

INFORMAZIONI PERSONALI

Stefano Ramacciotti

POSIZIONE ATTUALE

Grado: Contrammiraglio (AUS, dal 2023) – NATO OF-6
In Marina Militare dal 1982ESPERIENZA
PROFESSIONALE

[Gli ultimi 15 anni sono elencati dal più recente (in grassetto i compiti relativi alla Cybersecurity)]

Dal 02.10.2023 al continua

Consulenza

NITEL - Consorzio Nazionale Interuniversitario per i Trasporti e la Logistica che opera insieme ad un raggruppamento temporaneo di scopo composto da Sentech (mandatario), Swascan, Athonet (Roma)

Attività di consulenza per gli aspetti di sicurezza del progetto di ricerca "5G4Mil - Rete mobile 5G dedicata, sicura e integrata per applicazioni Militari"

Lavoro o settore: Information Assurance

Dal 23.11.2022 al 30.06.2023

Consulenza

Hermes Bay (Roma)

Attività di consulenza su laboratori di prova e metodi di certificazione

Lavoro o settore: Information Assurance

Dal 22.07.2022 al continua

Docenza

Gam Education & Consulting S.r.l. (Milano)

Attività di docenza su Information Security e Cybersecurity

Lavoro o settore: Cybersecurity

Dal 01.06.2022 al 31.12.2022

Consulenza

Romars (Roma)

Attività di consulenza per:

- **mappatura degli attuali sistemi satellitari utilizzati per scopi militari e delle funzioni svolte;**
- **descrizione delle principali caratteristiche tecniche dei sistemi satellitari con particolare riferimento a quelle riguardanti la sicurezza;**
- **definizione di scenari operativi;**
- **rassegna di tecniche di attacco e di difesa "cyber" di sistemi di comunicazione satellitari.**

Lavoro o settore: Cybersecurity

Dal 20.09.2018 al continua

DocenzaMaster di II livello "Competenze digitali per la protezione dei dati, la *cybersecurity* e la *privacy*", Università di Tor Vergata (Roma)**Attività di docenza su Perimetro di sicurezza cibernetica e la protezione del patrimonio informativo della Difesa, Certificazioni Common Criteria e attività di laboratorio (vds paragrafo Docenze)**

Lavoro o settore: Cybersecurity

Dal 6.09.2018 al continua

Docenza

Master di II livello "Cybersecurity and Critical Infrastructure Protection", DITEN – Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni – Università degli Studi di Genova

Attività di docenza su standard di sicurezza ICT (vds paragrafo Docenze)

Lavoro o settore: Information Assurance

Dal 15.09.2021 al continua

Presidente (ISC)² Italy Chapter(ISC)² Italy Chapter (<https://www.isc2chapter-italy.it/>) è un'associazione con più di 700 professionisti in

cybersecurity, che ha come missione diffondere la consapevolezza degli aspetti di sicurezza fisica e dell'informazione e favorire un uso maggiormente consapevole e sicuro degli strumenti informatici, anche da parte dei non addetti ai lavori, seguendo gli obiettivi, le linee di comportamento e favorendo le iniziative della più grande associazione a livello internazionale del settore, l'International Information Systems Security Certification Consortium, Inc., (ISC)²®, di cui l'associazione è il Capitolo Italiano. L'obiettivo è quello di avviare iniziative volte a condividere le esperienze e le informazioni di professionisti, o studiosi del campo della Sicurezza ICT sia nell'ottica degli obiettivi di (ISC)²®, che nell'ottica di approfondimenti nel settore della sicurezza informatica, che possono comprendere:

- **Facilitazione della formalizzazione delle competenze in sicurezza informatica mediante certificazioni ed iniziative volte all'orientamento e mantenimento di queste;**
- **Favorire il riconoscimento in Italia delle certificazioni e di altre iniziative che (ISC)²® intenderà promuovere;**
- **Attività propositiva/normativa in materia di sicurezza informatica;**
- **Iniziative nei confronti ed a supporto di persone, aziende, autorità competenti, organizzazioni nazionali ed internazionali in merito a tematiche di Information Security;**
- **Partecipazione attiva nella definizione delle politiche contro il cyber crime, la cyber security e relative alla cyber defence delle infrastrutture critiche;**
- **Attività di formazione e preparazione per certificazioni nel settore, gruppi di studio, seminari, monografie, riassunti, traduzione, adattamenti del materiale, training e tutoring per esami di certificazione professionale;**
- **Attività di diffusione della cultura della sicurezza anche presso le università, con attenzione a tematiche di ricerca, e gli istituti scolastici;**
- **Favorire le relazioni professionali tra gli associati, i rapporti con le aziende e l'orientamento al mondo della sicurezza informatica per i neo-laureati;**
- **Collaborare con altre associazioni nel settore, sfruttando sinergie ed obiettivi comuni.**

Lavoro o settore: Cybersecurity

Dal 16.02.2019 al 11.05.2019

Docenza

Università di Pisa (codice materia 76911) in Accademia Navale di Livorno:

Corso di *Cyber Defence* totali 52 ore (6 CFU), (vds paragrafo Docenze)

Lavoro o settore: Cyber Defence

Estate 2014

Consulente (attività extraprofessionale)

HiTrust S.r.l. (Pescara). Attività principali e responsabilità:

- **Attività extralavorativa per la HiTrust S.r.l. di Pescara di consulenza a grande impresa nazionale per mettere il sito di produzione in condizioni di essere certificato secondo la procedura di "Site Certification" di cui alla ISO/OSI 15408, mai effettuata in Italia ma prevista nell'ambito dell'accordo Common Criteria Recognition Arrangement, CCRA.**

Lavoro o settore: Information Assurance

Da Aprile 2011 al continua

Capo Delegazione (Head of delegation, HoD) e *National Body* del Gruppo di Lavoro 3, WG3 (Security Evaluation, Testing and Specification) del SC27 di ISO-IECJ/TC1 e delegato del JWG6 sulla sicurezza nell'automotive

Delega conferita da UNINFO, l'Ente di normazione per il settore delle tecnologie informatiche federato a UNI, l'Ente nazionale di certificazione e standardizzazione. Attività principali e responsabilità:

- **Elaborazione e revisione criteri di valutazione per la sicurezza IT, metodologia per la valutazione della sicurezza ICT, test di conformità dei meccanismi di sicurezza.**
- **Elaborazione e revisione "Cybersecurity requirements and evaluation activities for connected vehicle devices"**

Lavoro o settore: Information Assurance

Dal 16.09.2018 al 30.12.2020

Capo Ufficio Sicurezza

Il Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa e Organo Centrale di Sicurezza dello Stato Maggiore della Difesa. Attività principali e responsabilità:

- Ufficiale di cui si avvale l'Ufficiale alla Sicurezza dell'Organo Centrale di Sicurezza dello SMD per tutte le tematiche inerenti alla tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva nei **settori INFOSEC, Gestione del Rischio**, Segreteria Speciale, Gestione sicurezza del personale e Nulla Osta di Sicurezza, attività ispettiva e di **auditing INFOSEC** e COMSEC.

Lavoro o settore: Defence

Dal 01.03.2017 al 15.09.2018

Capo Sezione Tecnica INOSEC

Il Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa e Organo Centrale di Sicurezza dello Stato Maggiore della Difesa. Attività principali e responsabilità:

- **Ufficiale alla Sicurezza CIS dell'Organo Centrale di Sicurezza dello SMD;**
- **Analisi del rischio CIS, approvazione nuove architetture CIS, omologazioni di sistemi, audit di sicurezza CIS;**
- **Partecipazione Gruppi di Lavoro e Tavoli Tecnici relativi al settore Information Security sui principali progetti della Difesa.**

Lavoro o settore: Defence

Dal 01.12.2013 al 28.02.2017

Ufficiale di collegamento tra lo Stato maggiore della Marina (S.M.M.) e il Ministero dello Sviluppo Economico (Mi.S.E.)

Ministero dello Sviluppo Economico. Attività principali e responsabilità:

- Partecipazione Gruppi di Lavoro per recepimento Direttiva 2013/30/UE (Direttiva Offshore);
- **Focus su aspetti di sicurezza informatica e analisi del rischio;**
- Implementazione dell'accordo esecutivo.

Lavoro o settore: Defence

Estate 2014

Consulente (attività extraprofessionale)

HiTrust S.r.l. (Pescara). Attività principali e responsabilità:

- **Attività extralavorativa per la HiTrust S.r.l. di Pescara di consulenza a grande impresa nazionale per mettere il sito di produzione in condizioni di essere certificato secondo la procedura di "Site Certification" di cui alla ISO/OSI 15408, mai effettuata in Italia ma prevista nell'ambito dell'accordo Common Criteria Recognition Arrangement, CCRA.**

Lavoro o settore: Information Assurance

Dal 08.09.2007 al 30.11.2013

Direttore del Centro di Valutazione della Difesa, Ce.Va. Difesa (San Piero a Grado, Pisa)

Ce.Va. Difesa. Attività principali e responsabilità:

- **Direzione del Ce.Va. Difesa per valutazione della sicurezza di sistemi HW, SW e firmware, di cui: nr. 3 EAL1/1+, nr. 4 EAL4 e responsabile della valutazione e valutatore per l'*Italian Information Exchange Gateway (IEG-IT) (EAL1+)* della Difesa;**
- **Partecipazione a Gruppi di Lavoro sulla *Software Defined Radio*, SDR, in qualità di responsabile nazionale per la redazione dei requisiti di sicurezza della:**
 - ***Software Defined Radio* nazionale (SDR-N), per il progetto della piattaforma;**
 - ***European Secure Software defined Radio (ESSOR)*, rappresentante presso l'OCCAR per il progetto relativo ad una forma d'onda con *High Data Rate* (6 Paesi);**
 - ***Coalition Waveform Narrow Wideband (COALWNN)*, per una forma d'onda *narrow band* (11 Paesi).**
- **Attività di consulenza per gli aspetti di sicurezza sui principali progetti della Difesa (Forza NEC, DII, IT-EKMS, ecc.).**

Lavoro o settore: Defence

Dal 10.11.2005 al 07.09.2007

Capo del 15° Ufficio Firma Digitale, Referente Tecnico per la M.M. in ambito S.M.D. e responsabile per i rapporti con il CNIPA per la firma forte, Addetto al 13° Ufficio Sicurezza (dell'Agenzia di Sicurezza dello S.M.M.), Capo Sezione Normativa e tutela segreto di stato nonché responsabile della sicurezza dei sistemi informatici gestionali della M.M. (dal 2006) e Ufficiale alla sicurezza EAD della M.M. (da 13.06.2007)

Stato Maggiore della Marina. Attività principali e responsabilità:

- **Per la Firma Digitale della Marina Militare: gestione e configurazione dei sistemi, audit, implementazione del sistema di gestione della sicurezza delle informazioni, formazione, problematiche ICT relative alla *Business Continuity*. Nel corso del mandato è stato portato a compimento:**
 - “Direttiva per il rilascio e la gestione della Carta Multiservizi della Difesa (C.M.D.) in ambito Marina Militare” – S.M.M. (2006);
 - il progetto della PKI della Marina (con la emissione delle prime 6.000 smart card);
 - progetto della PKI della Difesa (in qualità di membro permanente dei G.d.L. per la Firma Digitale e per la Carta Multiservizi della Difesa);
 - la collaborazione con il C.N.I.P.A. per l'emissione delle carte con firma forte al personale M.M..
- Come Capo Sezione normativa e tutela del segreto di stato a seguito dell'analisi dell'impatto della normativa vigente sulla gestione della sicurezza IT, ho redatto il “**Regolamento Interno di sicurezza**” standard per i Comandi della M.M. (350 pag. circa) ed effettuato numerosi *audit*, in qualità di Capo Team Ispettore, per la tutela del segreto di stato, cifra ed E.A.D. e redatte le linee guida per il comparto “Sicurezza ICT della M.M.”;
- Come membro dell'O.C.S. di forza armata, effettuate attività di analisi del rischio per l'implementazione di soluzioni di sicurezza in conformità alle normative vigenti, e di stesura e controllo dei requisiti di sicurezza dei vari progetti in corso della M.M..

Lavoro o settore: Defence

Dal 20.09.2004 al 09.11.2005

Vice Direttore e Ufficiale alla sicurezza E.A.D. designato del Centro di Telecomunicazioni e Informatica della M.M. (MARITELE) Roma e Capo Reparto Gestione Sistemi

Centro di Telecomunicazioni e Informatica della M.M. (MARITELE) Roma. Attività principali e responsabilità:

- Gestione del personale del Centro (nr. 520 militari e nr. 63 civili della Difesa) e gestione diretta come **Capo Reparto del Reparto Gestione Sistemi** (circa 220 tra militari e civili);
- **Gestione tecnica con responsabilità sugli aspetti di sicurezza E.A.D. di circa 200 server;**
- **Membro del Gruppo di gestione DIFENET (dal 27.04.2005);**
- **Redattore del “Documento Programmatico per la Sicurezza” - Maritele Roma (2005).**

Lavoro o settore: Defence

Dal 1996 al 2004

Nel corso di vari incarichi provveduto a realizzare LAN presso vari Comandi e Unità Navali e operato come webmaster

Reti realizzate:

- 2003-2004: su Nave Urania di base a Augusta in qualità di Comandante ho operato come webmaster e ricoperto il compito di Ufficiale alla Sicurezza EAD
- 2002-2003: su Cacciatorpediniere Ardito di base a La Spezia in qualità di Comandante in Il operato come webmaster e ricoperto il compito di Ufficiale alla Sicurezza EAD 1996-1998: presso il Comando delle Forze di Contromisure Mine di La Spezia in qualità di Ufficiale TLC realizzata LAN con 25 PC e 40 utenti
- 2001-2002: su Fregata Libeccio di base a La Spezia in qualità di Comandante in Il collaborato a realizzare una LAN con 40 PC e 70 utenti e ricoperto il compito di Ufficiale alla Sicurezza EAD
- 1998-2001: su Nave San Marco di base a Brindisi di La Spezia in qualità di Capo Reparto Operazioni realizzata LAN con 50 PC e 80 utenti
- 1996-1998: presso il Comando delle Forze di Contromisure Mine di La Spezia in qualità di Ufficiale TLC realizzata LAN con 25 PC e 40 utenti

Lavoro o settore: Defence

ISTRUZIONE E FORMAZIONE

[Corsi elencati dal più recente (in grassetto i corsi relativi alla Sicurezza ICT)]

- 08.06.2020 – 19.06.2020 **Seminario C.V.-C.F. (con SLPP - Corso per Datori di Lavoro e Dirigenti. Esito: 30/30)**
Comando Scuole Marina Militare - Ancona
- **Comprendivo di corso per Datori di Lavoro e Dirigenti**
- 07.10.2019 – 11.10.2019 **Social Network Intelligence Course (risultato: promosso)**
Centro Interforze di Formazione Intelligence e Guerra Elettronica, CIFIGE (Roma)
- **Corso sugli aspetti Social Network Intelligence in ambito OSINT**
- 06.05.2019 – 10.05.2019 **Corso Propedeutico alle Computer Network Operations (esito: 30/30)**
Centro Interforze di Formazione Intelligence e Guerra Elettronica, CIFIGE (Roma)
- **Argomenti relative alle Computer Network Operations topics**
- 14.05.2018 – 08.06.2018 **Corso Network Security Tester 2.0 Course (esito: 27/30)**
Scuola di Telecomunicazione delle Forze Armate (Chiavari, GE)
- **Qualificato Vulnerability Assurance Tester**
- 03.04.2018 – 13.04.2018 **Corso Open Source Intelligence (OSINT) (esito: promosso)**
Centro Interforze di Formazione Intelligence e Guerra Elettronica, CIFIGE (Roma)
- **Qualificato Operatore OSINT**
- 18.09.2014 – 30.10.2014 **Corso Information Security Incident Handling (total: 6 hours) (esito: High Distinction 90/100)**
Charles Sturt University (Australia)
- **Gestione incidenti di Information Security, SOC e CSIRT**
- 16.07.2012 – 20.07.2012 **Corso NATO Communications and Information Systems Orientation Staff Officer (esito: favorevole)**
NATO Communications and Information Systems School, Latina
- **Sistemi CIS (Communication and Information System) della NATO**
- 21.11.2010 – 10.12.2010 **Corso di aggiornamento su "Common Criteria & Information Security course" (120 ore)**
CGI, Ottawa (Canada)
- **"Common Criteria & Information Security course", con particolare riguardo alle più recenti tecniche di attacco**
- 11.10.2010 – 15.10.2010 **Corso "Lead Auditor ISO/IEC 27001:2005"**
CSQA
- **Qualificato come valutatore di sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma UNI CEI ISO/IEC 27001:2006**
- 21.11.2009 esame (corso CISSP
CBK: 19.10.2009 - 23.10.2009) **Certificato CISSP (Certified Information System Security Professional) seguito effettuazione relativo corso**

(ISC)², International Information Systems Security Certification Consortium (<https://www.isc2.org>)

- **CISSP dal 02.04.2010** (link per verifica: https://www.credly.com/badges/c234554a-4059-4034-95d9-43f07043b8e7/public_url)

30.11.2009 – 4.12.2009 **Corso “Certified Hetical Hacker” (esito: favorevole)**

OVERNET education

- **Corso di aggiornamento su *ethical hacking***

22.07.2008-18.11.2008 **Corso “on-the-job training” sui Common Criteria**

Domus IT Security Lab - Ottawa (Canada)

- **Tecniche e strumenti per la ricerca di vulnerabilità, gestione laboratorio secondo lo standard ISO 17025, redazione manuale su “Attack tools and attack methods”**

06.10.2008-10.10.2008 **Corso FIPS 140-2**

Domus IT Security Lab - Ottawa (Canada)

- **Requisiti di sicurezza per moduli crittografici**

26.06.2008-20.07.2008 **Valutatore CC EAL4 seguito Corso sui Common Criteria vers. 3.1R2**

Domus IT Security Lab - Ottawa (Canada)

- **Ethical hacking refresh course**

23.06.2008-24.06.2008 **Valutatore CC EAL1 seguito Corso sui Common Criteria vers. 2.3 a cura del CESC**

Canadian Communication Security Establishment

- **Ethical hacking refresh course**

19.05.2008-25.06.2008 **Corso sui Common Criteria vers. 2.3 a cura Domus Lab.**

Domus IT Security Lab - Ottawa (Canada)

- **Ethical hacking refresh course**

12.12.2006 – 14.12.2006 **Corso “Risk assessment” (esito: favorevole)**

Araknos s.r.l. - Roma

- **Gestione e valutazione del rischio informatico.**

06.06.2005 – 14.10.2005 **2° Corso Sicurezza ICT – Modulo Avanzato (esito: 2° su 16 frequentatori con una media di 27,8/30)**

DCE Cecchignola e Consiglio Nazionale delle Ricerche con personale CNIPA

- Riconosciuto come **Master di I livello** per i possessori di laurea in Ingegneria, Informatica, Matematica e Fisica. Esami su:
 - Richiami sui sistemi operativi
 - Richiami sulle reti di calcolatori
 - Introduzione alla sicurezza informatica
 - Crittografia e sicurezza delle reti
 - Tecnologie per la sicurezza delle reti basate su metodi crittografici
 - Rapporto tra configurazione degli apparati di rete e sicurezza in scenari tipo
 - Tecnologie anti intrusione e sistemi di autenticazione
 - Sicurezza di sistema e sicurezza di rete
 - Aspetti normativi della sicurezza e certificazione

18.10.1982 – 26.04.1986

Laurea in “Scienze Marittime e Navali” (Università degli Studi di Pisa, classe delle lauree in “Scienze della Difesa e della Sicurezza”

Italian Naval Academy - Livorno

- **Scienze Marittime e Navali** comprensiva del Corso IGM con Specializzazione in Telecomunicazioni equivalente alla Laurea triennale in Ingegneria delle Telecomunicazioni.

COMPETENZE PERSONALI

[Aggiungere campi di interesse o più significativi]

Lingua madre Italiano

Altre lingue

Livello europeo (*)

Inglese

Francese

COMPRESIONE		PARLATO		PRODUZIONE SCRITTA
Ascolto	Lettura	Interazione orale	Produzione orale	
C1	C2	C1	C1	C2
Sostituire con il nome del certificato di lingua acquisito. Inserire il livello, se conosciuto				
A2	B1	A1	A1	A1
Sostituire con il nome del certificato di lingua acquisito. Inserire il livello, se conosciuto				

Livelli: A1/A2: Utente base - B1/B2: Utente intermedio - C1/C2: Utente avanzato

[Quadro Comune Europeo di Riferimento delle Lingue](#)

Inglese: ultimo censimento ambito MMI nel 1993 esito 78.80/100

Competenze comunicative

Dal 22/03/2012 socio fondatore e membro del Comitato Direttivo e di ISC2 *Italy Chapter* (capitolo italiano di *International Information System Security Certification Consortium*), e **responsabile nazionale del “Gruppo di lavoro Educazione alla Sicurezza Informatica”** dalla I Elementare alla V Superiore, con circa 70 formatori distribuiti in tutta Italia. Dal 15 settembre 2021 ricopro l'incarico di Presidente. **Alla data attuale effettuate presentazioni per la consapevolezza di studenti, insegnanti e personale A.T.A. per più di 58.00 persone da parte del GdL, di cui più di 14.500 raggiunte personalmente**

Competenze organizzative e gestionali

Gestione diretta di circa 590 persone

Competenze professionali

Tematiche di sicurezza in ambito Difesa.

Competenze digitali

AUTOVALUTAZIONE				
Elaborazione delle informazioni	Comunicazione	Creazione di Contenuti	Sicurezza	Risoluzione di problemi
Utente avanzato	Utente avanzato	Utente avanzato	Utente avanzato	Utente avanzato

Livelli: Utente base - Utente intermedio - Utente avanzato

[Competenze digitali - Scheda per l'autovalutazione](#)

Sostituire con il nome del certificato di lingua acquisito. Inserire il livello, se conosciuto

- Conoscenza approfondita di numerosi standard ISO di competenza del Security Evaluation Assurance Working Group;
- Ottima conoscenza di programmi MS Office™;
- Ottima conoscenza di vari pacchetti per *vulnerability assessment e penetration test (al 2018)*;
- Buona di attività sistemistica, Networking, progettazione, realizzazione e gestione di reti locali e di servizi per reti TCP/IP e hardening in ambiente misto Windows (Server e client) / Mac (Client) / Linux (Server e client) e sistemi di virtualizzazione (tecnologia VirtualBox, VMware);
- Buona conoscenza di linguaggi di programmazione/scripting: RPN, BASIC, C e C++, HTML;
- Buona conoscenza di Codice Privacy e Regolamento UE 2016/679.

Altre competenze Number Theory and Cryptography.

ULTERIORI INFORMAZIONI

[Aggiungere voci separate per ogni attività, iniziando dalla più recente]

Docenze Corso di alta formazione “Il professionista di security: competenze e abilità per nuove strategie integrate di sicurezza”, Scuola Internazionale Etica e Sicurezza - Milano - L'Aquila (corsi organizzati da Gam Education & Consulting S.r.l., Milano)

Ore lezione	Titolo	Data
3,5	<i>Information Security & Cybersecurity</i>	27.09.2023
4	<i>Information e Cyber Security al corso “Professionista di Security”</i>	15.07.2023
4	<i>Information e cybersecurity</i>	22.11.2022
4	<i>Il professionista di security: competenze e abilità per nuove strategie integrate di sicurezza - Lezione Scuola di Etica</i>	22.07.2022

Master di II livello “Competenze digitali per la protezione dei dati, la cybersecurity e la privacy”, Università di Tor Vergata (Roma)

Ore lezione	Titolo	Data
15	<i>Perimetro di sicurezza cibernetica e la protezione del patrimonio informativo della Difesa, Certificazioni Common Criteria e attività di laboratorio</i>	22.02.2024 06.11.2023 06.10.2023 15.09.2023
15	<i>Perimetro istituzionale di protezione delle informazioni ed il patrimonio informativo della Difesa e sua tutela: best practices</i>	23.07.2022 16.09.2022 17.09.2022 19.10.2022
8	<i>Perimetro istituzionale di protezione delle informazioni ed il patrimonio informativo della Difesa e sua tutela: best practices</i>	16.07.2021 24.09.2021
4	<i>Perimetro istituzionale di protezione delle informazioni ed il patrimonio informativo della Difesa e sua tutela: best practices</i>	24.10.2020
3	<i>Perimetro istituzionale di protezione delle informazioni ed il patrimonio informativo della Difesa e sua tutela: best practices</i>	29.10.2019
4	<i>Il patrimonio informativo e sua tutela: best practices</i>	20.09.2018

Master di II livello “Cybersecurity and Critical Infrastructure Protection”, DITEN – Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni – Università degli Studi di Genova

Ore lezione	Titolo	Data
4	<i>Standard & Best Practice in Information Security</i>	20.05.2023
4	<i>Standard & Best Practice in Information Security</i>	19.03.2022
2	<i>Gli standard di sicurezza ICT. Standards and Best Practices for Security and Safety</i>	04.02.2021
2	<i>La norma ISO/IEC 15408 (Common Criteria) per la Certificazione di sicurezza di prodotti e sistemi IT. Standards and Best Practices for Security and Safety</i>	30.01.2021
2	<i>Common Criteria Standard, PSNC e CVCN</i>	30.01.2020
4	<i>Standard & Best Practice in Information Security</i>	06.09.2018

Centro Interforze di Formazione Intelligence e Guerra Elettronica, CIFI (Roma)

Titolo	Data
<ul style="list-style-type: none"> ▪ Corso OSINT: “Cyber Defence”; ▪ Corso Intelligence Interforze: “La Sicurezza delle Informazioni”; ▪ Ufficiali CIS: “Corso di sicurezza CIS”; ▪ Personale Addettanze e Rappresentanze Militari all'estero (Addetti Militari, Coadiutori e Carabinieri di prossima destinazione all'estero): “La Sicurezza delle informazioni in ambito CIS e COMSEC”. 	Da maggio 2017 a dicembre 2020

Università di Pisa (codice materia 76911) in Accademia Navale di Livorno

Titolo	Data

<ul style="list-style-type: none"> ▪ Titolare del corso di <i>Cyber Defence</i> per totali 52 ore (6 CFU) ▪ Relatore alla tesi di Laurea in “<i>Cyber Defence</i>” dal titolo “La minaccia cyber e il quinto dominio operativo” discussa in data 26.06.2019 	dal 16.02.2019 al 11.05.2019
---	------------------------------

Scuola di Telecomunicazione delle FF.AA. (STELMILIT) a Chiavari (GE)

Titolo	Data
<ul style="list-style-type: none"> ▪ Seminari sui Common Criteria, “<i>Corso INFOSEC di 3° livello</i>” con cadenza semestrale 	da marzo 2010 a settembre 2013

Relatore conferenze

Relatore per diversi convegni, nazionali e **internazionali**, su tematiche legate alla sicurezza ICT:

- Presentazione su “*Evoluzione dei Common Criteri e punto di situazione sul loro aggiornamento*”, Security Summit (Clusit), Milano, 16 marzo 2023;
- Presentazione su “*Attività ISO/IEC JTC 1 SC 27 – WG 3, Sintesi dei lavori sulle norme e focus su ISO/IEC 15408/18045 e norme collegate*”, ambito UNINFO, 20 dicembre 2022;
- Presentazione “*Perimetro di Sicurezza Nazionale Cibernetica: cosè e che impatti avrà con particolare riguardo alle attività di certificazione*”, webinar (ISC)2 Italy Chapter 17 novembre 2022;
- Presentazione libro “*Rischio digitale innovazione e resilienza*”, al convegno Clusit “Security Summit 2022”, Milano, 16 marzo 2022, in qualità di team leader e autore per la parte relativa alle misure di sicurezza;
- Presentazione “*ISO/IEC 15408, Assurance continuity e certificazioni PSNC*”, al convegno Clusit “Security Summit 2021”, Milano, 11 novembre 2021, in qualità di Capo Delegazione UNIFO del JTC1/SC27/WG3 “Security Evaluation Criteria” di ISO;
- Presentazione su “*Social Media e ragazzi: quali pericoli*” al Convegno su “Cellulari, social network, mass media nella comunicazione dei giovani. Cosa si nasconde dietro un click”, Forte dei Marmi (LU), 10 marzo 2018;
- Presentazione “*Pericoli dei Social Network*”, al convegno sotto il patrocinio del MIUR “Smart Education & Technology Days”, Napoli, Città della Scienza 30 ottobre 2015;
- Webinar (ISC)2 Chapter Italy: “*Hic sunt leones ovvero il Deep & Dark Web*”, S. Ramacciotti e P. Paganini, 21 ottobre 2015;
- Presentazione “*Deep&Dark Web*”, al convegno Clusit “Security Summit 2016”, Roma 10 giugno 2016, in qualità docente Clusit;
- Webinar a favore Dipartimento di Psicologia – Università di Firenze: “*Deep&Dark Web*”, S. Ramacciotti e P. Paganini, 21 febbraio 2015;
- Presentazione al Festival Firenze: “*NON CADERE NELLA RETE - I giovani si esprimono sull’uso consapevole della Rete*”, convegno Lions Club Firenze, 09 maggio 2015;
- Presentazione su: “*La Sicurezza dei ragazzi su Internet*”, convegno Lions Club Carrara, 17 gennaio 2015; ;
- Presentazione su: “*La Sicurezza dei ragazzi su Internet*”, convegno Lions Club Cecina, 12 aprile 2014;
- Presentazione su: “*I Common Criteria: loro funzione e come stanno evolvendo*”, conferenza meeting ORACLE Security Community, Milano 16.05.2013;
- Presentazione su: “*I Common Criteria... perchè?*”, convegno sulla Cyber Defence in occasione del 60-ennale di STELMILIT, Chiavari 16.05.2012;
- **Presentazione su: “The Common Criteria and their practical application”, al convegno Cyber Defence & Network Security, London (UK), January 26, 2012;**
- **Presentazione su: “Evaluation strategies for a Software Defined Radio”, Amsterdam (NL), 28 october 2011;**
- Presentazione “*I requisiti di sicurezza per i moduli crittografici e la validazione degli algoritmi crittografici secondo lo standard FIPS 140-2*”, al convegno Clusit “Security Summit 2011”, Roma 09 giugno 2011, in qualità di Direttore Ce.Va. Difesa e docente Clusit;
- Presentazione “*Lo Schema Nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell’informazione, ai fini della tutela delle informazioni classificate, ed i Common Criteria*”, al convegno Clusit “Security Summit 2010”, Roma 09 giugno 2010, in qualità di Direttore Ce.Va. Difesa e docente Clusit;
- Presentazione “*I Common Criteria e lo Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell’informazione, ai fini della tutela delle informazioni classificate*”, al convegno “From SDR to Cognitive Networks”, 26 novembre 2009;
- Presentazione “*I Common Criteria 3.1 ad un anno di distanza dalla loro entrata in vigore. Cosa è cambiato dalla versione 2.3 alla 3.1R2*”, al convegno Clusit “Security Summit

2009”, Milano, 24 marzo 2009 e Roma 10 giugno 2009, in qualità di Direttore Ce.Va. Difesa e docente Clusit;

- Presentazione su “*I Common Criteria*”, al convegno Elsig Datamat “Security Forum 2007”, Francavilla al Mare (CH), 29 novembre 2007, in qualità di Direttore Ce.Va. Difesa;
- Relatore al Convegno: Security Day per la Difesa e per la Pubblica Amministrazione - Bancaeuropa - Roma, 09/11/2006;
- Relatore al Convegno: E-Government e Sicurezza per la PA e la Difesa - Bancaeuropa - Roma, 08/11/2006.

Pubblicazioni

- S. Ramacciotti e C. Gallotti, “*La modifica periodica delle password: giusto o sbagliato? Breve ricerca per scegliere con maggiore consapevolezza le nostre politiche*”, pubblicato sulla rivista Digeat, 19 marzo 2024, <https://digeat.info/articolo-rivista/la-modifica-periodica-delle-password-come-affrontare-professionalmente-un-argomento-tecnico/>;
- **S. Ramacciotti, “*Bridging the Gap: Strengthening Security Communities in Italy through Collaboration Training and Awareness*”, intervista a cura About Resilience, 10 gennaio 2024, sito <https://www.aboutresilience.com/>**
- S. Ramacciotti et al., “*La Business Continuity*”, whitepaper (ISC)2 Italy Chapter, 2023;
- S. Ramacciotti et al., “*Certificazioni professionali*”, aggiornamento pubblicazione Clusit relativamente alle certificazioni di (ISC)2, 2023;
- S. Ramacciotti et al., “*Ransomware*”, whitepaper (ISC)2 Italy Chapter, 2022;
- Security Community for Clusit, “*Rischio digitale innovazione e resilienza*”, Clusit, Ed. 2022, Milano;
- S. Ramacciotti, “*Internet e figli - insegniamo ai nostri figli a navigare in sicurezza*”, ebook reperibile su <http://www.isc2chapter-italy.it/wp-content/uploads/2016/10/20160930-ebook-ISC2-Sicurezza-Internet.pptx.pdf>, settembre 2016;
- S. Ramacciotti, “*Il progetto Sauro*”, Rivista Marittima, Ottobre 2015;
- S. Ramacciotti, Appendice sui Common Criteria e sulle FIPS 140 (10 pagg.), al libro “*Sicurezza delle Informazioni - Valutazione del rischio – I sistemi di gestione - La norma ISO/IEC 27001:2013*” di Cesare Gallotti, 2014;
- S. Ramacciotti (et altri) traduzione in italiano di “*ISO/IEC 27000 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*”;
- A. Rui, S. Ramacciotti, “*Formazione e consapevolezza, strumenti indispensabili per la Sicurezza delle Informazioni*”, Rapporto Clusit 2014;
- S. Ramacciotti, “*I Common Criteria... perchè?*”, “*Rivista Italiana Difesa*”, supplemento luglio 2012;
- S. Ramacciotti, “*La sicurezza delle informazioni al tempo di WikiLeaks. Dal “need-to-know” al “need-to-share” e ritorno*”, rivista “*Informazioni della Difesa*” n. 3 - 2011
- S. Ramacciotti, “*I Common Criteria e i compiti del CeVa Difesa*”, Pubblicato sulla Rivista “*Aeronautica*” N. 3 - 2011;
- **S. Ramacciotti e C. Zhou, “*Common Criteria: Its Limitations and Advice on Improvement*”, *ISSA Journal* | April 2011;**
- S. Ramacciotti, “*Lo Schema Nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, ed i Common Criteria*”, in Conference Proceeding del convegno “*From Software Defined Radio To Cognitive Networks. Trend evolutivi ed attività dei centri di eccellenza italiani nel settore*”, CISAM-Ist. Vallauri, 2009;
- C.A. V.E. Di Cecco, C.F. S. Ramacciotti, “*I Common Criteria ed il Centro di Valutazione della Difesa. Lo Standard ISO 15408 e le attività di valutazione del Ce.Va. Difesa*”, Pubblicato sulla Rivista “*Informazioni della Difesa*” N. 1 - 2008;
- C.A. V.E. Di Cecco, CF S. Ramacciotti, “*Esperienze e problematiche relative alla applicazione dello Schema Nazionale di valutazione e certificazione della sicurezza delle tecnologie in ambito governativo*”, pubblicato su “*Elsig Datamat Security Forum Report*”, 2007;
- Stefano Ramacciotti, “*La Carta Multiservizi della Difesa. Un nuovo strumento per il personale in servizio*”, Notiziario della Marina, Settembre/Ottobre, 2006;
- S. Ramacciotti, “*Pietro Micca*”, Notiziario della Marina, 1995.

- Traduzioni
- Traduzione di ISO/IEC 27005:2022 Information security management systems (in inglese) in UNI/CEI EN ISO/IEC 27005:2024 (in italiano)
 - Traduzione di ISO/IEC 27001:2022 Information security management systems (in inglese) in UNI/CEI EN ISO/IEC 27001:2024 (in italiano)
 - Traduzione di ISO/IEC 27002:2022 Information security management systems (in inglese) in UNI/CEI EN ISO/IEC 27002:2023 (in italiano), 10.02.2022 – 21.11.2022
 - Traduzione di ISO/IEC 27000:2017 Information security management systems (in inglese) in UNI/CEI EN ISO/IEC 27000:2017 (in italiano), 2017

- Organizzazione
convegni/conferenze
- Organizzatore e chairman convegno, in presenza e in streaming in italiano e inglese, presso l'Auditorium della sede distaccata dell'Università di Bologna, dal titolo *"Collaborative Business Continuity, Disaster Recovery & Crisis Management. Come affrontare il nuovo disordine globale: le lessons learned e come costruire una nuova armonia"*, Faenza (RA), 20 settembre 2022;
 - Organizzatore e chairman convegno sul GDPR presso l'Auditorium Fondazione Banca del Monte di Lucca *"Il Regolamento UE 2016/679 applicato alla realtà nazionale"*, Lucca, 12 maggio 2018.