Antonio Rossi

Data di nascita: 10/07/1975

Sesso: Maschile

CONTATTI

Via Trieste, 80, Condominio Gienstra, int. 08
04014 Pontinia, Italia
(Abitazione)

antonio.rossi@mac.com

(+39) 3883219400

europass

ESPERIENZA LAVORATIVA

Leonardo S.p.A. Roma, Italia

Cyber Security Manager

15/06/2014 – Attuale

Progettazione e implementazione di un modello operativo integrato SOC/CERT (Cyber Defence Operation Center), unificando le funzioni di Detection e Response in un unico centro di responsabilità tecnico-operativa. Il modello ha introdotto l'automazione della risposta su pattern noti, potenziato le capacità di Threat Hunting e Cyber Threat Intelligence e avviato un Cyber Response Lab per lo sviluppo di soluzioni tecnologiche proprietarie complementari ai prodotti di mercato.
Nella gestione del CERT, coordinamento H24 dei servizi di Incident Management, definizione delle procedure aziendali di segnalazione e gestione degli incidenti, concertazione dei piani di rimedio con le funzioni IT Security. Ideazione e realizzazione di CyberShield "Facing the Threat", esercitazione su scenari reali con telemetria avanzata e analisi real-time delle strategie di detection e mitigazione. Conseguimento delle certificazioni FIRST e Trusted Introducer per l'accreditamento del CERT nelle community internazionali di Incident Response. Partecipazione come speaker a eventi internazionali di settore e promozione di gruppi di lavoro inter-CERT per la condivisione strutturata delle informazioni.
Sul fronte della Security Awareness, progettazione e delivery di un programma formativo aziendale sulla prevenzione delle frodi informatiche — Business Email Compromise, Social Engineering, elicitazione — con materiale didattico multimediale, segmentazione per famiglia professionale e misurazione del livello di consapevolezza pre/post training. Formazione dei formatori con sessioni di tutoring e coaching. Nella gestione del personale tecnico, mappatura delle competenze mediante colloqui individuali, definizione di piani di formazione e certificazione e revisione dei flussi operativi con approccio bottom-up, coinvolgendo direttamente gli analisti nella ridefinizione di procedure e workflow.

Competenze specifiche:

- Security Operations & Incident Response SOC/CERT design e gestione operativa H24, DFIR, Threat Hunting, Cyber Threat Intelligence, SIEM/SOAR tuning e sviluppo use case, Vulnerability Management, Malware Analysis, Red/Purple Team.
- Digital Forensics Analisi forense di endpoint e memorie digitali, scripting su EnCase, acquisizione e preservazione delle evidenze digitali (catena di custodia), memory forensics.
- Cyber Threat Intelligence Gestione del ciclo vitale dell'intelligence, piattaforme MISP/OpenCTI (IoC/IoA in formato STIX/TAXII), analisi TTP con Diamond Model e Cyber Kill Chain, OSINT e Digital Risk Protection.
- Security Awareness & Human Risk Progettazione programmi di Awareness e Behavior Change, Phishing Simulation, sviluppo contenuti formativi multimediali, misurazione Human Risk Score.
- People & Process Management Gestione di team tecnici distribuiti, piani di formazione e certificazione, ottimizzazione di procedure operative e workflow inter-team.

Ordine dei Giornalisti Roma, Italia

Pubblicista

30/01/2014 – Attuale

- Key note speaker
- Saggista
- Divulgatore
- Trainer A.I.
- Formatore

Mnistero della Giustizia Roma, Italia

Consulente tecnico

05/2001 – 06/2014

CTU per il Tribunale e la Procura della Repubblica per l'esperimento di accertamenti tecnici di tipo information forensics

Italia

Consulente tecnico per indagini difensive

06/2013 – Attuale

Consulenza tecnica nell'ambito delle indagini difensive in tema di information forensics

Guardia di Finanza Roma, Italia

Maresciallo

17/11/1997 – 14/06/2014

Ispettore in servizio presso i Reparti Speciali del Corpo della Guardia di Finanza:

- Coordinamento e partecipazione ad attività operative di polizia giudiziaria e tributaria per la repressione di frodi e la gestione di incidenti di sicurezza informatica.
- Analisi su fonti aperte nell'ambito della gestione di segnalazioni per operazioni sospette e sviluppo di sistemi informativi valutari.
- Comando presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA/DigitPA), con incarichi di analista e consulente per la sicurezza informatica, inclusa la gestione di incidenti di sicurezza.
- Analisi forense di dispositivi digitali nell'ambito di indagini giudiziarie relative a frodi e illeciti economico-finanziari.
- Produzione di report investigativi e strategici attraverso l'analisi di dati provenienti da fonti aperte e istituzionali per supportare indagini di polizia tributaria e giudiziaria.

Competenze specifiche

- Cybersecurity e Incident Response: Gestione di incidenti di sicurezza informatica e mitigazione dei rischi.
- Open Source Intelligence (OSINT): Analisi avanzata di dati da fonti aperte per finalità investigative.
- Analisi Forense Digitale: Esperienza nell'acquisizione e analisi di prove digitali per supportare indagini giudiziarie.
- Investigazioni Tecnologiche e Sicurezza Pubblica: Supporto tecnico-operativo per la repressione di frodi e crimini informatici.

ISTRUZIONE E FORMAZIONE

07/02/2025 – 26/02/2026 Roma, Italia

Master 2 livello in Scienze Forensi Università degli Studi di Roma LA SAPIENZA

- **Security & Cyber:** Gestione direttiva della sicurezza, contrasto alla criminalità informatica, tutela della privacy e infrastrutture critiche.
- **Intelligence:** Pianificazione di strategie di intelligence aziendale, metodologie investigative in ambiente tecnologico e analisi del terrorismo/criminalità organizzata.
- **Investigazione e Forensics:** Indagini difensive, analisi della scena del crimine, criminologia (criminogenesi e criminodinamica), criminalistica e tecniche di indagine (Genetica, Balistica, Tossicologia, grafologia).
- **Criminologia e Giurisprudenza:** Sociologia criminale, diritto processuale penale, psicologia giuridica e criminal profiling.

Discussione della tesi in: "**Criminologia dell'insider threat: profili d'autore, indicatori di rischio e investigazione forense degli incidenti informatici**"

Livello EQF Livello 8 EQF

06/03/2025 – 21/01/2026 Novredate, Italia

Master di 1 livello in Management e Cybersecurity Università degli Studi eCampus

Percorso accademico di 1.500 ore focalizzato sulla governance del rischio e sulla protezione degli asset digitali in contesti aziendali complessi. La formazione ha coperto ambiti critici quali il Risk Management, la Cloud Security e la Cyber threat Intelligence, con un approccio volto a integrare la sicurezza informatica nei processi decisionali di business.

Discussione della tesi in: "**Algoritmi contro le minacce: l'integrazione dell'Intelligenza Artificiale nel Risk Management**

della Cybersecurity"

Livello EQF Livello 7 EQF

03/02/2025 – 17/11/2025 Roma, Italia

Corso di perfezionamento e aggiornamento professionale in Security Manager Università degli Studi Niccolò Cusano

Percorso di alta formazione multidisciplinare progettato in conformità ai requisiti della norma **UNI 10459 (Professionista della Security)**, volto a consolidare le competenze necessarie per la gestione integrata della sicurezza aziendale.
Il programma ha approfondito i pilastri della governance e della resilienza organizzativa:

- **Security Risk Management:** Analisi, quantificazione e valutazione dei rischi di origine criminosa e ambientale attraverso l'applicazione di metodologie e norme tecniche di settore.
- **Legal & Compliance:** Studio del quadro normativo su Privacy, infrastrutture critiche, crimine informatico e indagini difensive, con focus sui processi di intelligence e due diligence.
- **Management & Operations:** Elementi di economia aziendale e controllo di gestione applicati alla security, coordinamento della continuità operativa (**Business Continuity**) e gestione delle crisi.
- **Leadership & Human Factor:** Tecniche di comunicazione strategica, gestione delle Risorse Unite e psicologia delle masse per il coordinamento dei servizi di sicurezza integrata.

Discussione della tesi in: "**Sinapsi d'impresa: un grafo organizzativo basato su I.A. per il Cyber Risk Management**"

Livello EQF Livello 7 EQF

31/10/2023 – 05/12/2024 Roma, Italia

Laurea Magistrale in Scienze dell'Economia, corso di studi in e-commerce e digital management Università degli Studi E-Campus

Il percorso accademico è orientata al governo della **Digital Transformation** ed alla gestione di organizzazioni ad alta intensità tecnologica, focalizzandosi sui seguenti pilastri:

- **Governance e Strategia Digitale:** Sviluppo di modelli di business per l'economia digitale e gestione del cambiamento organizzativo verso processi nativamente digitali.
- **Gestione del Rischio e Prevenzione Frodi:** Studio delle tecniche di identificazione e mitigazione delle minacce finanziarie e operative, con particolare attenzione alla protezione del patrimonio aziendale in ecosistemi e-commerce.
- **Quadro Normativo e Compliance:** Analisi approfondita della disciplina giuridica dei mercati digitali, con focus su **Cyber Resilience Act (CRA)**, **NIS2** e tutela della privacy.
- **Analisi Quantitativa Data-Driven:** Utilizzo di indicatori economici e statistici per supportare decisioni manageriali basate sui dati e sul monitoraggio delle performance aziendali.

Tesi di Laurea Magistrale: *"Cyber Resilience: un vantaggio competitivo nell'economia digitale".* L'obiettivo della ricerca è il passaggio dalla cybersecurity tradizionale (difesa) alla **Cyber Resilienza** (capacità di adattamento e recupero) con specifico focus sull'integrazione dell'**Intelligenza Artificiale (AI)** e dell'**IoT** per la rilevazione proattiva delle anomalie e la risposta automatizzata agli incident con particolare riferimento al concetto di **"Antif ragilità"** (capacità di rinforzarsi durante le crisi) e studio di casi reali.

Sito Internet www.uniecampus.it | **Livello EQF** Livello 8 EQF

11/11/2022 – 11/11/2023 Como, Italia

Corso di Alta Formazione in Economia Università E-Campus

Sito Internet www.uniecampus.it | **Livello EQF** Livello 7 EQF

2023 – 2023 Roma, Italia

ICDL Full Standard Accredia

Sito Internet https://services-accredia.isipdev.com/fpsearch/accredia_professionalmask_remote.jsp?ID_LINK=1749&area=310&PROFESSIONAL_SEARCH_MASK_ODC=&PROFESSIONAL_SEARCH_MASK_SURNAME=&PROFESSIONAL_SE

2022 – 2022 Virginia, Stati Uniti

Forensic Accounting and Fraud Examination West Virginia University

Sito Internet https://coursera.org/share/bc5cda976aea46782c1009005ae90af8 | **Livello EQF** Livello 5 EQF

25/02/2022 Online, Stati Uniti

IBM Cybersecurity Analyst IBM

Sito Internet https://www.coursera.org/account/accomplishments/professional-cert/NJ6XS7QJUPXT | **Livello EQF** Livello 5 EQF

22/02/2022 On-line, Stati Uniti

Hardware Security University of Maryland, College Park

Sito Internet https://www.coursera.org/account/accomplishments/certificate/98C7RJ7YVDJN

02/02/2022 On-line, Stati Uniti

Building a Cybersecurity Awareness Program: Phishing Simulations LinkedIn

Sito Internet https://www.linkedin.com/learning/certificates/2656abab0cfd66b450adec4d2b08fe9627b6677ced68ab41dcf2e66559eeaa3f | **Livello EQF** Livello 6 EQF

02/02/2022 On-line, Stati Uniti

Creating a Cybersecurity Awareness Program LinkedIn

Sito Internet https://www.linkedin.com/learning/certificates/ac5583fe1e91952a868bfa4fc43f6ee0e4ddb145dc60b4329f0f8d6c836d7734 | **Livello EQF** Livello 5 EQF

09/02/2022 On-line, Stati Uniti

Cryptography University of Maryland, College Park

Sito Internet www.coursera.org/account/accomplishments/verify/9DKUT7W43XD5?utm_source=link&utm_medium=certificate&utm_content=cert_image&utm_campaign=pdf_header_button&utm_product=course

07/02/2022 On-line, Stati Uniti

Software Security University of Maryland

Sito Internet https://www.coursera.org/account/accomplishments/verify/WBT236AJKQWQ?utm_source=link&utm_medium=certificate&utm_content=cert_image&utm_campaign=sharing_cta&utm_product=course | **Livello EQF** Livello 5 EQF

03/02/2022 On-line, Stati Uniti

Usable Security University of Maryland

Sito Internet https://www.coursera.org/account/accomplishments/certificate/FMRRPK3AEN5F | **Livello EQF** Livello 5 EQF

02/02/2022 On-line, Stati Uniti

Implementing an Information Security Program LinkedIn

Sito Internet https://www.linkedin.com/learning/certificates/295d468f4ed04b4e81041cb8e36e9815338b2e7d265aa532dc7792f2b5346857?trk=share_certificate | **Livello EQF** Livello 5 EQF

2022 – 2022 Roma, Italia

Data journalism: Come trovare, rappresentare, raccontare i dati per fare informazione Ordine Nazionale dei Giornalisti

Sito Internet www.odg.roma.it | **Livello EQF** Livello 5 EQF

2019 – 2019 Roma, Italia

Constructive Journalism Ordine Nazionale dei Giornalisti

Sito Internet www.odg.roma.it | **Livello EQF** Livello 5 EQF

2019 – 2019 Roma, Italia

Tecniche di giornalismo investigativo Ordine Nazionale dei Giornalisti

Sito Internet www.odg.roma.it | **Livello EQF** Livello 5 EQF

05/12/2019 On-line, Stati Uniti

IT Security: Defense against the digital dark arts Google

Sito Internet https://www.coursera.org/account/accomplishments/certificate/4B4ERPWZZPZZ?utm_medium=certificate&utm_source=link&utm_campaign=copybutton_certificate

2019 – 2019 Boulder, Stati Uniti

Graphic Design University of Colorado Boulder

Sito Internet https://www.coursera.org/account/accomplishments/certificate/Y5GUM99HVS76?utm_medium=certificate&utm_source=link&utm_campaign=copybutton_certificate | **Livello EQF** Livello 5 EQF

19/11/2018 – 23/11/2018 London, Regno Unito

SANS SECURITY AWARENESS: How to build, Maintain, and Measure a Mature Awareness Program SANS

Sito Internet www.sans.com | **Campo di studio** Specialized Knowledge and Application | **Livello EQF** Livello 6 EQF | **Tipo di crediti** CPE | **Numero di crediti** 12

2018 – 2018 Roma, Italia

Il giornalismo dei dati Ordine Nazionale dei Giornalisti

Sito Internet www.odg.roma.it | **Livello EQF** Livello 5 EQF

10/2018 – 10/2018 Houston, Stati Uniti

MGT517 - Managing Security Operations: detection, response, and intelligence SANS

Sito Internet www.sans.com | **Livello EQF** Livello 7 EQF

2017 – 2017 Roma, Italia

Strumenti di verifica delle notizie e contrasto alle fake news Ordine dei Giornalisti del Lazio

Sito Internet www.odg.roma.it | **Livello EQF** Livello 6 EQF

2016 – 2016 San Diego, Stati Uniti

Information Design UC San Diego

Sito Internet https://www.coursera.org/account/accomplishments/verify/J8Z85EC5RT2Y | **Livello EQF** Livello 5 EQF

2016 – 2016 Stati Uniti

Executive Data Science Specialization The Johns Hopkins University

Sito Internet https://www.coursera.org/account/accomplishments/specialization/VH26U9ZM8Z8H | **Livello EQF** Livello 5 EQF

12/09/2016 On-line, Stati Uniti

Executive Data Science Executive Data Science

Sito Internet https://www.coursera.org/account/accomplishments/specialization/VH26U9ZM8Z8H

2015 – 2015 Roma, Italia

Corso di formazione e aggiornamento professionale sul fenomeno del "Social Engineering Leonardo S.p.A.

Sito Internet www.leoanrdo.com | **Livello EQF** Livello 5 EQF

2015 – 2015 Roma, Italia

Corso di specializzazione in Open Source Intelligence Janes

Sito Internet https://www.janes.com | **Livello EQF** Livello 5 EQF

2015 – 2015 Stati Uniti

Data Visualization University of Illinois at Urbana-Champaign

Sito Internet https://www.coursera.org/account/accomplishments/verify/EJEJT43M4P | **Livello EQF** Livello 5 EQF

2012 – 2012 Roma, Italia

Corso di qualificazione in Open Source Intelligence (OSINT) Guardia di Finanza - Scuola Superiore di Polizia Tributaria

Sito Internet www.gdf.gov.it | **Livello EQF** Livello 5 EQF

2010 – 2010 Roma, Italia

Certificazione nell'uso del software forense EnCase della Guidance Software "Professional development and training" Agid

Sito Internet www.agid.gov.it | **Livello EQF** Livello 5 EQF

2010 – 2010 Roma, Italia

Corso di aggiornamento in malware analysis and incident handling Symantec

Sito Internet www.symantec.com | **Livello EQF** Livello 5 EQF

2009 – 2009 Roma, Italia

Corso di aggiornamento in Incident handling and response Symantec

Sito Internet www.symantec.com | **Livello EQF** Livello 5 EQF

2006 – 2006 Roma, Italia

Certified Ethical Hacker Technology transfer

Sito Internet https://technologytransfer.it/it/technology-transfer-2/ | **Livello EQF** Livello 5 EQF

2005 – 2005 Roma, Italia

Antihacking Class Techonology Transfer

Sito Internet https://technologytransfer.it/it/technology-transfer-2/ | **Livello EQF** Livello 5 EQF

2004 – 2004 Roma, Italia

Network Investigations Techinology Transfer

Sito Internet https://technologytransfer.it/it/technology-transfer-2/ | **Livello EQF** Livello 5 EQF

01/01/2003 – 01/01/2005 Bologna, Italia

Laurea in Economia Università degli Studi di Bologna ALMA MATER STUDIORUM

Sito Internet www.unibo.it | **Livello EQF** Livello 6 EQF

01/2002 – 06/2002 Roma, Italia

Corso di Specializzazione in Ricerca Investigativa e Anticrime Tecnologico Luiss Business School

Sito Internet www.luissbusinessschool.it | **Livello EQF** Livello 6 EQF

01/2003 – 06/2003 L'Aquila, Italia

Corso di specializzazione "Le reti telefoniche fisse e mobili: aspetti relativi alle frodi e alle intercettazioni" Telecom Italia Learning Services presso la Scuola Reiss Romoli

Sito Internet www.reissromoli.it | **Livello EQF** Livello 6 EQF

2001 – 2001 Roma, Italia

Digital Forensic and Incident response Technology transfer

Sito Internet https://technologytransfer.it/it/technology-transfer-2/ | **Livello EQF** Livello 5 EQF

1995 – 1995 Latina, Italia

Programmatore C e C++ Regione Lazio

Livello EQF Livello 6 EQF

1995 – 1995 Latina, Italia

Office Automation Regione Lazio

Livello EQF Livello 6 EQF

COMPETENZE LINGUISTICHE

LINGUA MADRE: italiano

Altre lingue:

inglese

Ascolto B2	**Lettura** B2
Scrittura B2	

Livelli: A1 e A2: Livello elementare B1 e B2: Livello intermedio C1 e C2: Livello avanzato

ONORIFICENZE E RICONOSCIMENTI

08/11/2019 Presidente della Repubblica Italiana

Cavaliere della Repubblica

Il dott. Antonio Rossi si distingue come una figura di spicco per il suo profondo senso civico e la dedizione alla valorizzazione culturale e sociale di Pontinia. Le sue iniziative innovative hanno contribuito significativamente a promuovere il territorio, lasciando un'impronta unica e duratura. Tra i progetti più significativi si annovera la realizzazione di un'esposizione di edifici storici in LEGO presso il Museo dell'Agro Pontino, che ha saputo valorizzare l'architettura razionalista tipica del nucleo fondativo della città. Questo progetto, apprezzato a livello locale e regionale, è stato inserito nel catalogo delle "buone pratiche" della Regione Lazio, dimostrando la capacità di coniugare creatività, educazione e coinvolgimento delle giovani generazioni.

La spinta verso l'innovazione si è manifestata anche nell'introduzione di tecnologie all'avanguardia, come l'uso dei QR Code per fornire informazioni storiche sugli edifici più rappresentativi della città. Grazie a questa iniziativa, i visitatori e i cittadini hanno potuto trasformare i loro smartphone in vere e proprie guide turistiche, rendendo accessibile la storia di Pontinia in modo moderno e interattivo.

La capacità di networking del dott. Rossi è emersa chiaramente nel coinvolgimento di associazioni, istituzioni locali e imprenditori per la realizzazione di progetti di grande valore sociale. Tra questi si annovera la donazione di una fontana simbolica per il museo cittadino, frutto di una sinergia virtuosa tra pubblico e privato, e altre iniziative rivolte al supporto di persone con disabilità, come la donazione di mezzi e attrezzature.

Il suo contributo alla ricerca storica e accademica si è concretizzato nella pubblicazione del saggio *Agraldica*, che esplora in maniera innovativa il simbolismo araldico delle città di fondazione del Novecento. Questo studio, accolto con entusiasmo da istituzioni scolastiche e accademiche, ha permesso di riscoprire le radici identitarie di Pontinia, coniugando la tradizione con una visione moderna e accessibile.

Il dott. Rossi ha dimostrato un impegno costante nel volontariato e nella promozione della cultura, organizzando eventi teatrali e iniziative educative che hanno coinvolto in modo attivo le giovani generazioni. Ha inoltre contribuito alla sensibilizzazione sull'uso sicuro delle tecnologie attraverso rubriche giornalistiche e collaborazioni con istituzioni locali, consolidando il suo ruolo di guida e mentore per la comunità.

Con un passato nei reparti speciali della Guardia di Finanza, insignito della Croce d'Argento per anzianità di servizio e di numerosi riconoscimenti sia in ambito civile che militare, il dott. Rossi continua oggi a operare nel settore aerospaziale e della difesa, confermando il suo profilo di eccellenza professionale e personale. Per il suo instancabile impegno, le benemerenze acquisite nel campo della cultura, del volontariato e della promozione sociale, si propone il conferimento dell'onorificenza al Merito della Repubblica Italiana, come previsto dalla legge 3 marzo 1951, n. 178.

Link https://www.quirinale.it/onorificenze/ricerca

Guardia di Finanza

Encomio Solenne

Ispettore appartenente al nucleo speciale frodi telematiche forniva determinante apporto personale nell'esecuzione di una complessa indagine tecnica di polizia giudiziaria riguardante una serie di intrusioni telematiche in server istituzionali e non, perpetrate a mezzo della rete internet.
L'operazione di servizio, eseguita in coordinamento con due procure della repubblica, si concludeva con la denuncia di sei pirati informatici, di cui due minorenni, e la conseguente condanna definitiva dei quattro maggiorenni, nonché con il sequestro di un ingente quantitativo di materiale informatico reperito nel corso di nove perquisizioni locali effettuate.
La brillante attività investigativa riscuoteva vasta eco sulla stampa e sulle emittenti radiotelevisive a diffusione nazionale e internazionale, contribuendo in tal modo ad accrescere notevolmente il prestigio e l'immagine del Corpo.

26/02/2003 Guardia di Finanza

Elogio

Ispettore addetto alla prima Sezione del Gruppo Anticrimine Tecnologico del Nucleo Speciale Investigativo, animato da particolare impegno e costante perseveranza nell'esecuzione dei compiti assegnati, si distingueva per l'incondizionata dedizione ed il rilevante spirito di iniziativa, evidenziando solide qualità professionali nel prestare determinante supporto alle articolazioni operative nonché agli altri Reparti del Corpo. L'Ispettore, inoltre, dimostrava ottime capacità nell'affrontare le difficoltà conseguenti all'attività di Polizia Giudiziaria svolta a contrasto della criminalità informatica, quale espressione dei nuovi scenari operativi del Corpo e garantiva, costantemente, prezioso ausilio alle SS.GG. nella definizione delle metodologie operative e delle soluzioni investigative, riscuotendo anche l'apprezzamento delle Autorità Giudiziarie deleganti.

24/01/2002 United States Naval Criminal Investigative Service

Certificate of Appreciation

United States
Naval Criminal Investigative Services
Certificate of Appreciation
is presented to
Mar. Antonio ROSSI
GAT, Guardia di Finanza
for
outstanding assistance to the United States Government in identifying and arresting members of the "hi Tech Hate" hacker group, who systematically broke into over 200 servers throughout the United States.
Congratulations ad a job well done.

PUBBLICAZIONI

2021

HACK IN ART

Hack in Art is my suggestive retrospective to explore, join and understand cybersecurity abstract concepts, using classic and modern artwork, sculptures, and literature. Yes, it is possible!
The concept book involves the reader also in the design of the cover according to the answers of specially crafted sentences according to the book theme using a color scheme and pixel matrix to reproduce an artwork.
This is my original book to try another approach to learning cyber security tactics and techniques for Managing Directors, Executives.
The printed version of this particular book has an elegant layout design, drawn by me, and it is also a nice gift and original gadget related to cyber security domains.

Antonio ROSSI

Link https://www.antoniorossi.eu/Publications.html

2022

ULYSSES: THE FIRST HACKER

My social engineering training course about the human factor in the cyber threats pattern attack: Ulysses the first hacker. According to the Cyber Kill Chain framework, the human factor is leveraged by attackers in the reconnaissance and delivery attack phases: this means that frequently a successful attack is caused due to the lack of awareness by the end-user but also to the wrong posture of the developer and the assessment process to delivery in production hardware and software. Also, procedures and policies could be exploited by an attacker because they could contain unusable tools creating an elusive phenomenon for the user who wants to work and does not run a click-marathon authenticating through multiple security systems!
So in my vision, the role of the human factor in cyber security attacks is not limited to the end-user, but also the security and IT department when putting in place new technologies keeping in mind consultants and the suppliers.
Usually, every single department in the organization seems to run for its achievement: the result is each department is compliant with budget and requirements, but in the overall view the picture changes highlighting cracks that will be easily used by the attacker for social engineering activities against the people of the targeted organization. Be aware!

Antonio ROSSI

2020

MALWARE ANALYSIS

This is my info-design created to explain a new version of Turla's Penquin malware capabilities based on the MALWARE TECHNICAL INSIGHT report by Leonardo's Cyber & Security Division.
The visual approach takes an overview of malware attack patterns and features based on an original aggregated view of the MITRE Attack Matrix TTPs and the Cyber Kill Chain framework.

Antonio Rossi

2019

Next Generation CERTs

A business-aligned and adaptive Cyber Defence capabilities, enabled by a clear internal context knowledge and by the Cyber Threat Intelligence, is the target to move towards to counter face the new challenging and dynamic cyber threats. In an asymmetric scenario, like cybersecurity issues, trusted and skilled people, that perform process and use technologies, is critical factors in developing, implement, and handle cyber defense activities and projects. The definition of a Cyber Defence maturity model allows measuring the effectiveness and efficiency of this new approach.

NATO Science for Peace and Security Series - D: Information and Communication Security

Link https://ebooks.iospress.nl/volumearticle/52880?_gl=1*7tl9xs*_up*MQ..*_ga*NDEyNjk5NTQ5LjE3MzQ5NDYwMzg.*_ga_6N3Q0141SM*MTczNDk0NjAzNy4xLjAuMTczNDk0NjAzNy4wLjAuMA..

2015

Agraldica: l'araldica civica nelle città di fondazione dell'Agro Pontino

Quali sono i simboli delle città fondate in Agro Pontino negli anni 30 del Novecento? A quale tradizione sono ispirati? Cosa rappresentano? Come sono cambiati nel corso del tempo? Queste sono solo alcune delle domande che trovano risposta in questo saggio rivelando curiosità ed avvicinando il lettore all'Araldica civica con una introduzione che parte dalla quotidianità per far comprendere la valenza e la portata dei simboli che ci circondano. Rispetto alla ricerca storica, quella di tipo araldico non è stata ancora considerata quale utile strumento per la comprensione delle città di Latina, Aprilia ed i comuni di Sabaudia e Pontinia. Il saggio intende colmare questa lacuna offrendo una nuova prospettiva, analizzando la dimensione simbolica espressa negli stemmi araldici di questi centri concepiti ex novo, secondo un preciso progetto politico, sorti in un ambiente creato artificialmente, orfani - ab origine - di tradizioni e popolazioni autoctone.

Antonio ROSSI

Link www.agraldica.it

2018

IoC DATA MODEL

My data visualization about the Indicators of Compromise (IoC) Data Model. The data model was developed with other companies and government agencies in Italy to make actionable and usable taxonomy of an IoC based on MISP syntax rules. The goal was to share IoC within the community using a common data model to identify and enrich IoC for producers and consumers. I have designed this poster

to explain the taxonomy adopted to share IoC referring to other frameworks used in the security and cyber-security domains.

Antonio Rossi

LAVORI CREATIVI

2019 – 2019

Hacker Attack

I introduced gamification on the topic of cybersecurity by restoring and converting an old electromechanical pinball machine. In this mi idea and realization, the ball represents the cyber threat that enters the playing field, which represents the corporate network, through various inputs labeled e-mail, USB devices, mobile apps, cloud, suppliers, etc. The ball will inevitably fall (data breach) following the cyber kill chain; the slingshot (which represents the automated detection and response capabilities) will reject the threat. The bumpers make the attack pattern unpredictable by representing the lateral movements of the attacker. The player is ideally the incident responder who, through the flipper bat, rejects the cyber threat, the ball, away from the data breach (out hole) by engaging other teams to support the management of the incident by increasing the score. The player who holds the ball the longest in play wins. The insider threat as well as the zero-day vulnerabilities are represented by the out lanes where it is very difficult to prevent the ball from ending up in it, just like in the real management of a security incident.

Link https://www.antoniorossi.eu/Designs.html

2015 – 2016

ART ATTACK!

During my job experience, in every role and position, I have supported activities and projects creating something new, and disruptive with a low-cost budget, effort, and time. For example, to improve cyber security awareness I create a self-made bi-pyramid design by me with a cybersecurity message on each face to get a correct posture at the desktop! Practical and maker approaches are applied to abstract concepts to update our mindset against cyber threats and information security risks. The gadget was assembled during my training course to better involve attendees according to my idea of training and teaching. Another example is my cover of the "the answer's book" by Carol Bolt. This idea was designed by me to make irony about managing some cybersecurity issues in training classrooms. A creative and disruptive approach to teaching and sharing experiences focusing on epic fails and mistakes! The joke is: make a question about a decision to assume about cyber security countermeasures, browse randomly the book's page without see and when you are ready, stop browsing and read something like this: "Yes", "No", "try again", "keep it" and so on :-)

2016 – 2016

MY LEGO DESIGNS

My Lego design about the Italian Civilization Building placed in Rome, EUR neighbor: cultural marketing initiative to promote Italian rationalism architecture. Other my Lego creations are exposed in the Pontine Marshes Museum in Pontinia and earned an award as best practices to promote history, and involve people in discovering architecture to create aware citizens.

Link https://www.archilovers.com/projects/308030/lego-moc-palazzo-della-civiltà-italiana.html

2018 – 2018

My personal tribute to Leonardo's company: 70 years since foundation

The concept of the design is centered on the new name of the company: Leonardo. So I reproduced the machines designed by the Italian genius of the 500 and how those projects and intuitions, centuries later, were produced by the Italian company that bears his name. However, I have designed a specially crafted version of the "Vitruvian's man" on the right side: I introduce the wheel of gear as the symbol of man's ingenuity. The sections of the circumference bear signs representing the Fibonacci sequence and the sequence of prime numbers. This section of the drawing is completed by Leonardo's quotation: "knowledge is the daughter of experience". Furthermore, the whole drawing expresses the golden ratio of the segment as well as the division of the two scenes represented in the relationship between width and height. In the lower part of the design, I represented the evolution of the company logo and name from the date of foundation. The design is laser-printed on a plexiglass frame and mounted on a wood base with an integrated led strip so all the artwork became a lamp when it is powered on.

CONFERENZE E SEMINARI

18/11/2019 – 19/11/2019 London

European Security Awareness Summit 2019

Led the design and implementation of a cybersecurity awareness program aimed at fostering a culture of security within the organization. The initiative involved analyzing key vulnerabilities to tailor training content that was both engaging and effective. A creative approach was adopted, integrating interactive simulations and real-world examples to ensure practical learning outcomes.
The program emphasized continuous improvement through regular feedback and updates, aligning with the latest cybersecurity challenges. This effort not only reduced human-related cyber risks but also created a deeper understanding of shared responsibility for cybersecurity across all organizational levels.
The program was presented at a professional summit, showcasing its innovative approach and highlighting its role in strengthening organizational resilience.

23/06/2018 – 30/06/2018 Kuala Lumpur

30 FIRST ANNUAL CONFERENCE

Partecipazione alla 30 edizione del meeting annuale del Forum Incident Response Team con uno speech interattivo, che ha coinvolto la platea in stile CTF: è stato illustrato un incidente di sicurezza informatica reale causato da un attacco di tipo malvertising. Nel link sono disponibili le slide in formato PDF della sessione dove seguendo il framework NIST sono state illustrate tutte le fasi della gestione dell'incidente dalla detection al lesson Learned.
Oltre allo speech, nella conferenza sono stato anche moderatore di una round table sull'orchestration e sui SOAR
.

Link https://www.first.org/conference/2018/program#pmalvertising-an-italian-tale

22/05/2018 – 23/05/2018 Milano

Banche e Sicurezza

Nella sessione dedicata alla cyber security del convegno Banche e Sicurezza ho tenuto uno speech dal titolo "L'approccio [col]laterale alla cyber threat intelligence ed alla condivisione delle informazioni del CERT di Leonardo" utilizzando come slide solo fumetti per illustrare concetti e coinvolgere la platea.

Link https://bancaforte.it/folder/dossierpage/banche-e-sicurezza-2018-11680

12/05/2017 – 16/06/2017 Puerto Rico

29ª Conferenza Annuale del Forum of Incident Response and Security Teams (FIRST), intitolata "Fighting Pirates and Privateers",

29/02/2016 – 04/03/2016 San Francisco

RSA CONFERENCE

PROGETTI

2018 – ATTUALE

Cybersecurity Academy

Progettazione del concept della Cyber Academy per l'erogazione di corsi di formazione e programmi di awareness sui temi della Cyber & Information Scuriti, Digital Transformation, cultura della sicurezza, sia verso il Gruppo Leonardo, atteso il precedente incarico, che il mercato. Proposizione del business plan, del modello di funzionamento e del programma dell'offerta formativa. L'attività, svolta a 360 gradi, ha interessato il design degli spazi della Cyber Academy concepiti in funzione dell'idea di erogazione dei corsi, dunque non solo sul cosa insegnare ma anche sul come, creando ambienti ad hoc ed in linea con il concept ideato (gamification, simulazione di scenari di attacco e difesa - red, blu e purple team -, cyber security contest, bookshop).

Link https://cybersecurity.leonardo.com/it/

2016 – ATTUALE

Cybershield: il contest di Cyber & information security

L'esercitazione, a cadenza biennale, prevede la partecipazione a squadre per misurare la capacità di risolvere l'incidente di sicurezza simulato, valutando l'efficacia e l'efficenza delle strategie di analisi e di contenimento dell'incidente, il rispetto delle procedure interne all'organizzazione e degli adempimenti normativi previsti (es. GDPR, NISt, ecc).

L'esercitazione è articolata come una sorta di caccia al tesoro: partendo da un indizio iniziale, come la segnalazione di un evento di sicurezza, le squadre dovranno risolvere i successivi indizi che troveranno nel corso dell'analisi. Il contest è dedicato ai team di risposta degli incidenti (CERT) che, usando gli strumenti tipici (es. SIEM, TIP, EDR, ecc.), dovranno individuare le evidenze, disseminate nei log, sul web e nelle immagini forensi fornite, impiegando i tool ritenuti più idonei. Tutti i dati sono prodotti da appliance reali in formato raw per consentire ai team di importarli nei propri strumenti di analisi o impiegare quelli open source disponibili nella piattaforma di scoring dell'esercitazione. Dall'avvio dell'esercitazione decorre anche il tempo e quando si ritiene di aver indivuduato la risposta corretta, l'invio nella piattaforma di scoring misura il tempo: vince il team che nel minor tempo risolve l'incidente di sicurezza. Per rendere più accessibile il contest a team con livelli di maturità diversi, sono previsti dei suggerimenti che comportano delle penalità sul punteggio. Oltre ai player è prevista anche un'altra tipologia di partecipanti: gli osservatori che possono seguire, in una vista ad hoc della piattaforma di scoring, tutta l'esercitazione grazie alla telemetria ed alle funzionalità integrate. Il contest ideato ha una vera e propria regia, che in corso dell'esercitazione può intervenire nel gioco introducendo nuovi elementi, come ad esempio, la pubblicazione sui media di un data leak o altre emergenze impreviste che consentono di valutare la c.d. readiness dei team.

Link https://www.leonardo.com/documents/15646808/16758307/ComLDO_Cyber_Shield_14_12_2018_ITA.pdf?t=1549547001439

01/2015 – ATTUALE

Security awareness and communication program

Il programma di security awareness e comunicazione proposto, adottato ed ulteriormente ampliato dal top management si è articolato in:

- progettazione e realizzazione di un'applicazione web ad uso interno della constituency e della popolazione aziendale tramite la quale interagire e veicolare contenuti interattivi formativi ed informativi sui temi di sicurezza nelle varie aree di interesse (cyber security, governance, protezione aziendale, travel security, sicurezza industriale ecc.).

- ideazione ed implementazione di speciali training formativi dove in qualità di docente e formatore ho predisposto specifico materiale sia cartaceo che multimediale oltre ad alcuni "security gadget" in base alla tipologia di fascia della popolazione aziendale di volta in volta interessata dall'attività. I temi trattati sono stati: il fattore umano quale rischio implicito e minaccia alla sicurezza connesso alle minacce di tipo cyber security, le frodi nei vari ambiti delle funzioni aziendali, focus specifici sulla protezione aziendale e sicurezza industriale.

- progettazione e realizzazione di campagne di comunicazione di sicurezza mirate a specifiche famiglie professionali profilate in base al tipo di minaccia cui possono essere esposte rispetto sia allo scenario internazionale del settore aero-spazio e difesa sia e al contesto geografico e peculiare dell'Azienda con focus specifici sui temi del social engineering, delle frodi, degli attacchi di cyber-security.

Attesa la portata dell'iniziativa ed il coinvolgimento di molte fasce della popolazione aziendale ed il forte impatto sul business l'iniziativa è stata menzionata nel bilancio di sostenibilità ed innovazione

02/2014 – 06/2014

WhoIs? - analisi domini Internet

Definizione della metodologia per l'analisi dei domini internet e realizzazione applicazione web da utilizzare per finalità info-investigative nell'ambito dell'attività di Open Source Intelligence. L'applicazione prevede a fronte dell'inserimento di una URL o indirizzo IP, tramite una interfaccia utente minimalista e di immediata fruizione, la raccolta di diverse informazioni disponibili in Rete a partire dalla consultazione e parsing dei record Whois per l'archiviazione dei dati di interesse in un database MySQL, geo-localizzazione su una mappa della server farm dove è ospitata la risorsa ricercata con le relative informazioni di contatto, la disponibilità sul medesimo indirizzo IP di altri domini con possibilità di ulteriore "sprofondamento"; screenshot della home page e visualizzazione relativa al grafo della struttura del link. L'applicazione, inoltre, consente di generare un report riepilogativo di tutte le informazioni disponibili a fronte della ricerca con un layout grafico che prevede mappe, grafici di reputazione, rating sui motori di ricerca consentendo, pertanto, di avere una uniformità nella presentazione e referenza dei dati raccolti ed organizzati creando uno standard all'interno del Corpo e verso l'Autorità Giudiziaria nel presentare non più dati ma informazioni rispetto ad una attività OSINT sui domini internet che in molti casi è uno degli spunti investigativi per inoltrare richieste o richiedere provvedimenti. L'applicazione inoltre rispetto ad un nome di dominio o indirizzo IP già oggetto in precedenza di ricerca, propone i dati disponibili nella precedente ricerca confrontandoli con quelli più recenti evidenziando così le differenze. L'applicazione una volta a regime consentirà di ricercare indirizzi e-mail, nominativi, numeri di telefono ed altre informazioni raccolte

nelle varie ricerche effettuate e che potrebbero evidenziare collegamenti o "ricorrenze" fornendo informazioni di utilità investigativa altrimenti non disponibili.

04/2011 – 06/2011

App iOS del CERT-SPC

CERT-SPC è l'applicazione del CERT (Computer Emergency Response Team): l'unità di prevenzione degli incidenti informatici del governo italiano relativa al Sistema Pubblico di Connettività (SPC). L'applicazione, completamente gratuita disponibile fino al 2013 per dispositivi iOS e Android (versione beta) consente di essere aggiornati sugli ultimi bollettini di sicurezza informatica pubblicati dal CERT-SPC. E' necessaria una connessione EDGE o UMTS per poter visualizzare i contenuti che rimangono comunque memorizzati nell'applicazione fino al successivo aggiornamento. Pertanto, anche in assenza di connettività, i dati precedentemente scaricati sono comunque consultabili.
Il CERT-SPC opera presso Digit@PA (già CNIPA - AIPA): un ente pubblico non economico con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. DigitPA svolge funzioni di natura progettuale, tecnica ed operativa, con la missione di contribuire alla creazione di valore per cittadini e imprese da parte della pubblica amministrazione, attraverso la realizzazione dell'amministrazione digitale.

Link www.dati.gov.it/content/cert-spc | http://www.appato.com/antonio-rossi/cert-spc/ | https://www.corrierecomunicazioni.it/telco/warning-del-cert-spc-sbarcano-su-iphone-e-android/

05/2009 – 09/2011

Portale Internet del Computer Emergency Response Team del Sistema Pubblico di Connettivià

Ideazione, progettazione ed implementazione del portale del Computer Emergency Response Team del sistema Pubblico di Connettività (SPC) rivolto alla constituency delle pubbliche amministrazioni centrali e locali connesse a SPC. Il portale pubblicava avvisi di sicurezza per prevenire incidenti informatici rispetto alle infrastrutture informatiche e tecnologiche in uso presso le P.A. connesse; il portale, inoltre, erogava notizie di interesse per la constituency in termini di promozione di iniziative volte alla formazione ed alle nuove tecnologie tramite un osservatorio tecnologico oltre ad essere connesso alla rete dei cert europei. L'interazione tra i membri della constituency era assicurata da un blog dedicato e dall'applicazione RIM (Risorse Incident Management) appositamente realizzata (vgs progetto). Una delle caratteristiche del portale, impostato come una e-zine, attesa la mole delle informazioni presenti di natura multimediale, consentiva di personalizzare l'interfaccia utente oltre ad ospitare un potente motore di ricerca in grado di indicizzare in maniera dinamica, oltre ai contenuti gestiti dal CMS, i file presenti nella sezione download (PDF, PPT ecc.). Un sistema di rating degli articoli pubblicati e dei commenti consentiva di definire un main-stream degli argomenti di maggiore interesse.

Link http://www.key4biz.it/Analisi-e-Dati-RecenSiti-2009-06-Certspcit-cnipa-rim-eGovernment-ministero-pubblica-amministrazione-sicurezza-network-risorse-web-sito/

04/2008 – 05/2008

RIM - Risorse per l'incident Management

Collaborazione alla realizzazione delle RIM (Risorse per Incident Management) ideate e progettate da Matteo Cavallini, implementate da Eugenio De Santis con il supporto tecnico-legale di Gabriele Cicognani. La suite di applicazioni, basate su framework open source, consentono agli operatori della community della sicurezza del Sistema Pubblico di Connettività (SPC) di gestire gli incidenti informatici e le segnalazioni provenienti dal CERT-SPC offrendo uno strumento appositamente concepito per automatizzare il flusso delle comunicazioni, offrendo una avanzata piattaforma di trouble ticketing, una sistema di condivisione file, un servizio di messaggistica e notifica ed una console di gestione e altre funzionalità appositamente concepite per dare corso al dettato tecnico normativo che regola il funzionamento della sicurezza nel Sistema Pubblico di Connettività. Le RIM erano distribuite su supporto ottico dove era presente un virtual appliance con configurazione guidata per essere installato sia su ambiente server (versione di produzione) che su workstation (versione demo). Il contributo offerto all'iniziativa è stata la realizzazione dell'interfaccia utente relativa alla dashboard di avvio delle applicazioni, del manuale utente, della grafica e della comunicazione del progetto..

RISULTATI DEL TEST DELLE COMPETENZE DIGITALI

Alfabetizzazione informatica e digitale	**AVANZATO**	Livello 6 / 6
Comunicazione e collaborazione	**AVANZATO**	Livello 6 / 6
Creazione di contenuti digitali	**AVANZATO**	Livello 6 / 6
Sicurezza	**AVANZATO**	Livello 6 / 6

Risoluzione dei problemi **AVANZATO** Livello 6 / 6

Resultati da self-assessment basati su quadro europeo delle competenze digitali 2.1

Autorizzo il trattamento dei miei dati personali presenti nel CV ai sensi dell'art. 13 d. lgs. 30 giugno 2003 n. 196 - "Codice in materia di protezione dei dati personali" e dell'art. 13 GDPR 679/16 - "Regolamento europeo sulla protezione dei dati personali".