Rassegna stampa

16/12/2019

Cyber 4.0: presentazione del Competence Center per la cyber security

SAPIENZA
UNIVERSITÀ DI ROMA

a cura del settore Ufficio stampa e comunicazione

CORRIERE DELLA SERA

17-DIC-2019
da pag. 41
foglio 1

Dir. Resp.: Luciano Fontana

www.datastampa.it Tiratura: 293393 - Diffusione: 268950 - Lettori: 2044000: da enti certificatori o autocertificati Superficie: 2 %

Sussurri & Grida

Cibersecurity, al il via polo interuniversitario

Presentato ieri il Competence center per la Cyber Security e contro i crimini informatici nell'aula magna della Sapienza di Roma, alla presenza del Rettore, Eugenio Gaudio e della vicepresidente della Luiss, Paola Severino. «I crimini informatici nel 2017 hanno prodotto alle imprese danni per 4 miliardi di dollari, colpendo più di 300 mila utenti in 150 Paesi», ha ricordato Severino.

Il Messaggero
Dir. Resp.: Virman Cusenza
www.datastampa.it Tiratura: 113876 - Diffusione: 89490 - Lettori: 998000: da enti certificatori o autocertificati
17-DIC-2019
da pag. 18
foglio 1
Superficie: 7 %

Università, enti e imprese insieme per la cybersecurity

INDUSTRIA 4.0

ROMA È stato presentato ieri presso l'Università La Sapienza il nuovo "Competence Center per la cybersecurity", uno degli otto poli di competenza ad alta specializzazione su tematiche Industria 4.0 previsti dal ministero dello Sviluppo che aggrega università, tra cui la Luiss Guido Carli, oltre a istituzioni, centri di ricerca e imprese. Contrastare la criminalità informatica e fare ricerca sulla cybersicurezza, elaborando strategie efficaci a sostegno di imprese del territorio saranno le principali mission del nuovo polo, che mira anche ad avviare un percorso di orientamento e formazione sul tema, affrontato in tre specifiche declinazioni tematiche: e-health, automotive e spazio. Il nuovo Competence Center è nato dalla collaborazione di un partenariato pubblico e privato al quale hanno aderito, oltre alla Luiss e alla Sapienza, Tor Vergata, Roma Tre, l'Università della Tuscia, l'Università di Cassino, l'Università dell'Aquila. Tra i centri di ricerca: il CNR e l'INAIL. Per finire, una rete di 37 imprese tra piccole e grandi, con l'obiettivo di incrementare la sicurezza informatica e sostenere le imprese nella formazione di competenze in ambito Industria 4.0. Paola Severino, vicepresidente della Luiss ha spiegato che i crimini informatici «hanno prodotto danni al sistema imprese per un ammontare, nel solo 2017, di 4 miliardi, colpendo più di 300.000 utenti in oltre 150 Paesi».

16/12/2019 RAI 1
TG1 - 13:30 - Durata: 00.01.29

Conduttore: FRITTELLA MARCO - Servizio di: D'AQUINO ANDREANA - Da: anddel
Tecnologia. Nasce nuovo polo cybersecurity tra 7 università del Lazio tra cui la Luiss.
Int. Teodoro Valente (Univ. La Sapienza); Paola Severino (Luiss); Eugenio Gaudio (Rettore Univ. La Sapienza)

Link: http://www.askanews.it/economia/2019/12/16/cyber-security-manzella-avvio-competence-center-ottima-notizia-pn_20191216_00181/

CYBER SECURITY Lunedì 16 dicembre 2019 - 16:22

Cyber security, Manzella: avvio Competence center ottima notizia

Segna un altro passo avanti di Industria 4.0

Roma, 16 dic. (askanews) – "L'avvio del Competence Center dedicato alla Cyber-security è ottima notizia. Segna un altro passo avanti di Industria 4.0, 'il' programma italiano di politica industriale che con questa manovra abbiamo rafforzato e ampliato. Vogliamo che accedano ai finanziamenti il 40% di imprese in più: a partire da quelle piccole e medie imprese e quelle di un settore agricolo sempre più all'avanguardia tecnologica". Lo ha detto il sottosegretario al Mise, Gian Paolo Manzella, in occasione dell'evento di presentazione del Competence center per la Cyber Security che si è svolto oggi nell'Aula Magna dell'Università di Roma "La Sapienza".

"In questa strada agli 8 Competence Center attualmente esistenti a livello nazionale – ha aggiunto – è affidato il compito di diffondere la cultura 4.0 e sciogliere un nodo italiano, il rapporto tra ricerca, università e mondo delle imprese. Si gioca qui una delle grandi sfide del nostro futuro e per questo dobbiamo rendere questi organismi sempre più forti. Dal Mise sempre la massima

collaborazione a università, centri di ricerca e imprese affinché i 72 milioni stanziati per gli 8 centri siano utilizzati nel migliore dei modi e moltiplichino il ritorno per imprese e territori. Buon Lavoro".

16 dicembre 2019

Università La Sapienza
LUISS
Guido Carli
Fabio Cocurullo
Teodoro Valente

Salva
Commenta

LOTTA ALLA CRIMINALITÀ INFORMATICA

Industria 4.0: a Roma il nuovo Competence center per la cyber security

Si tratta di uno degli otto poli di competenza ad alta specializzazione su tematiche Industria 4.0, previsti dal ministero dello Sviluppo economico, che aggrega università, tra cui la Luiss Guido Carli, oltre a istituzioni, centri di ricerca e imprese

Cyber security, un asset fondamentale per la sicurezza nazionale

2' di lettura

Presentato all'Università La Sapienza il nuovo "Competence Center per la cyber security", uno degli otto poli di competenza ad alta specializzazione su tematiche Industria 4.0, previsti dal ministero dello Sviluppo economico, che aggrega università, tra cui la Luiss Guido Carli, oltre a istituzioni, centri di ricerca e imprese. Le principali missioni del nuovo polo, che mira anche ad avviare un percorso di orientamento, formazione e innovazione sul tema della cyber security, saranno il contrasto della criminalità informatica e la ricerca sulla cybersicurezza, elaborando strategie efficaci a sostegno di imprese del territorio.

Il nuovo Competence Center è nato dalla collaborazione di un partenariato pubblico e privato al quale hanno aderito, tra gli atenei: la **Luiss Guido Carli**, **La Sapienza**, **Tor Vergata**, **Roma Tre**, **l'Università della Tuscia**, **l'Università di Cassino**, **l'Università dell'Aquila**; tra i centri di ricerca: il **Cnr e l'Inail**; e una rete di 37 imprese tra piccole e grandi, con l'obiettivo di incrementare la sicurezza informatica, sostenere le imprese nella formazione di competenze in ambito Industria 4.0 e avviare progetti di innovazione, ricerca industriale e sviluppo sperimentale.

Prencipe: sfida da affrontare con dompetenze diverse

«Co-generare conoscenza in materia di cyber-security è una sfida da affrontare coinvolgendo attori con competenze diversificate: università, imprese e istituzioni vogliono collaborare insieme nel nuovo Competence Center per sviluppare un metodo efficace di contrasto alla criminalità informatica» ha spiegato il Rettore della Luiss Guido Carli **Andrea Prencipe**.

Severino: «Fare sistema per combattere i crimini informatici»

«La ricerca universitaria deve essere coerente con gli scopi promossi dalla Pubblica amministrazione e va proiettata verso le

aziende: la Luiss, la Sapienza e gli altri Atenei che partecipano al progetto Industria 4.0 vogliono "fare sistema" per analizzare i fenomeni di attacco alla sicurezza informatica e per combatterli efficacemente, in primis con la prevenzione» ha dichiarato la vicepresidente Luiss **Paola Severino**. «I crimini informatici - ha aggiunto - hanno prodotto danni al sistema delle imprese per un ammontare, nel solo 2017, di circa 4 bilioni di dollari, colpendo più di 300.000 utenti in oltre 150 Paesi». Le università, ha poi concluso, «possono dare il loro contributo anche formando i giovani a progetti multidisciplinari che li immetteranno nel mondo del lavoro con una specializzazione nella lotta alle aggressioni informatiche, particolarmente richiesta dalle imprese».

Il polo di competenza è stato presentato alla presenza di Gianpaolo Manzella, sottosegretario del ministero dello Sviluppo economico. Come relatori sono intervenuti, tra gli altri: Eugenio Gaudio Rettore Università La Sapienza, Teodoro Valente, Prorettore alla Ricerca La Sapienza e presidente Cybersecurity Competence Center, Alessandro Longo Agendadigitale.eu, e Fabio Cocurullo vicepresidente Cybersecurity Competence Center.

Per approfondire:

- "Security By Design": dalla direttiva europea al Cybersecurity act
- Il lavoro digitale più richiesto? Per Linkedin è l'esperto di protezione dati

Università La Sapienza LUISS Guido Carli Fabio Cocurullo Teodoro Valente

PER SAPERNE DI PIÙ

loading...

Brand connect

Loading...

Loading...

CYBER SECURITY: AL VIA IL COMPETENCE CENTER, PASSO AVANTI INDUSTRIA 4.0

Manzella (Mise): Realta' da potenziare, una sfida del futuro (Il Sole 24 Ore Radiocor Plus) - Roma, 16 dic - 'L'avvio del Competence Center dedicato alla Cyber security e' ottima notizia. Segna un altro passo avanti di Industria 4.0, 'il' programma italiano di politica industriale che con questa manovra abbiamo rafforzato e ampliato". Lo ha detto il sottosegretario allo Sviluppo Economico, Gian Paolo Manzella, in occasione dell'evento di presentazione del Competence center per la Cyber Security che si e' svolto oggi nell'Aula Magna dell'Universita' di Roma 'La Sapienza', alla presenza del Rettore, Eugenio Gaudio e della Vicepresidente dell'Universita' Luiss, Paola Severino. "Vogliamo che accedano ai finanziamenti - ha proseguito - il 40% di imprese in piu': a partire da quelle piccole e medie imprese e quelle di un settore agricolo sempre piu' all'avanguardia tecnologica. In questa strada agli 8 Competence Center attualmente esistenti a livello nazionale e' affidato il compito di diffondere la cultura 4.0 e sciogliere un nodo italiano, il rapporto tra ricerca, universita' e mondo delle imprese. Si gioca qui una delle grandi sfide del nostro futuro e per questo dobbiamo rendere questi organismi sempre piu' forti. Dal Mise sempre la massima collaborazione a universita', centri di ricerca e imprese affinche' i 72 milioni stanziati per gli 8 centri siano utilizzati nel migliore dei modi e moltiplichino il ritorno per imprese e territori'.

com-amm

(RADIOCOR) 16-12-19 16:09:55 (0478) 5 NNNN

TAG

ITALIA | EUROPA | ECONOMIA | ITA

EUROPEAN CYBER SECURITY CHALLENGE: ITALIA SECONDA IN CLASSIFICA

(di Giorgio Giacinto) 16/12/19 - Intervista a Emilio Coppa, Giovanni Lagorio e Mario Polino allenatori della squadra italiana di cyber defender "TEAM ITALY" formata da allievi del percorso formativo Cyberchallenge.IT (link).

Emilio Coppa è un assegnista di ricerca presso il Dipartimento di Ingegneria informatica, automatica e gestionale della Sapienza Università di Roma. Ha ricevuto un dottorato in Informatica nel 2015 e i suoi interessi di ricerca si focalizzano su tecniche di analisi statica e dinamica del software. Dal 2017 fa parte del comitato organizzativo di CyberChallenge.IT ed è uno dei responsabili della squadra nazionale per l'European Cyber Security Challenge (ECSC).

Giovanni Lagorio è ricercatore presso il DIBRIS dell'Università di Genova. Interessato alla sicurezza informatica e ad attività di ethical hacking, è fra i fondatori del team ZenHack e organizzatore di CyberChallenge.IT per la sede di Genova. Dal 2019 è uno dei responsabili della squadra nazionale di cyber-defender per l'European Cyber Security Challenge (ECSC).

Mario Polino è assegnista di ricerca presso il DEIB del Politecnico di Milano dove si occupa di Malware e Binary Analysis. Dal 2009 partecipa a competizione CTF con il team Tower of Hanoi e dal 2018 con mhackeroni. Dal 2019 è l'allenatore del team nazionale di cyber-defender per l'European Cyber Security Challenge (ECSC)

Prima di tutto una breve panoramica sui componenti della squadra. Quali sono le città di provenienza? Quali i corsi di studio di provenienza?

Ricordiamo ai lettori che i componenti della squadra vengono dal percorso di formazione CyberChallenge.IT, organizzato dal Laboratorio Nazionale Cybersecurity del CINI, che ha visto inizialmente 20 ragazzi formarsi in ciascuna delle 18 sedi universitarie partecipanti. Terminato il periodo di formazione, ciascuna sede ha selezionato quattro ragazzi per formare la squadra locale che ha partecipato alla finale nazionale a Chiavari, lo scorso 27 Giugno.
Grazie alla finale nazionale è stato possibile formare il team nazionale.
Il team è composto da dieci ragazzi che provengono da diverse realtà italiane.

Andrea Biondo (il capitano) e Riccardo Bonafede sono due studenti dell'Università degli studi di Padova. Il primo vive a Cassier (Treviso) ed è attualmente iscritto alla Magistrale in Informatica, mentre il secondo viene da Padova e sta completando la Triennale in Ingegneria Informatica. Sempre dal Veneto arriva Antonio Groza, che vive a Mirano (Venezia) e dopo essersi diplomato nel 2018 all'ITIS Levi Ponti ha deciso di intraprendere direttamente una carriera professionale.

Marco Bonelli, Andrea Laisa e Samuele Turci studiano a Milano. Marco viene da Terni e frequenta la triennale in Ingegneria Informatica presso il Politecnico di Milano. Andrea invece viene da Bergamo, studia sempre al Politecnico di Milano ma è iscritto alla triennale in Informatica. Infine, Samuele viene da Gatteo (Forlì-Cesena) ed è iscritto alla triennale in Informatica presso l'Università degli Studi di Milano.

A Roma studiano tre partecipanti del team: Qian Matteo Chen, Dario Petrillo e Michele Lizzit. Matteo vive a Roma ed è uno studente triennale di Informatica presso l'Università La Sapienza di Roma. Anche Dario vive a Roma e studia alla Sapienza, ma frequenta la triennale di Ingegneria Informatica. Infine, Michele vive a Pasian di Prato (Udine) e frequenta la Triennale in Management and Computer Science presso la Libera Università Internazionale degli Studi Sociali (LUISS) Guido Carli.

Scendendo geograficamente ancora più a sud, Davide Palma studia alla triennale di Informatica dell'Università degli studi di Bari e vive a Apricena (Foggia).

Con quale criterio sono stati selezionati i componenti della squadra nazionale a partire dai partecipanti alla finale?

Il pool di scelta era composto dai partecipanti di CyberChallenge.IT del 2019, ma anche degli anni precedenti. L'iniziativa è stata molto efficace e ha introdotto a questo tipo di competizioni molti giovani capaci, che nel tempo sono migliorati tanto fino ad arrivare a competere ai massimi livelli nonostante la loro giovane età. Scegliere non è stato facile, ci sono molti ragazzi in gamba, ma alcuni vincoli sulla composizione della squadra presenti nel regolamento della competizione hanno semplificato questa scelta.
Tutti e 10 i giocatori devono avere meno di 25 anni, e 5 di loro devono essere sotto i 20 anni. Ci sono tantissimi ragazzi bravi con meno di 25 anni. Meno, invece, per quanto riguarda la fascia fino ai 20. Questo regolamento divide fondamentalmente la squadra in due quote: Senior (21-25) e Junior (minori di 20 anni). Abbiamo quindi realizzato due classifiche, una per i Senior e una per i Junior, in cui abbiamo valutato le prestazioni dei candidati negli eventi passati. In particolare, abbiamo valutato la prova locale, cioè la sfida individuale che ogni partecipante di CyberChallenge.IT ha affrontato alla fine del percorso di formazione, la competizione nazionale, che si svolge a squadre fra le varie sedi, ma anche competizioni esterne a cui diversi membri del team finali hanno preso parte. Il risultato è stato un team formidabile e il posizionamento al secondo posto ne è la conferma.

EVENTI

Clicca sui giorni evidenziati in rosso e scopri cosa c'è in evidenza.

A questo punto passiamo alla fase di allenamento e di costruzione del vero e proprio "gioco di squadra". Come avete gestito la diversa provenienza geografica e di formazione di base?

L'allenatore ha selezionato i partecipanti scegliendo, di proposito, una formazione eterogenea, essenziale per essere pronti ad affrontare ogni tipo di sfida. La diversa provenienza geografica, invece, è stata mitigata organizzando, a metà settembre, un ritiro di quattro giorni presso la Scuola IMT Alti Studi di Lucca.

Lì i ragazzi hanno avuto modo di conoscersi, formando una squadra vera e propria, grazie a varie attività di gruppo. Fra queste, anche attività non strettamente legate all'informatica, ma non meno importanti, quali, per esempio, ripresa e montaggio del video, goliardico, di presentazione della squadra e birrate serali.

Potete raccontarci come si è organizzata la squadra in termini di divisione dei compiti? È stato nominato un capo o è emerso un leader spontaneo? Sicuramente questo aspetto è strettamente legato al tipo di competizione. Potete darci una breve descrizione della modalità di gioco?

Grazie al raduno di Lucca, il team è stato in grado di identificare le competenze che ogni membro del team poteva mettere a disposizione ai fini della competizione.

Come capitano della squadra, abbiamo immediatamente visto in Andrea Biondo il migliore candidato: parte del team che ha vinto CyberChallenge.IT 2018, membro dei team CTF Spritzers e mHACKeroni, membro della nazionale per ECSC nel 2018 e anche co-autore di articoli scientifici in conferenze di rilievo nell'ambito della cybersecurity.

La competizione si è svolta in due giornate seguendo un format jeopardy, in cui i team devono risolvere delle challenge per ottenere dei punti. Ogni challenge può essere vista come una sfida informatica, sia software che hardware, che replica uno scenario reale ma in un contesto isolato, permettendo ai ragazzi di divertirsi senza fare danni nel mondo reale. Esempi concreti di queste sfide possono essere dei portali web in cui occorre ottenere accesso amministrativo oppure dei sistemi embedded su cui identificare delle falle per far eseguire azioni non autorizzate.

Le 36 challenge preparate dagli organizzatori rumeni sono state egualmente divise fra i due giorni di gara, non permettendo ai ragazzi di risolvere challenge del primo giorno durante la seconda giornata. Il punteggio di ogni challenge è stato ottenuto in modo dinamico: tale meccanismo evita di dover assegnare un punteggio a priori in base alla difficoltà stimata (sempre molto difficile da valutare).

Oltre alle challenge hardware e software, gli organizzatori hanno assegnato ulteriori punti in base alla capacità dei vari team di: (a) superare una escape room caratterizzata da sfide hardware entro un tempo massimo di 30 minuti, (b) presentare in 5 minuti la soluzione di una delle challenge risolte ad una giuria composta da non esperti.

Durante le ultime due ore di gara, la scoreboard con i punteggi è stata oscurata, in attesa della premiazione avvenuta la sera del giorno dopo.

E ora veniamo ai momenti di gara, divisa in tre giornate. Potete descriverci quali sono state le emozioni provate dalla squadra durante le giornate? L'Italia già dalla seconda parte della prima giornata faceva parte del gruppo di testa, conquistando anche il primo posto in diverse fasi della gara. Come sono stati vissuti questi momenti?

Quale è stato l'aspetto più difficile della gara? Quale quello che vi ha dato più soddisfazione?
All'inizio eravamo tutti molto emozionati ma, una volta che abbiamo iniziato ad affrontare le varie sfide, la concentrazione era tale da non farci pensare molto ad altro.
Alcune challenge hanno richiesto diverse ore e il lavoro congiunto di vari membri, un po' per difficoltà tecniche, un po' perché non era chiarissimo cosa si doveva fare e la comunicazione con gli organizzatori era a volte difficoltosa. Chiaramente, rimanere bloccati per ore su una sfida può essere estremamente frustrante ma, come si dice, chi la dura la vince, e alla fine siamo riusciti a risolverne molte. Far parte del gruppo di testa fin da subito ci ha creato un po' di tensione, ma ogni sfida risolta ci ha dato una grande carica e fiducia in noi stessi, che ci hanno aiutato a mantenere la grinta per tutte quelle ore.
Il team ha funzionato molto bene e questo aspetto ha dato i suoi frutti, portandoci in alto in classifica. È questo, probabilmente, l'aspetto che ci ha dato più soddisfazione.

Ora che la gara è terminata portando a casa il secondo posto, quali sono i riflessi di questa esperienza che avranno sicuramente un effetto nelle vostre attività future nel campo della didattica e della ricerca? Qualcuno dei ragazzi ha pensato di lanciarsi nel lavoro con una start-up? Quando pensano al loro futuro si vedono in Italia o all'estero?

Faremo sicuramente tesoro di questa esperienza; alcuni ragazzi hanno già esperienze lavorative e stanno considerando anche la possibilità di lanciarsi in qualche startup. Altri puntano invece ad attività di ricerca: c'è chi pensa a un dottorato e chi invece vorrebbe entrare a far parte del settore ricerca e sviluppo di qualche grossa industria. Fortunatamente per il nostro paese, quando pensano al futuro alcuni si vedono in Italia, anche se non manca chi considera la possibilità di andare a lavorare per qualche colosso informatico dall'altra parte dell'oceano.

Per quanto riguarda la squadra, continuerà a partecipare ad altre competizioni? Cosa intendete fare per condividere la vostra esperienza coi più giovani?

Sicuramente la squadra parteciperà anche il prossimo anno a ECSC, alcuni membri supereranno il limite di età e quindi il team dovrà per forza cambiare un po'. Ma queste sono valutazioni da fare a valle della prossima edizione di CyberChallenge.IT dove ci aspettiamo, come è successo in passato, che i membri attuali del team aiutino a formare le nuove leve.
Nel frattempo, subito dopo la competizione in Romania, una grossa fetta del team è volato ad Abu Dhabi per la Hack in The Box CyberWeek, dove hanno preso parte in due competizioni diverse:

- *Una parte di loro ha partecipato e vinto la "Cyber Battle of The Emirates" una competizione pensata per giovani che si affacciano al mondo dei Capture the Flag e della security più in generale.*
- *Un'altra parte ha invece preso parte al ProCTF come "mhackeroni". Il ProCTF è una competizione senza restrizioni di età, e pensata per professionisti. Il Team mhackeroni è arrivato al terzo posto.*

Molti dei giocatori del Team Italy, ma anche gli altri partecipanti di CyberChallenge.IT, dopo questa esperienza continuano a giocare nei team locali delle varie sedi universitarie. Queste squadre sono formate non solo da novizi, ma anche da giocatori di lunga data, che durante l'anno si sfidano in varie competizioni. Esiste una lista pubblica dei Team Italiani che hanno assorbito partecipanti di CyberChallenge.IT o che sono nati proprio dai ragazzi che hanno partecipato a questa iniziativa: https://cyberchallenge.it/ctf-teams.

Uno di questi team è il team "mahckeroni" (https://mhackeroni.it/) che oramai da diversi anni partecipa al DEF CON CTF, una delle competizioni più difficili di questa categoria. Per partecipare a questa competizione bisogna qualificarsi vincendo uno degli eventi selezionati. Non ci sono restrizioni di età, numero, o professione, e a questo tipo di competizioni prendono

parte anche molti professionisti del settore. E solo le migliori 16 squadre al mondo riesco a vincere un posto per la finale di Las Vegas. Diversi membri del "Team Italy" fanno parte della squadra "mhackeroni" che lo scorso Agosto si è piazzata al 5° posto di questa competizione.

Grazie per il vostro impegno, teneteci informati sulle vostre attività. Difesa Online e i suoi lettori vi sostengono. In bocca al lupo a tutti!

https://europeancybersecuritychallenge.eu/

Tweet 71

09/12/19 | Cyber

APT 32 HACKERA BMW E HYUNDAI?

È di qualche giorno fa la notizia che degli hackers avrebbero colpito BMW e Hyundai. Gli hackers si sarebbero...

638 LEGGI

02/12/19 | Cyber

LOCKHEED MARTIN: QUALCHE AGGIORNAMENTO SULLE ANALISI DEI RISCHI CYBER

(A volte ritornano...) Qualche mese fa ci siamo soffermati ad analizzare i rischi cyber relativi all'F-35, questo ha...

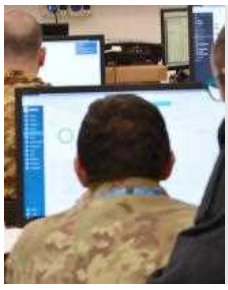
728 LEGGI

25/11/19 | Cyber

LA BRIGATA DEI "GUERRIERI OMBRA"

È di qualche giorno fa la notizia circa la costituzione del 127th Cyber Battalion della Army National Guard dello Stato...

1778 LEGGI



18/11/19 | Cyber

LO SVILUPPO DELLA CAPACITÀ CYBER DELL'ESERCITO

Il Centro Studi Esercito, Centro di Pensiero di riferimento della componente militare terrestre1, lancia il primo...

703 LEGGI

13/11/19 | Cyber

SICUREZZA 2019: AI E APT CON DIFESA ONLINE

Oggi alla fiera della SICUREZZA di Milano-Rho, ci vediamo alla "Cyber Arena" del Padiglione 5, l'area espositiva,...

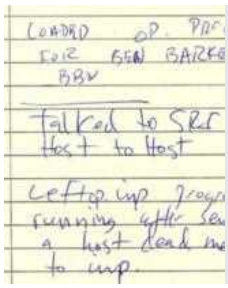
88 LEGGI

06/11/19 | Cyber

HACKING THE HACKERS! QUANDO A CADERE NELLA (CYBER) TELA È IL RAGNO STESSO...

Nei precedenti articoli il cyber-spazio è stato spesso rappresentato come il far west in cui sono ambientati i classici...

520 LEGGI



29/10/19 | Cyber

29 OTTOBRE 1969: NASCE ARPANET, L'ODIERNA INTERNET

Nel 1958 il presidente americano D.D. Eisenhower crea l'Advanced Research Project Agency, l'agenzia del del...

628 LEGGI

28/10/19 | Cyber

ITALIA: NUOVE TECNOLOGIE, FORMAZIONE E GOVERNO DEL RISCHIO INESISTENTE

Oggi il computer è in molti casi "invisibile" almeno nell'accezione di uno strumento necessariamente costituito da una...

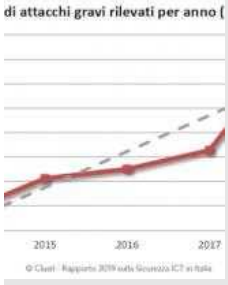
293 LEGGI

21/10/19 | Cyber

ATTACCO CYBER CONTRO L'IRAN? GLI STATI UNITI DICONO...

Il 16 ottobre, la Reuters esce con un articolo-sensazione "Exclusive: U.S. carried out secret cyber strike on Iran in...

1392 LEGGI



14/10/19 | Cyber

PERIMETRO DI SICUREZZA NAZIONALE: LE AZIENDE PUNTANO L'ATTENZIONE SU INFRASTRUTTURE E FORMAZIONE

Il recente decreto legge sul perimetro di sicurezza cibernetica è il frutto di nuove riflessioni sull'evoluzione della...

330 LEGGI