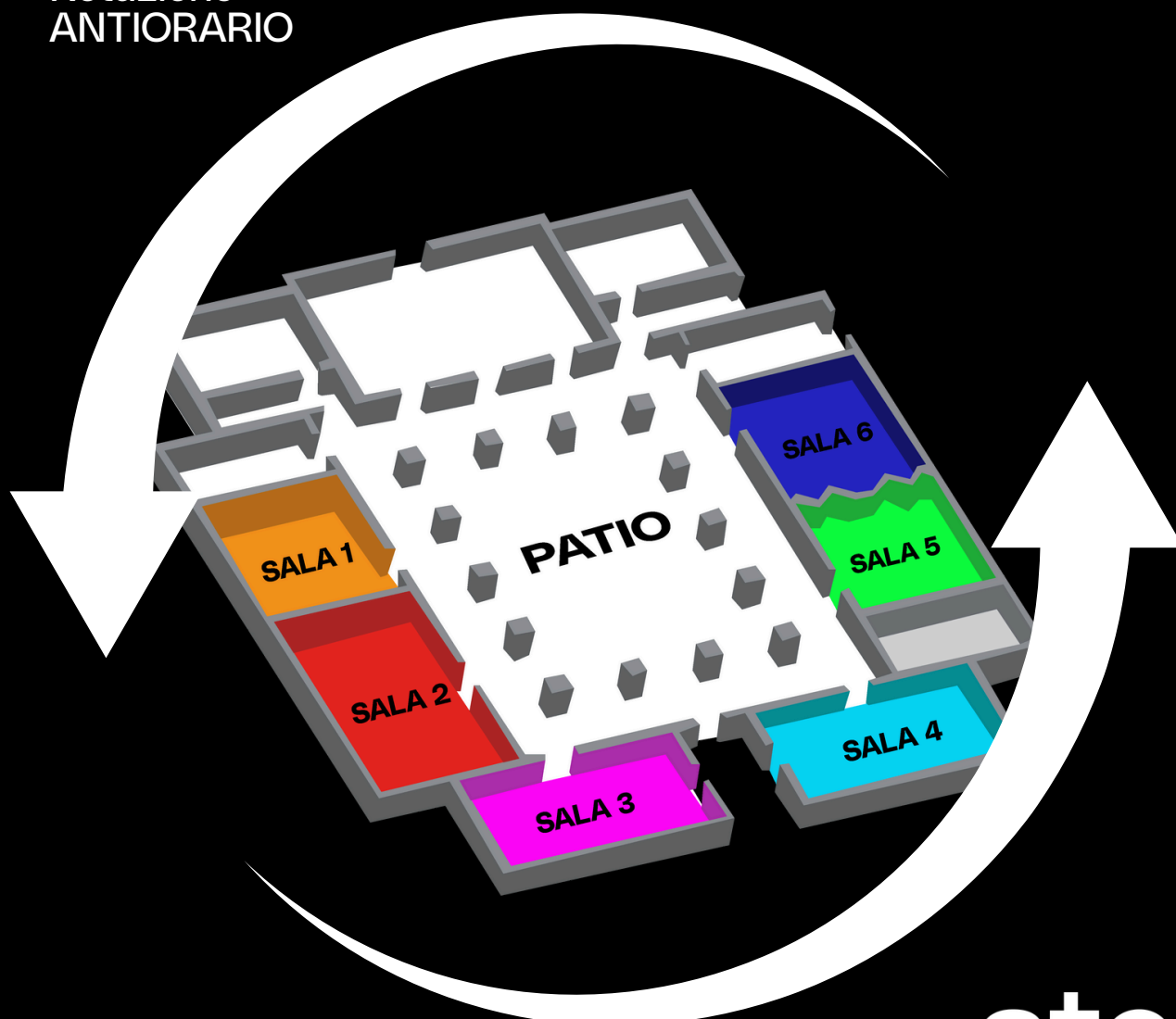


ORE 14:55 SESSIONE 2

Relatori e Workshop sale:

- Paolo Pezzoni SOC/ROC (Security/Risk Operation Center)
- Andrea Cappai e Alessio Loche: Lab Forense
- Andrea Pasin: Hacking Networks 101: La Falsa Sicurezza della Client Isolation
- Lorenzo Ladina: Attack Paths in Active Directory con BloodHound
- Gianni Ricca e Emanuele Bianchi: Microsegmentazione intelligente
- Martino Pozza: Cyber Challenge: Sopravvivi all'attacco!

Rotazione
ANTIORARIO

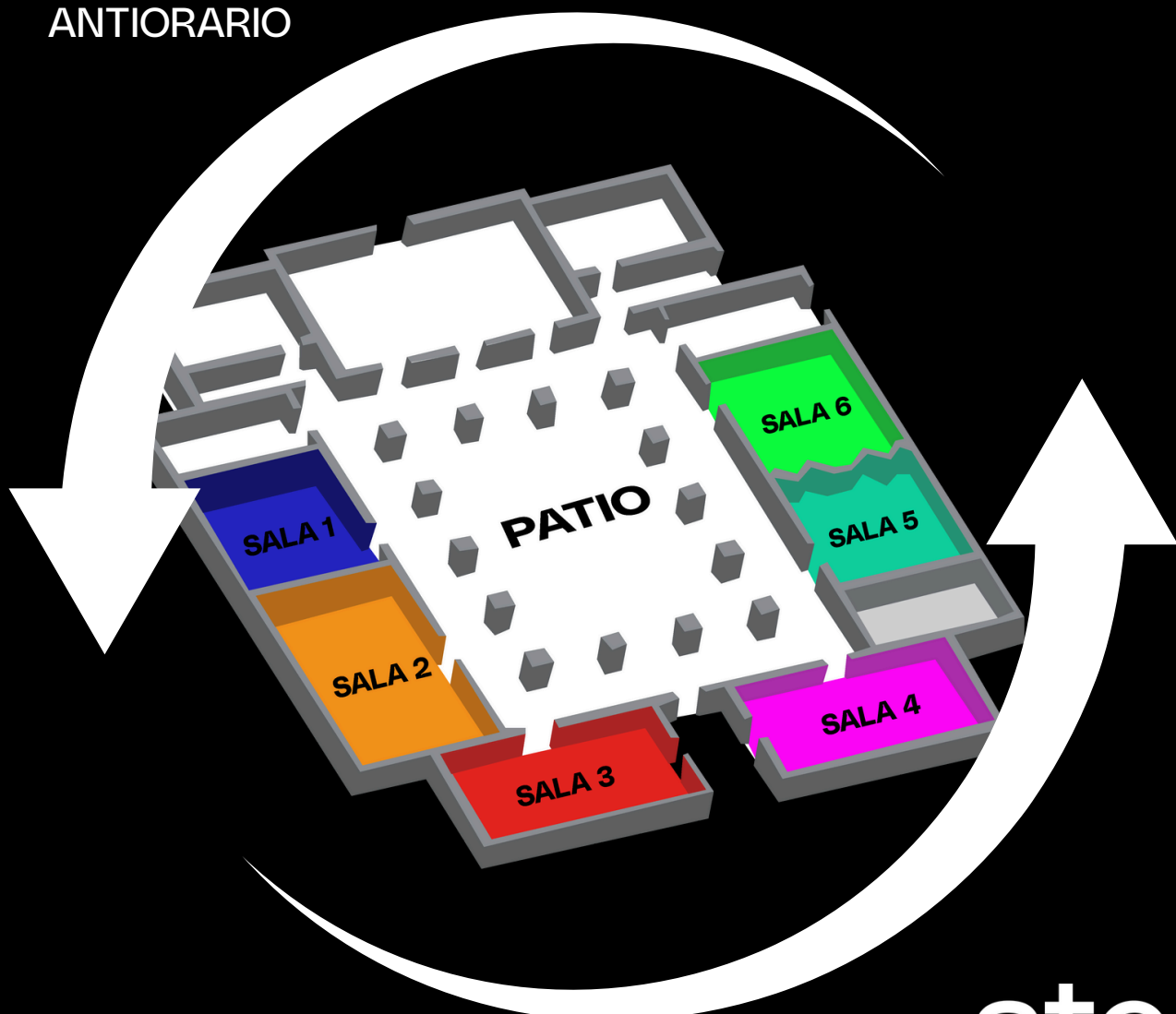


ORE 16:20 SESSIONE 4

Relatori e Workshop sale:

- Paolo Pezzoni SOC/ROC (Security/Risk Operation Center)
- Andrea Cappai e Alessio Loche: Lab Forense
- Andrea Pasin: Hacking Networks 101: La Falsa Sicurezza della Client Isolation
- Marta Muto e Andrea Roncoroni: I for Cybersecurity, OSINT e ingegneria sociale
- Alessandro Alampi: Dalle Basi ai Canali Nascosti
- AI e Security: Strumenti per attaccanti e difensori

Rotazione
ANTIORARIO

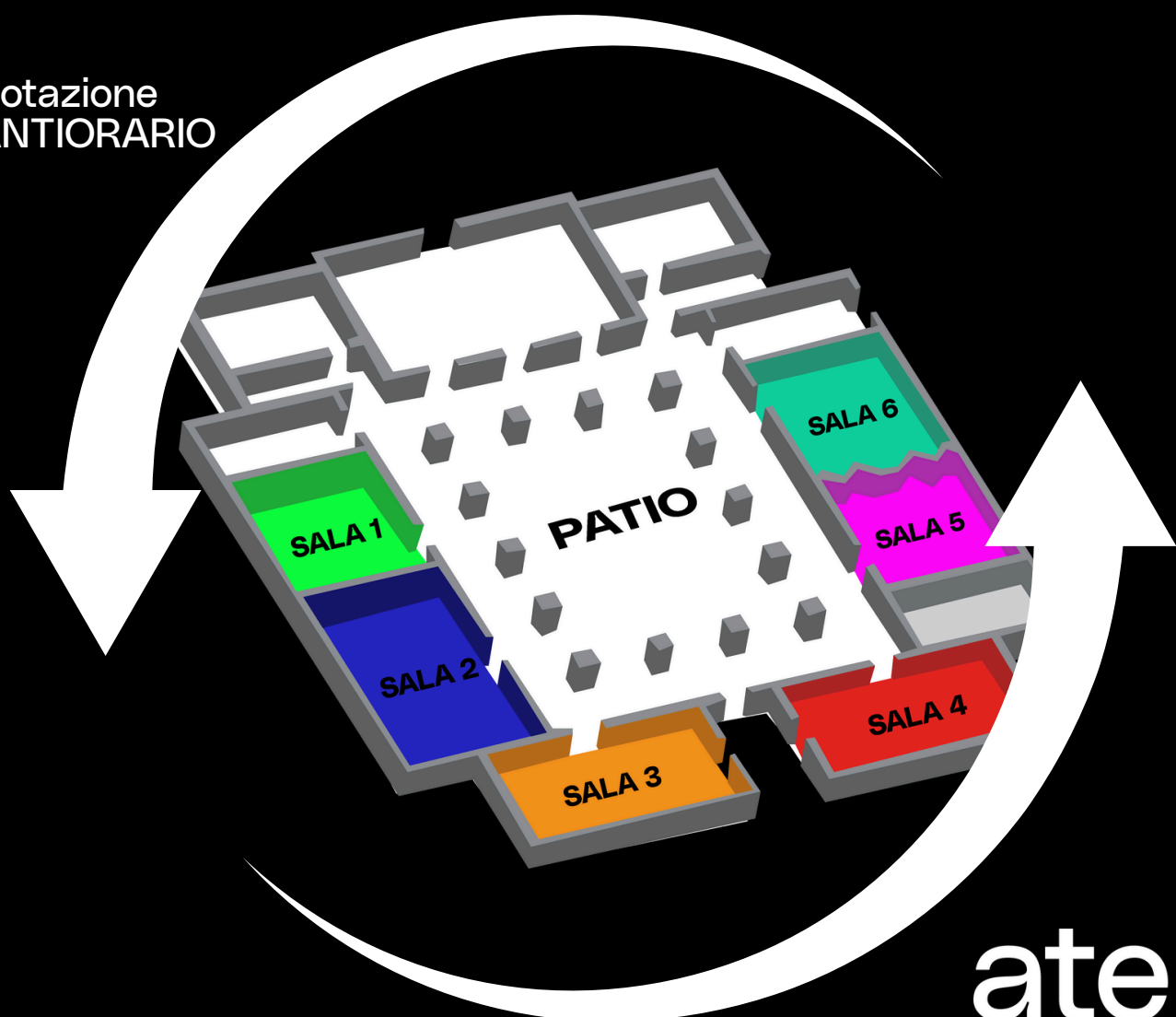


ORE 16:52 SESSIONE 5

Relatori e Workshop sale:

- Alessandro Alampi: alle Basi ai Canali Nascosti
- Marta Muto e Andrea Roncoroni: AI for Cybersecurity, OSINT e ingegneria sociale
- Andrea Cappai e Alessio Loche: Lab Forense
- Andrea Costantino: Dal lato oscuro del web alla Cyber Threat Intelligence
- Gianni Ricca e Emanuele Bianchi: Microsegmentazione intelligente
- Matteo Moro: Sovranità del dato: capire, valutare, agire

Rotazione
ANTIORARIO



RELATORI WORKSHOP



ated



ROCCO SICILIA

Esperto di sicurezza informatica con oltre 20 anni di esperienza, ha lavorato a lungo in contesti italiani e, con l'ingresso in NTS, ha ampliato la propria attività verso aziende internazionali ed europee. Collabora in particolare con grandi gruppi industriali e con il settore finance, soprattutto banche.

È specializzato in penetration testing e red teaming, con un approccio pratico e mirato alla protezione delle infrastrutture critiche. Partecipa regolarmente a conferenze di settore, portando contributi tecnici e case study reali.

Oltre al lavoro in azienda, segue progetti open source in ambito security e cura un blog e un podcast dedicati alla divulgazione e alla condivisione di conoscenza.

WORKSHOP:

Obiettivo della sessione: assumere la mentalità del threat actor per comprendere motivazioni, fasi e tecniche utilizzate nelle fasi più aggressive dell'attacco — in particolare exploiting, installation, C2 ed exfiltration. Verranno analizzati vettori e vulnerabilità tipiche, tecniche di social engineering e il percorso dall'accesso iniziale alla compromissione estesa; nella fase di installation si spiegheranno persistenza, uso di loader e occultamento di artefatti. La parte centrale sarà dedicata al C2: architetture comuni, beaconing, tunneling e tecniche di camuffamento del traffico, con gli indicatori rilevabili su host e rete. Per l'exfiltration illustreremo pattern pratici (chunking, timing, canali covert) e il relativo impatto operativo e normativo. Demo controllate in laboratorio mostreranno l'impatto su file, processi e connettività in ambienti isolati a fini didattici. La sessione si chiude con contromisure concrete e applicabili: system hardening, network segmentation, monitoraggio comportamentale e threat hunting mirato a C2 ed exfiltration.



PAOLO PEZZONI

Consulente senior in cyber defense, governance e gestione del rischio digitale.

SOC/ROC (Security/Risk Operation Center)

- Il workshop porta i partecipanti dentro la realtà di un centro operativo di sicurezza, simulando il rilevamento e la gestione di un incidente informatico. Verranno illustrate metodologie, strumenti e ruoli coinvolti in un SOC/ROC moderno, con attenzione al coordinamento tra tecnologia e fattore umano. L'obiettivo è far vivere l'esperienza pratica di come si affronta un attacco, dall'individuazione all'analisi fino alla risposta operativa.



ANDREA CAPPAI



ALESSIO LOCHE

Andrea Cappai Digital Forensics Expert, CEO ingK & Karel Sport, formatore in ambito investigazioni digitali

Alessio Loche consulente informatico forense e tecnico esperto di laboratorio

Lab Forense

- Estrazione logica e fisica dei dati: utilizzo di strumenti e procedure forensi per acquisire in maniera completa le informazioni contenute nei dispositivi mobili.
- Chip-off e micro-saldature: interventi su componenti elettronici (BGA, SMT, SMD) per accedere direttamente alla memoria in casi di gravi danneggiamenti.
- Bypass di protezioni e blocchi: tecniche hardware/software per superare ostacoli all'accesso ai dati, mantenendo la catena di custodia.
- Recupero dati da dispositivi compromessi: operazioni di laboratorio su smartphone danneggiati da urti, liquidi o guasti elettronici.
- Documentazione e validazione forense: produzione di report certificati sull'acquisizione, utili in ambito legale (civile o penale).



ANDREA PASIN

Offensive Security Engineer presso AWS, specializzato in Red Team e ricerca avanzata.

Hacking Networks 101: La Falsa Sicurezza della Client Isolation, a cura di Andrea Pasin

Molti credono che la funzionalità di Client Isolation garantisca la sicurezza su una rete Wi-Fi pubblica, isolando ogni utente. In questo workshop pratico, smonteremo questo mito. Dimostrerò come, sfruttando un punto debole spesso trascurato nel protocollo di rete, un attaccante possa bypassare questa protezione e causare un attacco di Denial of Service (DoS) che blocca l'intera rete. Scopri perché la vera sicurezza non si basa su una singola funzionalità, ma su una difesa a più livelli.



LORENZO LADINA

Penetration Tester, laureando magistrale in Computer Science & Engineering presso il Politecnico di Milano

Attack Paths in Active Directory con BloodHound

Appassionato di Active Directory, Red Teaming e Offensive Security, Lorenzo mostra come mappare e sfruttare i percorsi di escalation in ambienti enterprise usando BloodHound e tool complementari. Il workshop è pratico e orientato alle tecniche reali: dall'analisi di ACL/ACE fino ai percorsi che possono portare a Domain Admin. Concluderemo con mitigazioni e suggerimenti per detection.

A circular portrait of Gianni Ricca, a man with short grey hair, wearing a dark suit jacket over a light blue shirt. The portrait is framed by a green circular graphic with tick marks. The background of the entire slide is black with falling green binary code (0s and 1s).

GIANNI RICCA

A circular portrait of Emanuele Bianchi, a man with a beard and glasses, wearing a light-colored shirt. The portrait is framed by a green circular graphic with tick marks. The background of the entire slide is black with falling green binary code (0s and 1s).

**EMANUELE
BIANCHI**

Gianni Ricca Senior Network & Security Engineer
Emanuele Bianchi Responsabile EMEA di ZeroNetworks.

Microsegmentazione intelligente: difendere ambienti legacy e OT dai movimenti laterali – Zero Trust

- Le reti aziendali moderne comprendono spesso una combinazione di ambienti IT tradizionali, sistemi legacy e infrastrutture OT/ICS difficili da proteggere con i metodi classici. In questo workshop mostreremo come la microsegmentazione rappresenti oggi una delle strategie più efficaci per limitare i movimenti laterali degli attaccanti, ridurre la superficie d'attacco e rendere sostenibile la sicurezza anche in contesti complessi o non aggiornabili. Obiettivi del workshop è comprendere le differenze tra segmentazione tradizionale e microsegmentazione. Analizzare le sfide specifiche negli ambienti legacy e OT (assenza di agent, sistemi non patchabili, interruzioni minime). Mostrare come è possibile applicare policy di isolamento e controllo anche in sistemi ibridi. Dimostrare un esempio pratico di riduzione del rischio attraverso il blocco dei movimenti laterali.

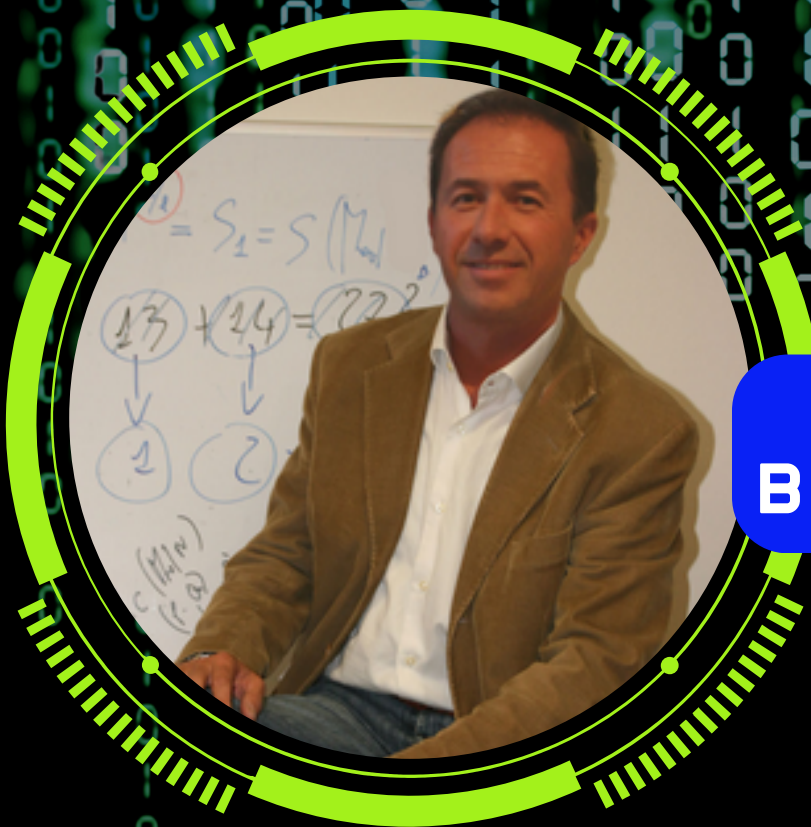


MARTINO POZZA

Security Governance e Risk Management Consultant presso AISEC Security Advisory

Cyber Challenge: Sopravvivi all'attacco!

Un'esperienza interattiva in formato "gioco di ruolo" che simula la gestione di un incidente informatico. I partecipanti collaboreranno per contenere un attacco entro 30 minuti, risolvendo enigmi e prendendo decisioni strategiche in modo da sperimentare un workflow di incident response facilmente adattabile al proprio contesto aziendale.



**MASSIMO
BERTACCINI PHD**

È un esperto riconosciuto in crittografia avanzata, sicurezza informatica, interfacce neurali e tecnologie quantistiche.

È autore e visionario nella progettazione del primo motore di ricerca su dati cifrati (Crypto Search Engine), capace di eseguire query senza la necessità di decifrare le informazioni — una svolta pionieristica nel campo della privacy e della protezione dei dati.

Attualmente è CEO e cofondatore di Cryptolab Inc., oltre a ricoprire ruoli accademici e di ricerca nelle aree emergenti del quantum computing e dell'interazione cervello-macchina (progetto BrainWaves)

CSE – Crypto Search Engine: cercare nei dati cifrati nell'era quantistica

Scoprire come un motore di ricerca possa operare su dati completamente cifrati, mantenendo prestazioni elevate, privacy totale e resilienza quantistica, grazie all'integrazione con tecnologie di crittografia e interfacce quantum-ready.

- Introduzione – Dal cloud sicuro all'era quantistica
- Demo live – Ricerca cifrata in azione
- Approfondimento tecnico – Quantum & Crypto Security
- Conclusioni e Q&A



**ALESSANDRO
ALAMPI**

Security Researcher e Incident Responder in Yarix (Var Group), esperto in programmazione e forensics.

Dalle Basi ai Canali Nascosti: Metodi di Esfiltrazione dati per il Ricercatore di Sicurezza

Questo workshop esplora le tecniche usate per trasferire dati fuori da una rete compromessa — dalle modalità più comuni e leggibili (Rclone, FTP, SFTP/WinSCP) fino ai canali più sofisticati e "covert" (DNS tunneling, steganografia, covert channels). L'approccio è orientato alla difesa: capire come funzionano i metodi d'esfiltrazione per poterli rilevare, mitigare e costruire contromisure efficaci.



**STEFANO
BONFANTI**



**MATTEO
BORDIGNON**



MARCO MOLINATI

Stefano Bonfanti, Matteo Bordignon, Marco Molinati:

AI e Security: Strumenti per attaccanti e difensori

Il workshop ha lo scopo di illustrare l'utilizzo dell'intelligenza artificiale da parte degli attaccanti e dei difensori. Andremo a ricostruire l'evoluzione del phishing partendo dalle prime campagne MAPS, passando per Ham e Spam, Feature Engineering e Deep Learning. Ci focalizzeremo sulle nuove campagne di phishing basate su AI e sulla facilità di utilizzo di questi strumenti da parte degli attaccanti. Illustreremo come l'AI può essere utilizzata dagli speciali del SOC per analizzare in modo avanzato le mail di phishing attraverso la descrizione di un software sviluppato a tale scopo. Presenteremo inoltre alcuni casi di simulazioni di phishing basate su Deepfake e Voice Phishing. Concluderemo con un'analisi dei modelli di Machine Learning

A circular portrait of a woman with long, wavy brown hair, wearing a grey and black striped sweater. The portrait is framed by a green circular border with a dashed line and a green arc at the top. The background of the entire slide is black with a green binary code (0s and 1s) pattern.

MARTA MUTO

A circular portrait of a man with short brown hair and glasses, wearing a dark blue button-down shirt. The portrait is framed by a green circular border with a dashed line and a green arc at the top.

**ANDREA
RONCORONI**

Marta Muto SOC Analyst L2 presso Cybersec services.

Andrea Roncoroni Senior Security Consultant presso Cybersec services.

AI for Cybersecurity, OSINT e ingegneria sociale: chi, dove, quando e perché lo sappiamo

- Il workshop esplora come l'intelligenza artificiale potenzi le tecniche di OSINT e di ingegneria sociale, mostrando come sia possibile raccogliere, analizzare e correlare informazioni sensibili da fonti aperte. Attraverso casi pratici, i partecipanti scopriranno l'impatto di questi strumenti sulla sicurezza delle organizzazioni e comprenderanno come prevenirne i rischi. Vuole stimolare un approccio critico e consapevole all'uso delle tecnologie emergenti in contesti cyber.

A circular portrait of a man with dark hair and a beard, wearing a dark suit jacket over a white shirt. The portrait is framed by a bright green circular graphic with radial lines and dots. The background of the entire slide is black with a green digital rain effect of binary code (0s and 1s).

ANDREA COSTANTINO

Senior Security Consultant specializzato in Penetration Test e Red Team Assessment presso Security Lab SA

Dal lato oscuro del web alla Cyber Threat Intelligence: comprendere per difendersi

Il Dark Web è la parte più nascosta e rischiosa di Internet, dove ogni giorno circolano dati rubati e strumenti di attacco. Capirne il funzionamento è essenziale per comprendere come nascono e si diffondono le minacce informatiche. In questo talk esploreremo i diversi livelli del Web e vedremo come la Cyber Threat Intelligence sfrutta queste fonti per trasformare i dati sulle minacce in conoscenza utile alla difesa.



MATTEO MORO

esperto di Security e Network, (ex Head of IT Infrastructure Solutions Delivery and Network di Viseca Payment Services SA)

Sovranità del dato: capire, valutare, agire

Il workshop si propone di offrire ai partecipanti strumenti concreti per analizzare le dipendenze digitali e tracciare un percorso verso una maggiore autonomia nella gestione dei dati aziendali e personali. Attraverso un approccio interattivo, i partecipanti saranno coinvolti nella costruzione di una mappa delle dipendenze (tecnologiche, operative, giuridiche e finanziarie) e nella valutazione dei costi (nascosti ed espliciti) che la dipendenza dai grandi provider cloud genera per le organizzazioni.

Temi chiave

- Identificazione delle principali dipendenze da infrastrutture, software e servizi cloud
- Analisi delle quattro dimensioni della sovranità digitale: giuridica, finanziaria, operativa e strategica.
- Discussione sui costi invisibili della dipendenza, come lock-in tecnologico, tempi di migrazione e perdita di autonomia.
- Strategie concrete di resilienza e indipendenza: multi-provider, open standard, roadmap di uscita graduale e interoperabilità.

Attività e interazione

Il workshop prevede momenti di autovalutazione e confronto diretto, con esercizi pratici e la costruzione di una matrice finale utile per identificare i primi passi concreti verso l'autonomia digitale dei partecipanti.



ALESSANDRO OTERI

Chief Information Security Officer (CISO), Alessandro Oteri è un professionista con consolidata esperienza nella sicurezza informatica, specializzato nella protezione delle infrastrutture digitali e nella gestione dei rischi legati al cybercrime. Nel corso della sua carriera ha ricoperto ruoli di responsabilità in ambito IT e Security, occupandosi di definire strategie di sicurezza, implementare processi di compliance e coordinare team dedicati alla difesa delle informazioni aziendali. In qualità di CISO, Oteri guida lo sviluppo e l'attuazione delle politiche di sicurezza, con un approccio che integra governance, tecnologia e formazione del personale. È anche co-autore del libro "Information Systems, from cloud to cybersecurity", testo di riferimento per comprendere i principi di protezione nel mondo del cloud. Oltre al ruolo manageriale e accademico, è attivo come divulgatore: è ideatore di un podcast di awareness sulla cybersecurity PensieroSicuro, seguito da oltre 60.000 utenti, attraverso cui diffonde conoscenze e buone pratiche per accrescere la consapevolezza digitale.

Cyber Persuasion: quando il business vuole investire, ma non lo sa ancora

Attraverso situazioni reali, esploreremo come riconoscere il momento giusto per proporre un investimento in sicurezza e come scegliere le parole che favoriscono l'ascolto invece della resistenza. Un'esperienza interattiva per capire quali termini evitare, quali usare e come adattare il linguaggio al contesto e alle persone. Non promette budget immediati, ma garantisce messaggi più chiari, credibili e orientati alla decisione.

PROGRAMMA SERALE

29 OTTOBRE 2025

Ore 18.00 Apertura Check-in

Ore 18.30 Inizio serata, presentazione di Luca Mauriello

Ore 18.40 Onorevole Norman Gobbi

Ore 18.50 VIP Guest: Greta Cristini - Cyber Geopolitics: strategie, poteri e vulnerabilità nel mondo interconnesso

Ore 19.10 Cyber Pillole a cura di Security Lab

Ore 19.15 Dante Marco Pollini e Michele Rusconi - Infrastrutture critiche

Ore 19.30 Cyber Pillole a cura di Ailanto

Ore 19.35 Nicolas Fasolo- Emergenza e psiche

Ore 19.50 Cyber Pillole a cura di Elmec Suisse

Ore 19.55 Panel finale moderato da Luca Mauriello
Ospiti: Massimo Baioni, Robert Bregy, Greta Cristini, Alessandro Oteri e Marta Muto

Ore 20.25 – Aperò-cena offerto da ated con Threema



GRETA CRISTINI

Analista geopolitica, inviata di guerra e giornalista. Dopo una carriera a New York come avvocatessa specializzata in anticorruzione, ha scelto di seguire la sua passione per la geopolitica e l'analisi dei conflitti, collaborando con testate e centri di ricerca internazionali. Dall'Ucraina ad altri teatri di crisi, racconta con rigore e chiarezza gli scenari globali, esplorando il ruolo delle tecnologie emergenti, delle minacce ibride e della cyber security.

Cyber Geopolitics: strategie, poteri e vulnerabilità nel mondo interconnesso



**DANTE MARCO
POLLINI**



**MICHELE
RUSCONI**

- **Dante Marco Pollini** Senior ICT Internal Auditor @ Ente Ospedaliero Cantonale (EOC)
- **Michele Rusconi** – Responsabile Servizi IT/OT e Cybersicurezza presso Aziende Industriali di Lugano (AIL) SA.

Infrastrutture critiche



NICOLAS FASOLO

Security Researcher, Incident Response Team Leader in Yarix (Var Group), CEH Master, divulgatore tecnico

Emergenza e psiche



GRETA CRISTINI



MARTA MUTO



MASSIMO BAIONI



ALESSANDRO OTERI



ROBERTO BREGY

ROUNDTABLE GUESTS

- Greta Cristini – Analista geopolitica, inviata di guerra e giornalista
- Massimo Baioni Head of Sales at di Tinext Cloud, si dedica ad accompagnare le aziende nel percorso di adozione del Cloud. Il suo obiettivo è garantire una gestione ottimale delle infrastrutture IT e creare opportunità di innovazione.
- Roberto Bregy Segretario Comunale della Città di Lugano.
- Alessandro Oteri, CISO ed esperto di cybersecurity, è co-autore di "Information Systems, from Cloud to Cybersecurity" e ideatore del podcast PensieroSicuro.
- Marta Muto SOC Analyst L2 presso Cybersec services.