NEWSLETTER
Speciale Security Summit Streaming Edition - novembre 2021

Clusit
Associazione Italiana per la Sicurezza Informatica

INDICE

1. Speciale Security Summit 2021

Dal 9 all'11 novembre si terrà l'edizione autunnale del Security Summit Streaming Edition 2021.
https://securitysummit.it/eventi/streaming-edition-novembre-2021/info

La partecipazione è libera e gratuita ma è necessario iscriversi on line

La partecipazione alle sessioni consente di acquisire crediti CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua.
L'Attestato di Partecipazione viene rilasciato solo a chi ha assistito in diretta all'intera sessione e risulta regolarmente registrato.
Gli attestati saranno inviati, per email, solo a chi ne farà richiesta a attestati@clusit.it.

Ringraziamo gli sponsor e i partner di questa edizione del 2021
https://securitysummit.it/eventi/streaming-edition-novembre-2021/sponsor.

Vi proponiamo 35 sessioni, di cui riportiamo di seguito i dettagli.
Maggiori informazioni sono disponibili su https://securitysummit.it/eventi/streaming-edition-novembre-2021/agenda.

2. Programma di martedì 9 novembre

09:00-11:00 - SALA AFRICA - SESSIONE PLENARIA

"Presentazione del Rapporto Clusit sulla sicurezza ICT in Italia – Edizione ottobre 2021"

Continua nei primi sei mesi dell'anno la crescita degli attacchi cyber a livello globale, che segnano tra l'altro nel periodo il record negativo degli eventi nel nostro Continente. Un quarto degli incidenti di sicurezza verificatisi tra gennaio e giugno 2021 è infatti avvenuto in Europa: questo e molti altri dati ancora tra i risultati emersi nel prossimo Rapporto Clusit.

Apre i lavori e introduce: Gabriele Faggioli, Presidente Clusit

Modera: Alessio Pennasilico, CTS Clusit

Ospite d'onore: Nunzia Ciardi, Direttore del Servizio Polizia Postale e delle Comunicazioni

Intervengono alcuni degli autori del Rapporto:
Andrea Zapparoli Manzoni, Clusit
Marco Raimondi, Fastweb

Segue una tavola rotonda con gli **esperti di security** di alcuni dei principali fornitori di prodotti e servizi di sicurezza ICT:
Aldo Di Mattia, Fortinet
Carlo Mauceli, Microsoft

Al termine della sessione, solo a partire dalle ore 11:30, il nuovo rapporto potrà essere richiesto su https://clusit.it/rapporto-clusit/

11:20-12:00 – SALA AFRICA - ATELIER TECNOLOGICO

"Come sconfiggere il ransomware scegliendo la sicurezza unificata"

L'emergere del ransomware, che a oggi è forse la forma di reato informatico più redditizia, segna un profondo cambiamento nel modo in cui i criminali informatici sfruttano i dati delle loro vittime per ottenere un vantaggio economico. Con il ransomware, gli aggressori non hanno più la necessità di rubare i dati per rivenderli, ma sfruttano l'importanza che quei dati assumono per la vittima. Questo cambiamento di modello espone innumerevoli organizzazioni, molte delle quali per parecchio tempo si sono sentite al riparo da questi attacchi perché di dimensioni contenute, al rischio di finire nel mirino dei criminali informatici. L'implementazione di una piattaforma di sicurezza unificata permette di intervenire in diversi punti della kill chain, impedendo la prosecuzione dell'attacco verso l'obiettivo. L'aspetto essenziale di questo approccio è la capacità di correlare gli eventi di sicurezza della rete e degli endpoint con l'intelligence sulle minacce per rilevare, dare priorità e intraprendere azioni immediate allo scopo di arrestare gli attacchi malware. Nel corso dell'atelier scopriremo come le organizzazioni di tutte le dimensioni possono difendersi dalle minacce malware avanzate, compresi gli attacchi ransomware, grazie all'utilizzo di una piattaforma multilivello.

Relatore: Gianluca Pucci

11:20-12:00 – SALA EUROPA - ATELIER TECNOLOGICO

"Internet delle cose (IoT): Benvenuti nel selvaggio West"

Quando è stata l'ultima volta che la vostra azienda ha monitorato i dispositivi IoT installati? Il vostro reparto IT si è dovuto occupare della loro manutenzione? Se avete risposto sì a una di queste domande, la vostra azienda potrebbe essere già stata compromessa, ad esempio attraverso una semplice stampante... L'IoT non è una novità, ma lo sapevate che oggi è l'area di vulnerabilità che sta crescendo più rapidamente? L'esperto di sicurezza Luca Pesce illustrerà le minacce e i semplici meccanismi che possono essere adottati per proteggere le organizzazioni. Non lasciate che l'IoT cresca in modo incontrollato!

Relatore: Luca Pesce

12:20-13:00 – SALA AFRICA - ATELIER TECNOLOGICO

"Case Study: Come Tiscali ha modernizzato le Security Operations"

Da operatore di telecomunicazioni e Internet Service Provider, è importante che Tiscali operi in modo sicuro per garantire la continuità del servizio e la protezione di dati personali dei suoi clienti. Disponendo di limitate risorse in ambito Cyber Security, ha optato per un'attività di comprensione iniziale dello stato delle Operations e successivamente di investire nel potenziamento della cyber vigilance.

Partecipa a questo atelier per comprendere come Tiscali:
Ha condotto un assessment sulla cyber security
Ha valutato i vendors per trovare la soluzione migliore al fine di soddisfare i requisiti di conformità e gli obiettivi strategici
Ora disponga di un sistema centralizzato di threat detection and response, con visibilità completa su tutta l'infrastruttura IT
Come Secureworks e DI.GI International hanno supportato Tiscali nella trasformazione della cyber security

Relatori: Luca Manunza, Angelo Salice, Antonio Pusceddu

12:20-13:00 – SALA EUROPA - ATELIER TECNOLOGICO

"Dopo un annus horribilis, non solo pandemia ma anche cybercrime"

Mentre la pandemia globale stravolgeva le routine lavorative e familiari, i criminali informatici coglievano la palla al balzo. E ora, nel 2021, questi criminali informatici fanno leva sul loro vantaggio moltiplicando gli attacchi. La kill chain di una serie di attacchi sempre piu sofisticati fa leva su debolezze umane, infrastrutture inadatte, cambio dell'ambiente di lavoro, nuove vulnerabiltià e vecchi trucchi ora più che mai efficaci, processi spesso non aggiornati agli strumenti digitali in uso, security basics non sempre solide.

Relatore: Antonio Ieranò

14:00-15:00 - SALA AFRICA - SESSIONE GESTIONE SICUREZZA

"Parola d'ordine: meno. Togliere per aggiungere valore alla cyber security"

La tecnologia progredisce ogni giorno, il business si trasforma, gli strumenti impiegati in azienda cambiano. E gli attaccanti? Sono già un passo avanti e trovano altri modi – o reinventano quelli già noti - per sfruttare eventuali lacune. Di fronte a minacce più sofisticate, ambienti IT più complessi, attacchi mirati, non serve aggiungere, bisogna semplificare. Al massimo. Dove stiamo andando? Come possiamo disegnare la cyber security di domani?

Relatori: Andrea Muzzi, Luca Bechelli

14:00-15:00 – SALA EUROPA – ATELIER TECNOLOGICO a cura del Dipartimento di Informatica "Giovanni Degli Antoni" dell'Università degli Studi di Milano

"La ricerca in cybersecurity: facciamo il punto"

Se oggi l'exploiting di un memory error exploit, che per vent'anni ha rappresentato il principali vettore di attacco, è diventato un'attività riservata a pochi, lo dobbiamo al lavoro di centinaia di ricercatori che nell'arco degli anni hanno messo a punto le contromisure che oggi, adottate da tutti i principali sistemi operativi, rendono estremamente complessa l'effettuazione di un simile attacco. La ricerca in cybersecurity, come in ogni altra disciplina, dovrebbe essere il principali strumento di contrasto alla insicurezza dei sistemi. Eppure non se ne parla mai. Gli eventi che parlano di cybersecurity si susseguono a ritmo forsennato ma la ricerca è il grande assente.
In quest'ora di chiacchierata cercheremo di fare il punto della situazione e forniremo una breve descrizione di due progetti di ricerca in corso presso il nostro laboratorio.

Relatore: Danilo Bruschi

"PoW-How: An Enduring Timing Side-Channel to Evade Online Malware Sandboxes"
Online malware scanners are one of the best weapons in the arsenal of cybersecurity companies and researchers. A fundamental part of such systems is the sandbox that provides an instrumented and isolated environment (virtualized or emulated) for any user to upload and run unknown artifacts and identify potentially malicious behaviors. The most common technique used by malware for evading the analysis system is to monitor the execution environment, detect the presence of any debugging artifacts, and hide its malicious behavior if needed. This is usually achieved by looking for signals suggesting that the execution environment is not belong to a the native machine, such as specific memory patterns or behavioral traits of certain CPU instructions. In this talk, I will show how an attacker can evade detection on such online services by incorporating a Proof-of-Work (PoW) algorithm into a malware sample. Specifically, we leverage the asymptotic behavior of the computational cost of PoW algorithms when they run on some classes of hardware platforms to effectively detect a non bare-metal environment of the malware sandbox analyzer.
Relatore: Andrea Lanzi

"Gli attacchi basati su side channel e fault injection, introduzione alla teoria e casi pratici"
Negli ultimi anni i dispositivi embedded sono sempre più presenti nelle nostre vite, ed alcuni di essi sono utilizzati anche in situazione safety-critical come ad esempio i dispositivi medicali o il supporto alla guida autonoma. Garantire la sicurezza ed il corretto funzionamento di questi sistemi diventa sempre più sfidante e le possibilità di attacco sempre più ampie. In questa presentazione vedremo un'introduzione ai concetti alla base degli attacchi side channel e fault injection e alcuni casi reali in cui sono stati utilizzati.
Relatore: Guido Bertoni

15:20-16:20 – SALA AFRICA - SESSIONE GESTIONE SICUREZZA

"Digital Transformation & Smart Working: solo una strategia olistica può proteggere le aziende"

La pandemia ha obbligato le aziende e i suoi dipendenti a modificare le modalità di lavoro: lo smart working è uno dei cambiamenti più evidenti. Il lavoro da remoto, però, sottopone le aziende a numerose minacce che ledono la propria sicurezza informatica. Quando si parla di Digital Transformation la cybersecurity è spesso un argomento che viene tralasciato, ma in un mercato che evolve e che sottopone le imprese a sempre più rischi informatici, la tecnologia è l'unico mezzo di supporto. La soluzione VMware Carbon Black è uno dei mezzi più efficaci cui le aziende possono affidarsi per avere un supporto immediato ai problemi che rientrano nel macro-tema degli incidenti informatici.

Modera: Alessio Pennasilico, Clusit

Partecipano:
Matteo Frare Barutti, Enterprise Account Executive dell'offering CyberSecurity, VMware
Massimo Brugnoli, Business Development Manager, Project Informatica
Vicki Vinci, Responsabile dello sviluppo di new business, Kirey Group

15:20-16:20 – SALA EUROPA – SESSIONE SULLA GESTIONE DELLA SICUREZZA

"Crisi d'Identità: mettere in sicurezza l'organizzazione aiuta a contrastare gli attacchi emergenti. Anche quando si chiamano ransomware"

Non parleremo della crisi di mezza età dei relatori (brillantemente in gestione - ndr). Andremo invece ad analizzare i dati del Rapporto Clusit confrontandoli con le survey CyberArk, per

comprendere come e perchè nonostante i più moderni aggiornamenti tecnologici le aziende sono ancora vittime dei medesimi attacchi. Non solo: cercheremo anche di fornire un punto di vista pratico su come i concetti di #zerotrust e #leastprivilege possono essere declinati in azioni concrete.

Relatori: Luca Bechelli, Massimo Carlotti

16:40-17:40 – SALA AFRICA - SESSIONE GESTIONE SICUREZZA

"Sicurezza dei dispositivi e continuità aziendale: come conciliare questi due aspetti nel nuovo mondo ibrido"

La fase di trasformazione post-pandemica sta ridefinendo i perimetri tradizionali del lavoro e le relative esigenze di sicurezza; le organizzazioni si orientano verso uno modello ibrido e 'distribuito', più flessibile, ma potenzialmente più a rischio per la cybersecurity. È importante contenere gli attacchi informatici in prossimità del punto di origine, circoscrivendo rapidamente l'azione dell'hacker e limitando così eventuali danni. Un altro aspetto chiave è estendere il concetto di Zero Trust anche agli endpoint, perché è proprio dai PC degli utenti finali che parte il numero maggiore di attacchi. Questo approccio presuppone una maggiore 'responsabilità' degli utenti, che spesso si mostrano frustrati o insofferenti alle limitazioni e alle procedure richieste dai responsabili per aumentare la protezione degli strumenti di lavoro. HP ha introdotto sul mercato una nuova generazione di soluzioni per aumentare la protezione e la cyber-resilienza degli endpoint, senza però incidere sulla produttività.

Relatori: Giampaolo Parravicini, Alessio Pennasilico

16:40-17:20 – SALA EUROPA – ATELIER TECNOLOGICO

"Confidential Computing to complete Data Protection Life Cycle"

La tecnologia legata al Confidential Computing può aiutare le aziende mantenere riservatezza, protezione ed integrità dei dati anche a livello computazionale, ovvero quando gli stessi vengono trattati dalle applicazioni. Nella sessione verranno presentate le soluzioni tecnologiche ad oggi disponibili, gli scenari di adozione e di sviluppo.

Relatori: Domenico Stranieri, Giuseppe Di Pasquale

18:00-19:30 – SALA AFRICA – SESSIONE PLENARIA - Women For Security 2021

"Mentoring e Cyber Security: utopia o possibilità nascosta?"

Ulisse prima di partire per Troia, chiese a Mentore (amico fidato e consigliere) di prendersi cura di suo figlio Telemaco e di prepararlo a succedergli al trono. Nel corso del poema, la Dea Atena assume la forma di Mentore per guidare, proteggere e istruire Telemaco durante i suoi viaggi. In questo ruolo, Mentore (ed Atena) ha la funzione di insegnante, di guardiano e di protettore, infondendo saggezza e fornendo consigli.
Attraverso questo passaggio, si può già intuire una delle funzioni del mentoring applicato, quella della gestione dei passaggi generazionali. Nel Medioevo, percorsi di mentoring tipici di role modeling si possono trovare nelle professioni dei mercanti, artigiani e degli avvocati, che per tramandare i segreti della professione affiancavano giovani apprendisti a maestri, considerati eccellenti nelle loro arti.
Nella Cyber Security il "role modeling" potrebbe assumere importanza fondamentale per lo sviluppo di nuove competenze e professionalità, ma in Italia è spesso confuso con la formazione tout court.

Nel corso della tavola rotonda analizzeremo la differenza tra formazione/coaching e mentoring, a partire dalle esperienze dirette dei nostri ospiti.

Introduzione di Gabriele Faggioli, Presidente Clusit

Modera: Cinzia Ercolano

Partecipano: Cristina Magro, Sonia Montegiove, Alessio Pennasilico, Anna Vaccarelli, Cristina Gaia, Lisa Ventura

2. Programma di mercoledì 10 novembre

09:00-10:00 – SALA AFRICA - SESSIONE SULLA GESTIONE DELLA SICUREZZA

"Passare dall'era dell'EDR a quella dell'Enterprise Detection and Response"

Come la condivisione delle informazioni aiuta la Security Operations a difendersi dalle più recente tecniche di attacco secondo il panorama delle minacce

Relatori: Luca Bechelli, Luca Nilo Livrieri

09:00-09:40 – SALA EUROPA - ATELIER TECNOLOGICO

"Cyber AI autonoma: ridefinire la sicurezza aziendale"

In questa nuova era di minacce informatiche, caratterizzata da attacchi lenti e furtivi e campagne rapide e automatizzate, gli strumenti di sicurezza statici e in silos stanno fallendo. Le organizzazioni devono ripensare con urgenza la propria strategia, per garantire la protezione delle persone e dei dati critici, ovunque si trovino. Alimentate dalla Cyber AI, le difese "self-learning" di oggi sono in grado di identificare e neutralizzare gli incidenti di sicurezza in soli pochi secondi.
In questa sessione, scopri come l'AI "self-learning":
- Rileva, indaga e risponde alle minacce
- Protegge l'intera forza lavoro e l'ambiente digitale, ovunque si trovino, qualunque siano i dati
- Difende da zero-day e altri attacchi avanzati, senza interrompere l'attività aziendale

Relatori: Luca Ciucciomini, Leonardo Ruvituso

10:00-10:40 – SALA EUROPA – ATELIER TECNOLOGICO

"Attacchi sistematici alle identità digitali: cosa insegna il caso NOBELIUM"

La protezione delle identità deve essere considerata un cardine imprescindibile nella strategia di protezione dei servizi IT. Come dimostra la nuova vasta e perdurante campagna di attacco condotta da NOBELIUM e segnalata da Microsoft lo scorso 24 ottobre, la protezione delle identità assume una rilevanza ancor più drammaticamente critica laddove ci sono aziende che operano come fornitori di servizi IT su infrastrutture cloud ed on-premises di diversi clienti finali. In questa sessione vedremo quali funzionalità mette a disposizione Microsoft per proteggere le identità, identificare e rispondere agli attacchi con il fine di ridurre i rischi legati alla compromissione delle stesse.

Relatori: Stefano Pescosolido, Donato Salamina

10:20-11:20 - SALA AFRICA - SESSIONE GESTIONE SICUREZZA

"Sicurezza per le rete di accesso: dall´OnPrem al Cloud"

Stiamo vivendo una delle più grandi trasformazioni digitali di tutti i tempi, che cambierà il modo in cui affrontiamo i problemi IT che ci affliggono di più, in un modo completamente nuovo. Non possiamo più affrontarli come prima: da un unico centro di controllo statico, senza flessibilità né resilienza.Abbiamo bisogno di sfruttare la logica dell'automazione e dell'intelligenza artificiale, in modo che i problemi vengano rilevati prima che creino impatti negativi sulla nostra esperienza digitale, il tutto garantendo un ambiente sicuro. Nel corso della sessione annalizzeremolo stato e dei benefici delle architetture di rete Zero Trust e SASE, approfondendo inoltreil livello di consapevolezza e dell'adozione da parte del mercato.

Relatori: Luca Bechelli, Alessandro Ercoli, Stefano Terfani

11:00-11:40 – SALA EUROPA – ATELIER TECNOLOGICO

"Check Point is Cloud Security – Best Practice per la Cloud Network Security"

La Cloud Security è ormai diventata business-critical: analizzare gli aspetti fondamentali per la messa in sicurezza della rete cloud non è più procrastinabile. Come si evince anche dal Check Point Security Report 2021 il 75% delle organizzazioni si definisce "estremamente preoccupato" per la sicurezza in cloud. Quali sono quindi le funzionalità che le soluzioni di sicurezza in Cloud dovrebbero avere? E come è possibile essere sicuri che i Cloud-Vendor abbiano le capacità necessarie per il successo e la sicurezza di una organizzazione? Scopri come implementare security gateway in cloud per fornire prevenzione avanzata dalle minacce, ispezione del traffico e micro-segmentazione e scopri come semplificare le operazioni di sicurezza, riducendo al minimo il numero di soluzioni di sicurezza singole grazie ad una integrazione funzionale con i Cloud Provider.

Relatore: Giorgio Brembati

11:40-12:40 – SALA AFRICA - SESSIONE GESTIONE SICUREZZA

"Intelligenza Artificiale in azione: come si evolve la Sicurezza informatica e l'IT Operation"

L’intelligenza Artificiale è ormai da tempo entrata nel mondo dell'IT, come strumento necessario ad analizzare enormi quantità di dati e per accelerare i tempi di elaborazione, apprendimento e pianificazione all’interno dei processi di business; chiunque usufruisce di servizi digitali fornisce dati e informazioni che vengono elaborate a fini statistici o per ottimizzare ricerche di mercato e cicli di vendita.
Le statistiche dei FortiGuard Labs evidenziano che siamo coinvolti in una vera e propria guerra informatica, in cui l'intelligenza artificiale è uno strumento a disposizione: un'arma che può essere utilizzata sia per l'attacco che per la difesa e chi la utilizza nel modo migliore è destinato a vincere. L’obiettivo, quindi, deve essere cavalcare l'opportunità della evoluzione tecnologica che ancora una volta non può essere fermata, cercando però di minimizzare i rischi connessi e l'utilizzo inappropriato per scopi offensivi.
Il percorso di Fortinet all'interno della ricerca sull'intelligenza artificiale prevede sia lo sviluppo di soluzioni innovative sia l'arricchimento di soluzioni tradizionali che acquisiscono così una maggiore efficacia dal punto di vista della protezione dagli attacchi informatici. Inoltre Fortinet non trascura il contributo che può fornire l'intelligenza artificiale alle attività quotidiane di gestione delle reti complesse, soprattutto in termini di supporto ad individuare azioni correttive che riescono a prevenire problemi imminenti.

SOC e NOC hanno quindi a disposizione nuovi strumenti in una fase storica in cui uomo e macchina devono correre insieme per far fronte ad una ulteriore sfida della Trasformazione Digitale.

Relatori: Federico Sarao', Alessio Pennasilico

12:00-13:00 – SALA EUROPA – ATELIER TECNOLOGICO

"EIDAS 2.0"

Connettere l'Europa in modo sicuro e rispettoso dei diritti e delle libertà degli individui, passa necessariamente attraverso il tema dell'identità digitale. Con il nuovo regolamento EIDAS, oggetto di questa sessione, cambieranno diverse cose come il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), la Carta di Identità Elettronica (CIE) e i wallet per autenticarsi ed entrare nei servizi.

Introduce: Alessandro Vallega
Partecipano: Emiliano Anzellotti e Andrea Caccia

14:00-15:30 – SALA AFRICA – TAVOLA ROTONDA

"La Pubblica Amministrazione verso il "new normal": il ruolo chiave delle in-house"

Che cosa abbiamo imparato in questi due anni in cui abbiamo vissuto in maniera diversa?
È fondamentale ripartire in sicurezza, ma quali sono le sfide che dobbiamo affrontare? Quali ambiti occorre rafforzare e come reagire alla luce delle tante criticità emerse in questo ultimo periodo?
Durante la pandemia abbiamo assistito a un enorme esercizio di resilienza che ha consentito salti culturali e forti accelerazioni della digitalizzazione della PA che deve completare tale percorso in modo sempre più strutturato e consapevole: la strategia da perseguire è ora contenuta nell'attuazione dl PNRR.
Dall'altro lato sono cresciuti esponenzialmente a livello locale e internazionale gli attacchi informatici. Cosa è possibile fare per mitigare ulteriormente quelli che puntano soprattutto sulle debolezze umane? Quali strategie possiamo adottare per innalzare il livello di attenzione?
Inoltre, il quadro normativo sta cambiando. Dobbiamo tenerne conto per affrontare il ritorno al "new normal".
Le società in-house, con il loro approccio olistico, giocano un ruolo sempre più importante nella fase di ripartenza che stiamo vivendo, non solo in qualità di partner e fornitori di servizi informatici, ma soprattutto come supporto e affiancamento proattivo degli Enti della Pubblica Amministrazione.
Questi alcuni dei temi su cui si confronteranno durante la tavola rotonda le quattro in-house, CSI Piemonte, Liguria Digitale, Insiel e Aria.

Modera: Enzo Veiluva, CSI Piemonte, Direttivo Clusit

Intervengono:
Maurizio Pastore, Liguria Digitale
Andrea Angeletta, Aria
Diego Mezzina, Insiel
Pier Paolo gruero, CSI

14:00-15:00 – SALA EUROPA – SESSIONE LEGALE

"Cybersecurity, accountability e sanzioni dei Garanti europei (2018-2021): un viaggio tra gli errori più comuni"

Sono più di un migliaio le sanzioni, oggi, comminate dalle Autorità garanti di tutti i Paesi dell'Unione Europea. Tra queste, molte sono correlate alla cybersecurity e alle misure di sicurezza. In questo incontro discuteremo dei casi più significativi per comprendere quanto sia importante pensare alla cybersecurity anche in un'ottica normativa (e di verifica da parte delle autorità di controllo), e non solo tecnica e organizzativa.

Relatore: Giovanni Ziccardi

15:20-16:00 – SALA EUROPA – ATELIER TECNOLOGICO

"Sblockchain: sfide e soluzioni per il successo dei sistemi DLT oltre la FinTech"

Scopo di questo intervento è offrire una panoramica su limiti ed opportunità offerte dalle tecnologie a registro distribuito (DLT) in campi diversi dalla FinTech, grazie alle esperienze accumulate negli ultimi quattro anni presso l'Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) del Consiglio Nazionale delle Ricerche. L'ICAR svolge ricerca e sviluppo in Artificial Intelligence, Data Science, Cyber Physical Systems e High Performance Computing, anche grazie a numerose collaborazioni con le PA (AGID, MEF, Ministero della Salute), Grandi Imprese, Università e Centri di Ricerca, nazionali ed internazionali. Un team di ricercatori dell'ICAR è coinvolto nella progettazione e nello sviluppo di applicazioni decentralizzate in campi applicativi quali l'eHealth, la dematerializzazione documentale e l'eVoting, anche nel contesto di consulenze e supporto alle aziende interessate all'impiego di DLT. Nel presente intervento saranno illustrate alcune delle attività e dei risultati acquisiti dal team in tali settori, quali esempi alle aziende per comprendere se e come le DLT possano essere vantaggiosamente applicate al loro business.

Relatore: Giovanni Schmid

16:00-17:30 – SALA AFRICA – TAVOLA ROTONDA a cura della Clusit Community for Security

"Future Trends in Cybersecurity and Data Protection"

La trasformazione digitale galoppa. Gli incidenti di sicurezza informatica crescono esponenzialmente. Nuove leggi e regolamenti provano a farci reagire. La tecnologia migliora per i difensori ma purtroppo anche per gli attaccanti e crea nuove sfide di privacy.
Questa sessione vuole dare degli spunti di riflessione su quello che sarà il nostro mondo fra 10 o 15 anni senza avere la pretesa di rispondere a tutte le domande. Avremo il piacere di sentire l'opinione di Eline Chivot che è senior adviser sulla politica digitale al Partito Popolare Europeo (PPE) a Bruxelles (intervento in inglese) e di alcuni dei team leader e partecipanti della Clusit Community for Security che da tempo si confrontano su questo nei gruppi di lavoro della stessa (https://c4s.clusit.it)

Introduce e modera: Alessandro Vallega

Partecipano: Eline Chivot, Orlando Arena, Andrea Cabras, Bruno Filippelli, Cesare Gallotti, Marco Locatelli, Roberto Obialero, Silvio Sperzani, Chiara Gatti

16:30-17:30 – SALA EUROPA – SEMINARIO a cura di AUSED

"Il nuovo paradigma della sicurezza del dato information centric"

Modera: Stefano Lombardi

Intervengono: Ugo Morra, Giovanni Simoncelli e Alessio di Angelo

18:00-19:30 – SALA AFRICA – SESSIONE PLENARIA

"Premio Tesi Innovare la sicurezza delle informazioni" 16a edizione - Tesi del 2020

Clusit procederà alla presentazione e premiazione delle migliori tesi universitarie del 2020.
Il premio, oltre a incentivare gli studenti a confrontarsi con i temi della Sicurezza Informatica, ha lo scopo di promuovere una collaborazione tra aziende, Università e studenti: un punto di scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro.

Modera: Claudio Telmon, coordinatore del Premio Clusit.

Intervengono alcuni degli studenti premiati.

Partecipano anche i partner del Premio:
Roberta Battagli, Oracle
Fabio Guasconi, Bl4ckswan
Paolo Da Ros, Da Ros & Associati
Ferdinando Lamagna, BSI Group

3. Programma di giovedì 11 novembre

9:00-10:00 – SALA AFRICA – SEMINARIO ANORC

"La custodia dei dati nelle strategie di trasformazione digitale delle PA. I modelli da sviluppare e le competenze da possedere"

La valorizzazione e la tutela del patrimonio informativo e documentale pubblico sono tra gli obiettivi strategici per affrontare efficacemente le nuove sfide poste dalla data economy, sostenendo la costruzione del mercato unico europeo per i dati e garantendo la creazione di servizi digitali per cittadini e imprese. I dati e i documenti informatici rappresentano il fulcro della trasformazione digitale. E in mancanza di modelli adeguati al loro trattamento, non sarà possibile assicurare una maggiore efficacia all'attività amministrativa in tutti i processi che riguardano sia lo scambio, che il riuso, per finalità commerciali e non, secondo il paradigma degli open data. In tale contesto, è indispensabile affidarsi a figure professionali specializzate nell'ambito della data governance che siano in grado di gestire e sfruttare appieno il potenziale dei dati. Per affrontare le nuove sfide poste dal Piano Nazionale di Ripresa e Resilienza (PNRR) occorre acquisire nuove skills per garantire un'alta qualità dei risultati in particolari settori emergenti quali l'ambiente, la privacy e la digitalizzazione.

Modera: Andrea Lisi, Presidente ANORC Professioni, Coordinatore di Digital & Law Department

Intervengono:
Franco Cardin, Consiglio Direttivo di ANORC e ANORC Professioni
Donato Antonio Limone, Professore ordinario di informatica giuridica, Presidente del Comitato tecnico-scientifico di ANORC Professioni
Michele Melchionda*, Responsabile della transizione al digitale della Presidenza del Consiglio dei Ministri, Consiglio Direttivo di ANORC Professioni

(*Relatore invitato e in attesa di conferma)

9:00-10:00 – SALA EUROPA – SESSIONE LEGALE

"Tecnologie avanzate, tracciamento dei clienti, mobile, trattamento dati e sicurezza"

Relatrice: Anna Cataleta

10:20–11:20 – SALA AFRICA – ATELIER TECNOLOGICO

"Quando ad Internet si collegano Macchinari, Impianti, Oggetti"

In questo Atelier illustreremo alcune criticità e relative contromisure in contesti ove sia necessario gestire informazioni e dati provenienti da oggetti, macchine, impianti.
Partendo dall'utilizzo di OT/IoT/IIoT nella vita di tutti i giorni, in fabbrica e nelle smart cities degli anni a venire: semafori intelligenti che rilevano le persone senza dover premere il pulsante per farli diventare verdi o quando arrivano le connected cars, irrigazione del verde che si interrompe quando passa qualcuno, di come da qui a 5/10 anni il 5G consentirà la creazione di reti di servizio cittadine e di come le persone coi cellulari 5G verranno integrate sia nella mobilità sia negli altri servizi in modo sempre più semplice e trasparente, menzionando alcuni problemi di security e privacy insiti in queste applicazioni. Per quanto riguarda gli impatti di OT/IoT/IIoT per Industria4.0, parleremo del concetto di Digital Twin o Gemello Digitale, ovvero la possibilità di utilizzare la simulazione generando un “oggetto/impianto virtuale” in Cloud che sia una copia di un “oggetto del mondo reale” ai fini di migliorare performance dell’impianto, controllare il comportamento nell’uso, prevedere la manutenzione nel tempo, migliorare la qualità del prodotto e delle prestazioni dell’oggetto/impianto stesso, con tutti i risvolti relativi alla protezione delle informazioni e delle connessioni in Cloud.

Intervengono:
Enzo M Tieghi, Amm.Del. ServiTecno, membro del Comitato Scientifico di CLUSIT
Lorenzo Ivaldi, professore al DITEN Università di Genova, membro del Comitato Scientifico di CLUSIT
Franco Callegati, professore al Dipartimento Informatica: Scienza e Ingegneria (DIS), Alma Mater Studiorum - Università Bologna

10:20-11:00 – SALA EUROPA – ATELIER TECNOLOGICO

"Hybrid Work: Gestione proattiva del rischio in un ambiente di lavoro moderno"

Nell'attuale scenario post-pandemico in cui il lavoro ibrido, l'iperconnettività, le modalità innovative di lavorare si stanno consolidando, gli scenari di rischio ICT & Cyber stanno evolvendo, creando una maggiore superfice di attacco e nuove modalità di materializzazione di eventi malevoli. Una gestione responsabile del rischio prevede la formazione del personale, l'utilizzo di processi di lavoro ibrido e di tecnologie evolute, robuste ed integrate. Il punto di partenza per la resilienza aziendale è un maggiore controllo degli asset aziendali coadiuvato da una gestione end to end della sicurezza informatica.
La sessione quindi affronterà temi legati all'analisi e gestione del rischio, tramite diversi strumenti cloud-based forniti da Microsoft, quali Microsoft Endpoint Manager e Windows 365, che permettono la gestione sicura degli asset aziendali e forniscono soluzioni alternative ai classici pc, adattandosi alle diverse esigenze dei nostri clienti. Tramite scenari pratici, vedremo come elementi di controllo

innovativi potranno migliorare la collaborazione delle risorse, ottimizzare l'effort nella gestione del rischio e permettere una visione strategica attraverso decisioni informate.

Relatori: Maura Perra, Francesco Manca

11:20-12:00 – SALA EUROPA - ATELIER TECNOLOGICO

"Acronis e FC Internazionale Milano: l'importanza dei dati e della loro protezione"

La Cyber Protection ha un' importanza strategica nella gestione dei dati in sicurezza imprescindibile soprattutto a seguito della trasformazione digitale avvenuta negli ultimi tempi. Tutte le aziende necessitano di una protezione completa ed integrata in grado di proteggere i dati sensibili. Nel corso della sessione analizzeremo alcuni casi concreti a partire dall'esperienza del Club FC Internazionale Milano .

Relatori: Stefano Bucci, Lorenzo Antognoli

11:40-12:40 – SALA AFRICA – SEMINARIO a cura di UNINFO

"Aggiornamenti dal mondo della normazione: famiglia ISO/IEC 27001, regolamento eIDAS, ISO/IEC 15408 e schemi sulla protezione dei dati personali"

Prosegue la vivace stagione del mondo della normazione. L'imminente uscita della ISO/IEC 27002 porterà una serie di cambiamenti in tutta la famiglia delle norme, il regolamento eIDAS e la ISO/IEC 15408 sono anch'essi oggetto di significative revisioni mentre progrediscono le nuove iniziative in ambito CEN e ISO/IEC sulla protezione dei dati personali.

Intervengono: Cesare Gallotti, Dorotea De Marco, Andrea Caccia, Stefano Ramacciotti, Fabio Guasconi

12:20 -13:00 - SALA EUROPA - ATELIER TECNOLOGICO

"Five Ways to strengthen active directory security and prevent ransomware attacks"

Attackers start by leveraging vulnerabilities, social engineering, misconfigurations and other flaws. Once ransomware actors gain access to your network, they will almost always systematically exploit Active Directory to achieve mass deployment. Led by Tenable Active Directory security expert, this session will share insights and proven solutions for strengthening Active Directory to prevent ransomware exploitation.

Key takeaways:
- Five issues plaguing every Active Directory environment and five corresponding actions for dramatically improve your AD security
- Preventing privilege escalation by avoiding AD and group policy misconfigurations
- Proven actions you can take to close backdoors

Relatore: Aitor Alvarez (intervento in inglese)

14:00-15:00 – SALA AFRICA – SEMINARIO a cura di IISFA

"OSINT: dalla ricerca all'acquisizione forense delle digital evidence"

Coordina: Gerardo Costabile, Presidente IISFA

Intervengono: Dario Beniamini e Paolo dal Checco, consulenti informatici forensi

14:00-15:00 – SALA EUROPA – SEMINARIO a cura di OWASP ITALY

Sono previsti due interventi.

"TLSAssistant: uno strumento per identificare e mitigare le vulnerabilità di TLS"

Gli ultimi anni hanno visto una crescita esponenziale dell'utilizzo di TLS (Transport Layer Security) per la messa in sicurezza di servizi ed applicazioni on-line. Nonostante questa popolarità, molti amministratori di sistema non riescono a gestire correttamente i problemi di sicurezza che derivano da configurazioni errate (ad esempio, l'utilizzo di cifrari deboli). Per questo motivo, sono stati sviluppati molti strumenti automatici per l'identificazione di vulnerabilità nelle implementazioni di TLS. Nonostante la semplicità di utilizzo, tali strumenti non assistono gli amministratori nel difficile compito di applicare le adeguate misure per mitigare i problemi riscontrati. Di conseguenza, agli amministratori viene richiesto di investire una grande quantità di tempo, che di solito non hanno a disposizione, per trovare, comprendere e tradurre in azioni concrete che portano alle opportune modifiche della configurazione di TLS. Per ovviare a questi problemi, l'unità Security & Trust di FBK ha sviluppato TLSAssistant, uno strumento capace di individuare non solo i potenziali problemi di sicurezza in una configurazione di TLS ma anche di generare un rapporto in grado di guidare amministratori di sistema e sviluppatori Android verso una risoluzione rapida ed efficace dei problemi rilevati.
Relatore: Salvatore Manfredi

"Un’introduzione alla sicurezza dell’AI"

L’utilizzo di algoritmi di Machine Learning (ML) in diversi ambiti applicativi come la guida autonoma e malware detection è divenuto estremamente popolare nell’ultimo decennio. Tuttavia, l’adozione di ML in applicazioni security-critical deve essere valutata con attenzione. Infatti nell’ultimo decennio la letteratura accademica ha visto l’aumento esponenziale del numero di pubblicazioni riguardanti la sicurezza di algoritmi di apprendimento supervisionato e delle loro applicazioni ai task di classificazione. Gli attacchi proposti vengono dimostrati efficaci anche contro classificatori effettivamente utilizzati dalle aziende e spesso offerti da piattaforme di Machine Learning as a Service (MLaaS) come Google Cloud Vision e Clarify.com. È necessario quindi che anche i professionisti siano a conoscenza delle possibili vulnerabilità della ML pipeline. Nel corso di questo breve seminario verranno introdotti alcuni attacchi e vulnerabilità di algoritmi di classificazione basati su ML che possono influenzare gravemente le performance dei classificatori stessi o portare a rivelare informazioni sensibili, al fine di introdurre i professionisti ad alcune delle possibili minacce a cui possono incorrere nell’adozione dell’AI in produzione.
Relatore: Lorenzo Cazzaro

16:00-18:00 – SALA AFRICA – SESSIONE PLENARIA

"Difesa del Sistema Paese: le sfide e l'importanza dell'Intelligence oggi"

I Servizi segreti di ogni paese si trovano oggi ad affrontare una complessa situazione mondiale che sta mutando in maniera sempre più rapida e quindi difficilmente prevedibile. Per analizzare al meglio ogni singola dinamica globale è importante capire prima di tutto cosa sono realmente i Servizi segreti, come operano e come l’Intelligence potrà o meno indagare a fondo questo mondo così

complesso, appeso tra minaccia cibernetica e nuove minacce emergenti in ambito di Terrorismo internazionale.

Modera: Gabriele Faggioli, presidente Clusit

Partecipano:
Angelo Tofalo, Parlamentare, autore del libro "Intelligence Collettiva. Appunti di un Ingegnere rapito dai Servizi Segreti"
Umberto Saccone, Presidente IFI Advisory
Marco Santarelli, Direttore scientifico Fondazione Margherita Hack
Stefano Quintarelli, Co-fondatore e membro del direttivo Clusit
Corrado Giustozzi, Senior partner Rexilience, nel direttivo Clusit

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Sede legale presso l'Università degli Studi di Milano
Dipartimento di Informatica "Giovanni Degli Antoni"
Via Celoria 18, 20133 Milano
Sede amministrativa: Via Copernico 38, 20125 Milano - cell. 347.2319285
* associazione senza fini di lucro, costituita il 4 luglio 2000