



## Curriculum Vitae Europass

### Informazioni personali

Nome / Cognome

**Christian Catalano**

P.Iva

Telefono

E-mail

web

Cittadinanza

Italiana

### Esperienza professionale

Date

Febbraio 2018 – ad Oggi

Lavoro o posizione ricoperti

Assegnista di Ricerca in Cybersecurity CoreLab – LIIS Unisalento

Principali attività e responsabilità

Ricerca di metodologie e analisi di vulnerabilità su sistemi unix like (es. GNU/Linux, Android) Rischi, Minacce e Vulnerabilità nei sistemi e nelle piattaforme di pagamento ed interoperabilità tra sistemi.  
Identificazione ed analisi minacce, attacchi e vulnerabilità nei sistemi SCADA, ICS e sistemi IoT ad uso industriale.

Ricerca in ambito Computer Forensics e metodologie di verifica per la prevenzione di attacchi e compromissione dei sistemi oggetto di analisi

Identificazione ed analisi di tecniche di cyberwarfare e cyberguerrilla

Correlatore tesi laurea di 1° Livello in Ingegneria dell'Informazione:

- Un testbed per l'applicazione della tecnologia Blockchain in ambito IoT e industriale
- Testbed di smart contracts e Blockchain in ambito industriale
- Analisi e Test delle vulnerabilità di sistemi SCADA ed ICS
- Stato dell'arte delle tecniche forensi per il recupero di informazioni da wallet di criptovalute
- Progettazione e integrazione di un Vulnerability Management System
- Un testbed per l'applicazione della tecnologia Blockchain in ambito Web
- Progettazione e realizzazione prototipo di un sistema "Server-Side" per acquisizione forense di contenuti dal web
- Progettazione e sviluppo di Blockchain Smart Contracts
- Analisi ed implementazione di un algoritmo per la rivelazione dell'utilizzo di tecniche "Keyword Stuffing" e "Hidden Text" all'interno di siti web
- A study on Denial of Service vulnerabilities in Web Browsers

Correlatore tesi laurea di 2° Livello in Computer Engineering:

- Detecting Cryptocurrency Mining with behavior and performance combined client-side approach
- A kernel fuzzing approach for \*nix systems to extends the attack surface
- A study and an implementation of a multicore x86\_64 architectures kernel rootkit immune to rootkits detection

Paper:

Titolo: Mobile Session Fixation Attack in Micropayment Systems

Autori: Tommasi, F., Catalano, C., Fornaro, M., & Taurino, I.

Rivista: *IEEE Access*, 7, 41576-41583

<p>Tipo di attività - settore</p>	<p>Erogato corsi in cybersecurity per programma Cyberchallenge 2019 - Unisalento Secure Programming Reverse engineering Web Security <a href="https://cyberchallenge.it/venue/unislnit">https://cyberchallenge.it/venue/unislnit</a></p>
<p>Universit� del Salento - <a href="http://www.unisalento.it">www.unisalento.it</a> CoreLab - <a href="http://cpdm.unisalento.it">cpdm.unisalento.it</a> LiS Lab - <a href="http://www.liis.it">www.liis.it</a></p>	
<p>Date</p>	<p>Maggio 2010 – ad Oggi</p>
<p>Lavoro o posizione ricoperti</p>	<p>Penetration Tester - IT Security Engineer – Independent Security Researcher</p>
<p>Principali attivit� e responsabilit�</p>	<p>Esecuzione di test che simulano attacchi informatici come: Web Application Penetration Testing, Internal and External Penetration Testing, Vulnerability Assessment, Network penetration testing &amp; Vulnerability Assessment. Test di sicurezza basati sulle metodologie OWASP ed OSSTMM Scrittura report e documentazione tecnica finalizzata a valutare oggettivamente il grado di efficacia, efficienza e robustezza delle contromisure di sicurezza e delle infrastrutture tecnologiche oggetto di analisi, identificando le eventuali vulnerabilit� e fornendo le indicazioni necessarie alla stesura del piano correttivo di rientro. Scrittura di script ed exploit per la verifica di vulnerabilit� note e Oday. Attivit� di Reverse Engineering in ambito Automotive ed Industriale.</p> <p>Attivit� erogate per alcuni clienti pi� rappresentativi:</p> <p>Settore Telco: Telecom Italia e Vodafone Settore Banking: Unicredit, Banca Carige, Unipol Banca, Fideuram - Intesa Sanpaolo, Banca SAI Banca Etruria, Banca Popolare di Puglia e Basilicata Pubblica Amministrazione: Regione Emilia-Romagna, Regione Valle d'Aosta e ASL Reggio Emilia Settore Difesa: Selex, Leonardo e Fincantieri Settore Assicurazioni: Generali Settore Industriale: CNHi, Socomec, Sage Technology, EHC, Qatar Gas e Qatar Petroleum</p> <p>Redazione della documentazione tecnica per vulnerabilit� Oday, secondo linee guida OSF (Researcher Security Advisory Writing Guidelines) con CVE-ID (cve.mitre.org). Ultimo Oday pubblicato nella Hall of fame di Microsoft: Command Injection in Microsoft Outlook 365 – Novembre 2018</p> <p>Consulenze informatiche forensi, perizie informatiche ed indagini digitali nell'ambito della computer forensics. Consulenze nell'ambito della sicurezza informatica, attacchi informatici e crimini connessi Erogazione di seminari accademici, divulgativi e corsi di formazione in ambito Sicurezza Informatica, Penetration Testing ed Ethical Hacking.</p>
<p>Tipo di attivit� - settore</p>	<p>Lavori svolti per clienti in Italia ed Estero: EU, Middle East, Asia e Australia</p>
<p>Lavoro o posizione ricoperti</p>	<p>Lavoro svolto per diversi clienti che operano nei settori, contratti coperti da NDA: Government - Banking &amp; Financial - Telecommunications - IT Systems Integrator - Automotive – Energy and Oil</p>
<p>Date</p>	<p>Gennaio 2005 – Maggio 2010</p>
<p>Principali attivit� e responsabilit�</p>	<p>Cyber Security Engineer - Software Engineer</p> <p>Analisi e sviluppo software per diversi clienti del Gruppo Altran e per il Centro di Ricerche Motorola Electronics Torino R&amp;D. Consulenze nell'ambito della sicurezza informatica, attacchi informatici e crimini connessi Scrittura report e documentazione tecnica finalizzata a valutare oggettivamente il grado di efficacia, efficienza e robustezza delle contromisure di sicurezza e delle infrastrutture tecnologiche oggetto di analisi, identificando le eventuali vulnerabilit� e fornendo le indicazioni necessarie alla stesura del piano correttivo di rientro. Consulenze informatiche per valutare attacchi informatici e reale compromissione dei sistemi</p>

Tipo di attività - settore Lavoro svolto per diversi clienti che operano nei settori: Aerospazio – Telecomunicazioni – Banche e Finanza - Pubblica Amministrazione

## Istruzione e formazione

Date Giugno 2019  
Titolo Industry Digital Evolution Summer School 2019  
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione IDE19: [www.idenetwork.it](http://www.idenetwork.it)  
Corelab - Unisalento

Date Gennaio 2018  
Titolo della qualifica rilasciata Information Security Management System (ISMS) Auditor/Lead Auditor ISO/IEC 27001  
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione Aicq Sicev [www.aicqsicev.it](http://www.aicqsicev.it)

Date Settembre 2014  
Titolo Phd Summer School on Computer Security & Privacy  
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione Department of Electrical and Electronic Engineering  
University of Cagliari  
Area di Interesse Computer Security

Date Ottobre 2010  
Titolo della qualifica rilasciata Certificazione OSSTMM (OPST) Professional Security Tester  
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione ISECOM Institute For Security and Open Methodologies [www.isecom.org](http://www.isecom.org)

Date Aprile 2007  
Titolo della qualifica rilasciata Laurea Magistrale in Ingegneria Informatica (quinquennale, pre-riforma)

- Tesi di Laurea sperimentale: "Progetto e realizzazione di un sistema di Network Monitoring open source" – R&D Motorola Electronics S.p.A. - Torino.
- Relatori: Prof. Mario Baldi, Ing. Fulvio Giovanni Rizzo.

  
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy [www.polito.it](http://www.polito.it)

Date Luglio 1998  
Titolo della qualifica rilasciata Diploma di Ragioniere Programmatore  
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione Istituto Tecnico "Ing. Adriano Olivetti", Lecce

## Capacità e competenze personali

Madrelingua **Italiano**

Altra lingua

English	Understanding				Speaking				Writing	
	Listening		Reading		Spoken interaction		Spoken production			
	B2	Independent	B2	Independent	B2	Independent	B2	Independent	B2	Independent

	<p>18/01/2010 – 12/02/2010 Certificate of English presso la Embassy CES, Melbourne, Australia: corso di inglese livello "intermediate"</p> <p>2007 Certificato IELTS (International English Language Testing System) rilasciato da: University of Cambridge ESOL - Examinations (Cambridge ESOL) - British Council <a href="http://www.ielts.org">www.ielts.org</a></p>
Capacità e competenze sociali	<p>Possiedo un'ottima capacità di lavoro in gruppo, grazie ad una propensione naturale e ai progetti sviluppati in collaborazione con altri colleghi durante le mie esperienze lavorative.</p> <p>Sono in grado di relazionarmi con persone di diversa nazionalità e cultura grazie all'esperienza maturata prima al Politecnico, collaborando a progetti educativi con studenti provenienti da tutte le parti del mondo, e dopo con diverse esperienze lavorative all'estero in UAE, Qatar, Bangladesh e Australia.</p>
Capacità e competenze organizzative	<p>Sono in grado di organizzare autonomamente il lavoro, definendo priorità e assumendo responsabilità acquisite tramite le diverse esperienze professionali sopra elencate nelle quali mi è sempre stato richiesto di gestire autonomamente le diverse attività rispettando le scadenze e gli obiettivi prefissati.</p>
Capacità e competenze informatiche	<p>Durante gli anni di studio e lavoro ho maturato le seguenti conoscenze informatiche:</p> <ul style="list-style-type: none"> <li>• Sistemi Operativi: sistemi della famiglia Microsoft, O.S. della famiglia Unix (Backtrack Kali, Gentoo, Debian, RedHat SunOS/Solaris).</li> <li>• Linguaggi: C/C++, Pro*C, Java, Perl, Grails, Pascal, Assembler 8086, x86_32, x86_64, VHDL, SQL, PL\SQL Linguaggi di scripting diffusi per sistemi GNU\Linux</li> <li>• Linguaggi di modellazione: UML, Flow Chart.</li> <li>• Tools per analisi di sicurezza ed il reverse engineering(Nmap, Nessun, OpenVas, Paros Proxy, Burp, Acunetix, SoapUI, ILSpy, IDA-pro ecc..)</li> <li>• Software Tecnici: Toad, Matlab, LaTeX.</li> <li>• Buona conoscenza dei diversi tipi di attacchi informatici, tecniche hacking e metodologia per l'analisi e la gestione della sicurezza informatica aziendale.</li> </ul>
Patente	<p>Patente B</p>
<b>Ulteriori informazioni</b>	<p>Scrittura di articoli tecnici per magazine online [Hack]in(Sight) <a href="http://www.hackinsight.org">www.hackinsight.org</a>          Interesse per i servizi di Sicurezza Proattiva, Ethical Hacking e Penetration Testing          Interesse per la programmazione di sistemi Linux\Linux embedded          Interesse per il Reverse Engineering          Interesse per l'agile programming e l'extreme programming          Interesse per la lettura ed i viaggi.</p>