IMT SCUOLA ALTI STUDI LUCCA

NATIONAL PHD PROGRAMME IN "CYBERSECURITY" – XLII CYCLE

CANDIDATES ADMITTED TO THE INTERVIEW

Application ID	Project
2722083	Towards Trustworthy Confidential AI: A Cyber-Social Security Framework for Multidomain Assessment
2730942	Defending Systems and Critical Infrastructures Against AI-Enabled Cyber Threats Powered by Frontier Large Language Models
2730942	Architectures and Methods for Sovereign AI-Driven High-Assurance Cybersecurity Analysis
2732552	Threat Modelling and Mitigation Strategies for Cyber-Physical Systems
2732552	AI-Driven Integration of Cyber Threat Intelligence into Dynamic Cybersecurity Risk Assessment
2732552	Quantificazione del rischio cibernetico (Cyber Risk Quantification): metodologie e applicazioni di supporto alle decisioni aziendali
2742210	Calibrated Security Evidence for AI-Generated Code in CI/CD Pipelines
2742210	Methods and tools for the security assessment of critical information infrastructures
2742777	Calibrated Security Evidence for AI-Generated Code in CI/CD Pipelines
2742777	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2742777	AI-Driven Integration of Cyber Threat Intelligence into Dynamic Cybersecurity Risk Assessment
2744482	Boundary-Aware Testing and Fuzzing for Trustworthy AI-Enabled and Agentic Software Systems
2745828	Preventing, investigating and fighting cybercrimes: substantial and procedural issues
2745828	The governance of the cybersecurity
2746297	A Cross-Country Study of AI-Based News Reliability Assessment
2747067	Artificial intelligence for vulnerability detection and threat intelligence
2748336	Formal Verification of Cryptographic Protocols for Embedded Systems
2748336	Methods and tools for the security assessment of critical information infrastructures
2748336	Cryptographic Techniques for Verifiable Privacy Compliance
2748449	Boundary-Aware Testing and Fuzzing for Trustworthy AI-Enabled and Agentic Software Systems
2748449	A methodology for identifying and mitigating harms in complex digital ecosystems
2749535	Boundary-Aware Testing and Fuzzing for Trustworthy AI-Enabled and Agentic Software Systems
2751234	Multi-Hop Quantum Key Distribution and Post-Quantum Integration for Secure Cloud-Edge Infrastructures
2751234	Formal Verification of Cryptographic Protocols for Embedded Systems
2751861	Towards Trustworthy Confidential AI: A Cyber-Social Security Framework for Multidomain Assessment

IMT SCUOLA ALTI STUDI LUCCA

NATIONAL PHD PROGRAMME IN "CYBERSECURITY" – XLII CYCLE

CANDIDATES ADMITTED TO THE INTERVIEW

Application ID	Project
2751861	Regional CSIRTs and Cybersecurity Governance: Organizational Models and Regulatory Frameworks Under the NIS2 Directive
2754748	AI-Driven Cyber-Resilient Digital Twins for Human-Centric Industrial Cyber-Physical Systems
2755340	Formal Verification of Cryptographic Protocols for Embedded Systems
2755658	Towards Trustworthy Confidential AI: A Cyber-Social Security Framework for Multidomain Assessment
2755716	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2755774	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2755774	Calibrated Security Evidence for AI-Generated Code in CI/CD Pipelines
2755774	Artificial intelligence for vulnerability detection and threat intelligence
2756205	Cryptographic Techniques for Verifiable Privacy Compliance
2756872	Cryptographic Techniques for Verifiable Privacy Compliance
2757589	Methods and tools for the security assessment of critical information infrastructures
2758942	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2759513	Boundary-Aware Testing and Fuzzing for Trustworthy AI-Enabled and Agentic Software Systems
2759981	Artificial intelligence for vulnerability detection and threat intelligence
2760404	Quantificazione del rischio cibernetico (Cyber Risk Quantification): metodologie e applicazioni di supporto alle decisioni aziendali
2760404	AI-Driven Integration of Cyber Threat Intelligence into Dynamic Cybersecurity Risk Assessment
2760555	AI-Driven Cyber-Resilient Digital Twins for Human-Centric Industrial Cyber-Physical Systems
2760605	Quantificazione del rischio cibernetico (Cyber Risk Quantification): metodologie e applicazioni di supporto alle decisioni aziendali
2761902	Cryptographic Techniques for Verifiable Privacy Compliance
2761902	LLM-Based Multi-Modal Analysis for Security, Privacy, and Network Resilience in Mobile and Wearable Ecosystems
2763207	Preventing, investigating and fighting cybercrimes: substantial and procedural issues
2763207	Modello giuridico-operativo per la gestione degli incidenti e delle crisi cyber nello CSIRT regionale
2763207	Regional CSIRTs and Cybersecurity Governance: Organizational Models and Regulatory Frameworks Under the NIS2 Directive
2763207	The governance of the cybersecurity
2763247	The Role of Women in the History of Software Design and an Analysis of the Impact of Gender on Systems Security

IMT SCUOLA ALTI STUDI LUCCA

NATIONAL PHD PROGRAMME IN "CYBERSECURITY" – XLII CYCLE

CANDIDATES ADMITTED TO THE INTERVIEW

Application ID	Project
2763250	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2766064	The Role of Women in the History of Software Design and an Analysis of the Impact of Gender on Systems Security
2766833	AI-Driven Cyber-Resilient Digital Twins for Human-Centric Industrial Cyber-Physical Systems
2767081	Cryptographic Techniques for Verifiable Privacy Compliance
2768323	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2768482	AI-Driven Integration of Cyber Threat Intelligence into Dynamic Cybersecurity Risk Assessment
2769076	Modello giuridico-operativo per la gestione degli incidenti e delle crisi cyber nello CSIRT regionale
2769076	Regional CSIRTs and Cybersecurity Governance: Organizational Models and Regulatory Frameworks Under the NIS2 Directive
2769213	Artificial intelligence for vulnerability detection and threat intelligence
2771959	Multi-Hop Quantum Key Distribution and Post-Quantum Integration for Secure Cloud-Edge Infrastructures
2773319	Methods and tools for the security assessment of critical information infrastructures
2773319	Formal Verification of Cryptographic Protocols for Embedded Systems
2773319	Cryptographic Techniques for Verifiable Privacy Compliance
2773778	Defending Systems and Critical Infrastructures Against AI-Enabled Cyber Threats Powered by Frontier Large Language Models
2775310	A methodology for identifying and mitigating harms in complex digital ecosystems
2776453	AI-Driven Integration of Cyber Threat Intelligence into Dynamic Cybersecurity Risk Assessment
2776548	Artificial intelligence for vulnerability detection and threat intelligence
2777456	Boundary-Aware Testing and Fuzzing for Trustworthy AI-Enabled and Agentic Software Systems
2779077	Artificial intelligence for vulnerability detection and threat intelligence
2780079	Preventing, investigating and fighting cybercrimes: substantial and procedural issues
2780743	The governance of the cybersecurity
2781484	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2782050	A methodology for identifying and mitigating harms in complex digital ecosystems
2784957	Methods and tools for the security assessment of critical information infrastructures

IMT SCUOLA ALTI STUDI LUCCA

NATIONAL PHD PROGRAMME IN "CYBERSECURITY" – XLII CYCLE

CANDIDATES ADMITTED TO THE INTERVIEW

2784957	Learning under Change: Resilient Decentralized AI for Dynamic, Constrained Environments
Application ID	**Project**
2786286	Methods and tools for the security assessment of critical information infrastructures
2786286	The Role of Women in the History of Software Design and an Analysis of the Impact of Gender on Systems Security
2786473	Artificial intelligence for vulnerability detection and threat intelligence
2787691	LLM-Based Multi-Modal Analysis for Security, Privacy, and Network Resilience in Mobile and Wearable Ecosystems
2787691	Cryptographic Techniques for Verifiable Privacy Compliance
2788618	AI-Driven Cyber-Resilient Digital Twins for Human-Centric Industrial Cyber-Physical Systems
2789204	Cryptographic Techniques for Verifiable Privacy Compliance
2789204	LLM-Based Multi-Modal Analysis for Security, Privacy, and Network Resilience in Mobile and Wearable Ecosystems
2789204	AI-Driven Integration of Cyber Threat Intelligence into Dynamic Cybersecurity Risk Assessment
2789405	Boundary-Aware Testing and Fuzzing for Trustworthy AI-Enabled and Agentic Software Systems
2789496	Preventing, investigating and fighting cybercrimes: substantial and procedural issues
2789496	Modello giuridico-operativo per la gestione degli incidenti e delle crisi cyber nello CSIRT regionale
2789496	Regional CSIRTs and Cybersecurity Governance: Organizational Models and Regulatory Frameworks Under the NIS2 Directive
2789496	The governance of the cybersecurity
2789533	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2790137	Autonomous Threat Management: Integrating Graph Neural Networks and Large Language Models for Proactive Vulnerability and Malware Analysis
2790155	AI-Driven Cyber-Resilient Digital Twins for Human-Centric Industrial Cyber-Physical Systems
2790310	Cryptographic Techniques for Verifiable Privacy Compliance
2790487	Cryptographic Techniques for Verifiable Privacy Compliance
2790491	AI-Driven Cyber-Resilient Digital Twins for Human-Centric Industrial Cyber-Physical Systems
2790667	Artificial intelligence for vulnerability detection and threat intelligence
2791032	Defending Systems and Critical Infrastructures Against AI-Enabled Cyber Threats Powered by Frontier Large Language Models
2791032	Security Testing of Cyber-Physical Systems in Operational Environments
2791077	A methodology for identifying and mitigating harms in complex digital ecosystems

IMT SCUOLA ALTI STUDI LUCCA

NATIONAL PHD PROGRAMME IN "CYBERSECURITY" – XLII CYCLE

CANDIDATES ADMITTED TO THE INTERVIEW

2791217	Preventing, investigating and fighting cybercrimes: substantial and procedural issues
Application ID	**Project**
2791251	Multi-Hop Quantum Key Distribution and Post-Quantum Integration for Secure Cloud-Edge Infrastructures
2791251	Cryptographic Techniques for Verifiable Privacy Compliance
2791481	Multi-Hop Quantum Key Distribution and Post-Quantum Integration for Secure Cloud-Edge Infrastructures
2791675	Calibrated Security Evidence for AI-Generated Code in CI/CD Pipelines
2791675	Defending Systems and Critical Infrastructures Against AI-Enabled Cyber Threats Powered by Frontier Large Language Models

Lucca, 2 ottobre 2026

La responsabile del procedimento amministrativo

Dott.ssa Serena Argentieri

(f.to Serena Argentieri)