ALESSANDRO PALMA
Curriculum Vitae

Part II – Education

Type	Year	Institution	Notes (Degree, Experience,…)
PhD	2025	Sapienza University of Rome	Doctor Europeaus Cum Laude
Post-graduate studies	2020	Sapienza University of Rome	110 cum Laude
Bachelor	2018	University of Rome Tor Vergata	110/110
Licensure	2020	National qualification to practice as Engineer	Information Engineering, Section A

Part III – Appointments

III.A – Academic Appointments

Start	End	Institution	Position
2025	Now	Sapienza University of Rome	Post Doctoral Researcher
Feb 2024	Jul 2024	Télécom Sud Paris – Institute Polytechnique de Paris	Visiting research scholar
2021	2024	Sapienza University of Rome	PhD Student

III.B – Other Appointments

Start	End	Institution	Position
2020	2021	CINI Cybersecurity National Lab	Computer Engineer Research Fellow

Part IV – Teaching experience

Year	Institution	Lecture/Course
2025	National Accounting Office (Ragioneria di Stato)	Lecturer of the course on Incident and Event Management
2025	Sapienza University of Rome	Welcome and tutoring service for international students
2023-2025	Sapienza University of Rome	Seminars on “Cybersecurity Certification Process”
2022	Sapienza University of Rome	Tutor of the course “Fondamenti di Informatica”
2023	Sapienza University of Rome	Tutor of the course “Dependable Distributed Systems”

Part V - Society memberberships, Awards and Honors

Year	Title
2025	Best paper award at the 20th International Conference on Software Engineering for

	Adaptive and Self-Managing Systems
2025	ACM member
2024	Distinguished paper award runner up at the 29th European Symposium on Research in Computer Security
2024	Best paper award runner up at 19th International Conference on Availability, Reliability and Security
2020	Honour program at Sapienza University of Rome

Part VI - Funding Information [grants as PI-principal investigator or I-investigator]

Year	Title	Program	Grant value
2024	SELFIE: SELF-protection of Intelligent Environments	Bando Avvio alla ricerca	2000,00 €
2023	Automated solutions for Attack Graph generation and Cyber Risk assessment	Ph.D. Mobility Program	1000,00 €
2022	ADDIM: Automated Data Driven Incident Management	Bando Avvio alla ricerca	1830,00 €

Part VII – Academic Activities

VII.A – Research Activities

Topics	Brief Description
Autonomic cybersecurity Self-protection Self-adaptive systems	**Autonomic Cybersecurity**: Focuses on developing self-managing cybersecurity systems that can autonomously detect, analyze, and respond to threats with minimal human intervention. Research emphasizes modeling for self-protection and self-healing, while addressing challenges of trust and transparency in autonomous decision-making.
Information Security Governance Incident management Cyber risk management Security processes	**Information Security Governance (ISG)**: Enhance decision-making in organizational security strategies such as incident and risk management. Research explores quantitative methods to reduce cognitive bias and improve the reliability of ISG processes.
Threat modelling Cyber risk assessment	**Attack Graphs**: Investigates scalable models for representing multi-step cyberattacks. Research targets enhancing the scalability of attack graph generation and integrating threat intelligence to move beyond traditional infrastructure-based vulnerability models.

VII.B – Project participation

From	To	Project	Role
Nov 2024	Now	**EU EDF- EU-GUARDIAN**	**Member**

Link : https://www.eu-guardian.eu/

Brief Description: EU-GUARDIAN is the most ambitious European effort to explore Cyberspace Operations (COs) in the context of the Mosaic Warfare concept. The project aims at creating an AI-based solution that operates and automates large parts of incident management and cyber defence processes. EU-GUARDIAN focuses primarily on the ability to detect, mitigate and respond to security challenges

semi-automatically or automatically; support human operators, analysts and decision-makers at all levels; and contributing to enhance cyber situational awareness, military infrastructure resilience and protection against advanced cyber threats. **Contributions:** Alessandro Palma contributed to the design and development of data modeling for AI-based cybersecurity under different perspectives. He designed and developed an NLP-based methodology to assess cyber risks automatically leveraging explainable AI. Additionally, he designed adaptive visual interfaces to communicate to stakeholders cybersecurity emergencies considering contextual information (e.g., stress of the users, state of emergency).			
Feb 2024	Jul 2024	**EU Horizon Di-Hydro**	**Member**
Link : https://dihydro-project.eu/ Brief Description: Di-Hydro is a European-funded project committed to advancing the potential of hydropower (HP) plants and clusters in alignment with the ambitious goals of the European Green Deal and the Paris Agreement. The mission is to revolutionise the way hydropower plants operate, making them smarter, more efficient, and environmentally conscious. At Di-Hydro, the vision is to empower sustainable energy production through the development of cutting-edge digital and smart decision-making tools for hydropower plants, regardless of their digitization level, ensuring they play a pivotal role in a greener future. **Contributions:** Alessandro Palma designed, developed, and tested a novel architecture to ensure security during the HP management in IoT environments. In particular, he adopted strategies for securing data communication during HP management.			

VII.C – Supervision of MSc students

- 2025. "Design and Implementation of an Online Attack Graph Generator". Valerio Amodeo (co-supervised with Prof. Silvia Bonomi), MSc in Cybersecurity, Sapienza University of Rome
- 2025. "LLM-enhanced Attack Graph Generation for Explainable Threat Modelling of Multi-Step Attacks". Francesco Scarati (co-supervised with Prof. Silvia Bonomi), MSc in Cybersecurity, Sapienza University of Rome
- 2025. "Integrating CAPEC Attack Patterns into Privilege Escalation Assessment for Enhanced Threat Modelling". Giuseppe Cesare Zizzo (co-supervised with Prof. Simone Lenti), MSc in Cybersecurity, Sapienza University of Rome
- 2025. "An NLP-assisted framework for (semi)-automatic correlation of CVE vulnerabilities and CAPEC patterns". Andrea Ciavotta (co-supervised with Prof. Silvia Bonomi and Prof. Simone Lenti), MSc in Cybersecurity, Sapienza University of Rome
- 2025. "Enabling Human-Centric Visual Analysis and Exploration of Attack Surfaces through Progressive Attack Graphs". Claudio Cicimurri (co-supervised with Prof. Marco Angelini), MSc in Cybersecurity, Sapienza University of Rome
- 2024. "PERSEO: A Process-centric Multiple-Perspective Assessment System for the Incident Management Process". Jonathan Christof Orth (co-supervised with Prof. Marco Angelini), MSc in Cybersecurity, Sapienza University of Rome
- 2024. "Extending the STIX Communication Standard for Cyber Threat Intelligence Platforms". Philipp Eisermann (co-supervised with Prof. Joaquin Garcia-Alfaro), MSc in Informatics, Technical University of Munich
- 2024. "Design and Implementation of a Benchmark for Incident Management Process Assessment". Nicola Bartoloni (co-supervised with Prof. Marco Angelini), MSc in Cybersecurity, Sapienza University of Rome
- 2022. "A Graph-Based Model for Security Awareness Analysis". Andrea Sorrentino (co-supervised with Prof. Silvia Bonomi), MSc in Cybersecurity, Sapienza University of Rome

VII.D – Peer-review activities

International journals, external reviewer for:

- IEEE Transactions on Information Forensics & Security (TIFS)
- ACM Computing Surveys (CSUR)
- Elsevier Computer & Security (COSE)
- Elsevier Information Security and Applications (JISAS)
- Elsevier Information Sciences (INS)
- Elsevier Computer Networks (COMNET)
- ACM Transactions on Autonomous and Adaptive Systems (TAAS)
- Wiley Corporate Social Responsibility and Environmental Management (CSR)
- IOS Press Computer Security (JCS)
- Elsevier Heliyon
- MDPI Mathematics, Electronics, Energies
- IEEE Access

International conferences, external reviewer for:

- SMC 2025, International Conference on Systems, Man, and Cybernetics
- INTERACT 2025, International Conference on Human-Computer Interaction

Technical Program Committee member

- HotDiML 2025, International Workshop on Hot Topics in Distributed Machine Learning
- SAFE-ML 2025, International Workshop on Secure, Accountable, and Verifiable Machine Learning
- EXTRAAMAS 2025, International Workshop on EXplainable and TRAnsparent AI and Multi-Agent Systems
- IEEE CSR SDG 2024, Workshop on Synthetic Data Generation for a Cyber-Physical World
- EXTRAAMAS 2024, International Workshop on EXplainable and TRAnsparent AI and Multi-Agent Systems
- AVI 2024 (Poster and Demo), International Conference on Advanced Visual Interfaces
- AVI 2022 (Poster and Demo), International Conference on Advanced Visual Interfaces

VII.E – Organization of conferences and workshops

- Track Chair Leader at SAC 2026 (ASH track: Applications and Systems for Healthcare)
- Student Volunteer at EuroVIS 2022
- Student Volunteer at EuroSys 2023
- Student Volunteer at EuroVIS 2024

VII.F – Speaker at conferences

- 2025. 40th ACM/SIGAPP Symposium on Applied Computing (SAC '25)
- 2025. 9th National Conference on Cybersecurity (ITASEC’25)
- 2024. International Conference on Risks and Security of Internet and Systems (CRiSIS’24)
- 2024. 29th European Symposium on Research in Computer Security. (ESORICS’24)
- 2024. 9th International Conference on Availability, Reliability and Security (ARES '24)
- 2024. 16th International EuroVis Workshop on Visual Analytics. (EuroVA’24)

- 2023. 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'23)
- 2022. 6th National Conference on Cybersecurity (ITASEC'22)

Part VIII – Summary of Scientific Achievements

Product type	Number	Data Base	Start	End
Papers [international]	13	Scopus	2021	2025
Papers [international]	17	Google Scholar	2021	2025

Total Citations	34 (Scopus) 65 (Google Scholar)
Hirsch (H) index	4 (Scopus) 6 (Google Scholar)

Part IX– Selected Publications

List of the publications selected for the evaluation. For each publication report title, authors, reference data, journal IF (if applicable), citations, press/media release (if any).

International peer reviewed journals

- Behind the scenes of attack graphs: Vulnerable network generator for in-depth experimental evaluation of attack graph scalability. Palma, A.; and Bonomi, S. Computers & Security, 157: 104586. October 2025. **JOURNAL IF: 4.8.**
- IMPAVID: Enhancing incident management process compliance assessment with visual analytics. Palma, A.; and Angelini, M. Computers & Security, 157: 104586. October 2025. **JOURNAL IF: 2.8.**
- How to assess measurement capabilities of a security monitoring infrastructure and plan investment through a graph-based approach. Palma, A.; Sorrentino, A.; and Bonomi, S. Expert Systems with Applications, 262: 125623. March 2025. **JOURNAL IF: 7.5.**
- A compliance assessment system for Incident Management process. Palma, A.; Acitelli, G.; Marrella, A.; Bonomi, S.; and Angelini, M. Computers & Security, 146: 104070. November 2024. **JOURNAL IF: 4.8.**

International conferences and workshops

- SPARQ: A QoS-aware Framework for Mitigating Cyber Risk in Self-Protecting IoT Systems. Palma A., Hajj Hassan H., Bouloukakis G.. In The 20th International Conference on Software Engineering for Adaptive and Self-Managing Systems (SEAMS). April 2025. **Conference rank: A.**
- SHIELD: Assessing Security-by-Design in Federated Data Spaces Using Attack Graphs. Palma, A.; Papadakis, N.; Bouloukakis, G.; Garcia-Alfaro, J.; Sospetti, M.; and Magoutis, K. In Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing, of SAC '25, pages 480–489, New York, NY, USA, May 2025. Association for Computing Machinery **Conference rank: B.**
- Improving Attack Graph-Based Self-protecting Systems: A Computational Pipeline for Accuracy-Scalability Trade-off. Bonomi, S.; Cuoci, M.; Lenti, S.; and Palma, A. In Collart-Dutilleul, S.; Ouchani, S.; Cuppens, N.; and Cuppens, F., editor(s), Risks and Security of Internet and Systems, pages 525–542, Cham, 2025. Springer Nature Switzerland. **Conference rank: C.**
- It is Time To Steer: A Scalable Framework for Analysis-Driven Attack Graph Generation. Palma, A.; and Angelini, M. In Garcia-Alfaro, J.; Kozik, R.; Choraś, M.; and Katsikas, S., editor(s), Computer Security – ESORICS 2024, pages 229–250, Cham, 2024. Springer Nature Switzerland. **Conference rank: A.**
- BenchIMP: A Benchmark for Quantitative Evaluation of the Incident Management Process Assessment. Palma, A.; Bartoloni, N.; and Angelini, M. In Proceedings of the 19th International

Conference on Availability, Reliability and Security, of ARES '24, pages 1–12, New York, NY, USA, July 2024. Association for Computing Machinery. **Conference rank: B.**

- Visually Supporting the Assessment of the Incident Management Process. Palma, A.; and Angelini, M. EuroVA@EuroVIS. The Eurographics Association, 2024. **Conference rank: C.**
- A Workflow for Distributed and Resilient Attack Graph Generation. Palma, A.; and Bonomi, S. In 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S), pages 185–187, June 2023. ISSN: 2833-292X. **Conference rank: A.**
- Context-Aware Trace Alignment with Automated Planning. Acitelli, G.; Angelini, M.; Bonomi, S.; Maggi, F. M.; Marrella, A.; and Palma, A. In 2022 4th International Conference on Process Mining (ICPM), pages 104–111, October 2022. **Conference rank: B.**
- Toward a Context-Aware Methodology for Information Security Governance Assessment Validation. Angelini, M.; Bonomi, S.; Ciccotelli, C.; and Palma, A. In Abie, H.; Ranise, S.; Verderame, L.; Cambiaso, E.; Ugarelli, R.; Giunta, G.; Praça, I.; and Battisti, F., editor(s), Cyber-Physical Security for Critical Infrastructures Protection, pages 171–187, Cham, 2021. Springer International Publishing. **Conference rank: -**