

# Matteo GRECO

## Security Engineer

 [linkedin.com/in/matteogreek](https://www.linkedin.com/in/matteogreek)  [matteogreek.github.io](https://github.com/matteogreek)  
 [matgrec@gmail.com](mailto:matgrec@gmail.com)

Security Engineer with expertise in both Red and Blue Team operations. Skilled in optimizing real-time threat detection through SIEM and XDR management, leveraging threat intelligence, and executing incident response and forensic investigations. Specialized in Red Team operations, performing adversary simulation and targeted penetration testing to emulate real-world attacks and uncover exploitable vulnerabilities. Experienced trainer, delivering cybersecurity awareness to enhance defensive capabilities across teams. Previous experience at SAP included developing tools for automated vulnerability mining to find vulnerability fixes in open-source software repositories.

## PROFESSIONAL EXPERIENCE

Present November 2023	<b>Security Engineer, BE INNOVA, Italy</b> <ul style="list-style-type: none"><li>&gt; Operate within the Security Operations Center of a MSSP, leveraging SIEM platforms and XDR solutions.</li><li>&gt; Conduct incident response and digital forensics investigations to identify root causes, mitigate threats, and support remediation processes.</li><li>&gt; Contribute to the Red Team by performing vulnerability assessments, network and web application penetration testing, and Active Directory security evaluations, following OWASP and NIST testing frameworks, using both standard tools and custom scripts.</li><li>&gt; Deliver cybersecurity awareness training to client organizations promoting secure practices, focusing on attack simulation scenarios, phishing defense, NIS2, and incident handling best practices.</li><li>&gt; Mentor and support Tier 1 analysts, providing internal training on alert triage, threat correlation, and response procedures.</li></ul>
July 2023 February 2023	<b>Security Research Intern, SAP, France</b> <ul style="list-style-type: none"><li>&gt; Contributed to the development of <i>Prospector</i> (part of <i>Project-KB</i>) for finding vulnerability fixes in open-source software repositories.</li><li>&gt; Worked with Python, Redis, PostgreSQL, Docker, and GitHub Actions.</li><li>&gt; Co-authored a paper, <i>Known Vulnerabilities of Open Source Projects : Where Are the Fixes?</i>, published in IEEE S&amp;P Journal (DOI : 10.1109/MSEC.2023.3343836)</li></ul>
July 2017 May 2017	<b>Erasmus+ Internship, BIAŁYSTOK SCIENCE AND TECHNOLOGY PARK, Poland</b> <ul style="list-style-type: none"><li>&gt; Assisted System Administrators in their daily operations</li><li>&gt; Collaborated in an international environment, enhancing communication and teamwork skills.</li></ul>

## EDUCATION

2021 - 2023 University of Trento, Italy	<b>Master's Degree in Cyber Security</b> <ul style="list-style-type: none"><li>&gt; Coursework included Offensive Technologies, Cryptography, Network Security, Risk Assessment, and Security Testing.</li><li>&gt; Thesis : <i>Enhancing Prospector : Pipeline Development and Empirical Analysis of an Automated Vulnerability Fix Finder</i>. Designed and implemented automated pipelines for mining and validating vulnerability-fixing commits.</li><li>&gt; Final Mark : 110/110 cum laude</li></ul>
2018 - 2021 University of Trento, Italy	<b>Bachelor's Degree in Information Engineering and Business Organization</b> <ul style="list-style-type: none"><li>&gt; Curriculum emphasized Computer Networks, Software Engineering and Business Innovation.</li><li>&gt; Thesis : <i>Evaluation of Techniques and Tools for Network Measurement in Softwarized Networks</i>. Analyzed SDN monitoring tools, assessing performance and scalability in simulated environments.</li></ul>

## CERTIFICATIONS

**Holmes CTF 2025** - A competitive cybersecurity challenge focused on digital forensics.  
**Bitdefender Certified Technical Specialist** - Certified proficiency in managing Bitdefender solutions.  
**Flagship2 Participant** - A CyberSec4Europe simulation focused on practical SOC skills.  
**Devlympics 2021 Competitor** - A competition challenging participants in secure programming practices.