Andrea Palmieri

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

A cybersecurity specialist with experience in cybercrime investigations, threat intelligence, and information security. Proven ability to analyze and respond to advanced cyber threats, conduct investigations, and collaborate with cross-functional teams to mitigate cyber-fraud cases. Desiring to use analytical and research skills to protect, prevent, and mitigate computer security issues when the stakes are high.

KEY SKILLS

- Extensive experience in researching, analyzing, and mitigating advanced cyber threats using tools such as Splunk, Anomali, and YARA, with a focus on phishing, mobile malware, and fraud-related activities.
- Developed comprehensive tactical, operational, and strategic threat intelligence reports, providing actionable insights for senior management and improving overall cybersecurity posture.
- Strong skills in Python and Go, focusing on developing security tools, including GoLang applications for malware analysis and custom Python scripts for vulnerability exploitation.
- 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.
- Experienced in delivering public presentations on cybersecurity trends and threat intelligence at industry conferences, enhancing organizational visibility. Proficient in producing high-quality technical documentation for diverse audiences.
- Proficient in detecting, responding to, and investigating security incidents using technologies like Microsoft Sentinel, Kusto Query Language (KQL), and Splunk.
- 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 and solutions.

WORK EXPERIENCE

Senior Cyber Fraud Response Analyst
UBS
Zurich, Switzerland
October 2022 - Present

- Led investigations into hundreds of cyber fraud cases, working closely with cybersecurity, law enforcement, legal, and fraud teams to resolve incidents and mitigate risks.
- Tracked and analyzed advanced threats like mobile banking malware and phishing kits, identifying malicious campaigns and providing actionable insights that strengthened client security and reduced response times.
- 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 advanced cyber actors using tools like Anomali, YARA, VirusTotal, and Urlscan, uncovering their tactics and infrastructure to inform senior leadership.
- 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.
- Delivered presentations on threat intelligence and cybersecurity trends at industry conferences, enhancing the company’s visibility and professional reputation.

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 applications. Project resulted in a patent.
- Analyzed the results of experiments using Python and JupyterLab, refining the fingerprinting algorithm and evaluating the effectiveness of the system.
- Collaborated with senior researchers to enhance the project's scope, contributing to the design and implementation of advanced techniques for web application security.

PROJECTS

Cyber security blog
Authored posts on malware analysis, machine learning, and phishing for my personal blog: andpalmier.com

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

EDUCATION

Master Degree in Cybersecurity
University of Trento / EURECOM (EIT Digital double degree)
Trento, Italy / Sophia Antipolis, France
September 2017 - September 2019

Bachelor Degree in Computer Science
University of Trento
Trento, Italy
September 2013 - March 2017

PUBLICATIONS

"Application security through multi-factor fingerprinting". Patent US20210160277A1 and presentation at SecWeb workshop 2020

"MQTTSA: A Tool for Automatically Assisting the Secure Deployments of MQTT Brokers". DOI: 10.1109/SERVICES.2019.00023. Publication and presentation at IEEE World Congress on Services 2019

CERTIFICATIONS

Malware analysis - Pluralsight (October 2023)
Google's Foundations of Project Management - Coursera (September 2022)
Google's Data Analytics Specialization - Coursera (June 2022)
Data Analytics summer school (August 2018)

LANGUAGES

Italian - Native speaker
English - Fluent
German - Basics