

Andrea Palmieri

email: andpalmier@gmail.com
website: andpalmier.com
location: Zurich, Switzerland
linkedin: linkedin.com/in/andpalmier
github: github.com/andpalmier

Cybersecurity specialist with experience in cybercrime investigations, threat intelligence, and information security. Skilled in analyzing and responding to cyber threats, conducting investigations, and collaborating with CERTs, cybersecurity communities, law enforcement, and cross-functional teams to mitigate emerging threats. Desiring to use analytical and research skills to protect, contain and prevent cyber security issues when the stakes are high.

KEY SKILLS

- Extensive experience in researching, analyzing, and mitigating cyber threats using tools such as Splunk, Anomali, URLscan, and YARA; with a focus on phishing, mobile malware, and fraud-related activities.
- Actively involved in national and international CERT communities, participating in collaborative efforts to fight cybercrime, sharing knowledge, and staying updated on the latest cybersecurity threats.
- Experienced in delivering presentations on cybersecurity trends and threat intelligence at industry conferences. Proficient in producing high-quality technical documentation for diverse audiences.
- Proficient in GoLang and Python with a focus on developing security tools. Notable projects include GoLang applications for malware analysis and web threat detection.
- Developed comprehensive tactical, operational, and strategic threat intelligence reports, providing actionable insights for senior management and improving overall cybersecurity posture.
- Hands-on experience in managing cybersecurity projects, including leading cyber fraud investigations and coordinating with cross-functional teams (cybersecurity, law enforcement, legal, fraud) to ensure timely resolution of incidents and reduced risk exposure.
- Proficient in detecting, responding to, and investigating security incidents using technologies like Microsoft Sentinel, Kusto Query Language (KQL), and Splunk.

WORK EXPERIENCE

Senior Cyber Fraud Response Specialist

UBS
Zurich, Switzerland
October 2022 - Present

- Tracked and analyzed advanced threats like mobile banking malware and phishing kits, identifying malicious campaigns and providing actionable insights that improved client security and reduced response times.
- Delivered presentations on threat intelligence and cybersecurity projects at industry conferences, enhancing the company's visibility and professional reputation.
- Led investigations into thousands of cyber fraud cases, collaborating with global security, law enforcement, legal, and fraud teams to resolve incidents and strengthen threat response.
- Developed Splunk queries and dashboards to analyze logs of cyber fraud cases, detecting and preventing fraud, leading to a significant reduction in both incidents and financial losses.

Cyber Threat Intelligence Analyst

UBS
Zurich, Switzerland
January 2021 - September 2022

- Tracked threat actors using tools like Anomali, YARA, VirusTotal, and Urlscan, to uncover phishing and malware distribution networks.
- Created 30+ tactical, operational, and strategic threat intelligence reports for senior management, providing actionable insights on advanced threats to strengthen the organization's overall security posture.
- Provided cross-regional and cross-functional threat briefings to key stakeholders, utilizing frameworks like MITRE ATT&CK and the Cyber Kill Chain to deliver structured analysis and risk assessments.
- Collaborated with national and international CERT communities to fight cybercrime and stay informed on emerging cyberthreats.

Security Incident Responder

PartnerRe

Zurich, Switzerland

October 2019 - December 2020

- Responded and mitigated hundreds of cyber security incidents, including malware infections, phishing attacks, and attempted unauthorised access.
- Improved security incident detection and response efforts, using tools such as Microsoft Sentinel with Kusto Query Language (KQL) to monitor, analyze, and investigate security events across different environments.
- Led phishing awareness campaigns for 2000+ employees, significantly reducing phishing attacks.

Junior researcher

SAP

Sophia Antipolis, France

March 2019 - September 2019

- Created a JavaScript tool to trace and isolate threat actors in web apps, the project resulted in a patent.
- Used Python and JupyterLab to analyze experimental results, refining the fingerprinting algorithm and optimizing system performance for more accurate threat detection.
- Collaborated with senior researchers to expand the project scope, contributing to the design and implementation of advanced techniques that strengthened web application security.

EDUCATION

Master Degree in Cybersecurity

University of Trento / EURECOM (EIT Digital double degree)

September 2017 - September 2019

Bachelor Degree in Computer Science

University of Trento

September 2013 - March 2017

PROJECTS

Open-source cyber security tools

Created several open-source cybersecurity tools, available on my GitHub profile: github.com/andpalmier

Cyber security blog: andpalmier.com

Authored posts on malware analysis, machine learning, and tech-related topics for my personal blog

PUBLICATIONS AND PRESENTATIONS

- **2025 - Presentation at Digital Investigation Conference (DIC Zurich)**
“The subtle art of jailbreaking and defending Large Language Models”
- **2024 - Presentation at [TLP:RED CONFERENCE]**
“Introducing SEADS: an ads scanner for Search Engines”
- **2020 - Patent [US20210160277A1](#) & Presentation at SecWeb workshop**
“Application security through multi-factor fingerprinting”
- **2019 - Paper [10.1109/SERVICES.2019.00023](#) & Presentation at IEEE World Congress Services**
“MQTTSA: A Tool for Automatically Assisting the Secure Deployments of MQTT Brokers”

CERTIFICATIONS

“Malware analysis” by **Pluralsight** (2023)

“Google's Foundations of Project Management” by **Coursera** (2022)

“Google's Data Analytics Specialization” by **Coursera** (2022)

LANGUAGES

Italian - Native speaker

English - Fluent

German - Basics