Daniel Kapellmann Zafra

Netherlands, Amsterdam | danielkapellmann.z@mandiant.com
(+31) 06 1185 8915| www.kapell.tech

SUMMARY OF QUALIFICATIONS

- Main focus on cyber-physical security intelligence (ICS/OT), Information Operations, and product development.
- Frequent speaker on operational technology (ICS/OT) topics at international conferences.
- Accomplished SANS 612 ICS Security In-Depth, 515 ICS Active Defense Training, SEC488: Cloud Security Essentials, DHS Industrial Control Systems Security (301 and 401). Certified CISSP, CompTIA CSAP, and AWS Cloud Practitioner.
- Studies related to Information Security and Business Intelligence with experience in a variety of industries.
- Excellent communication and writing skills developed through research and journalism.
- Languages: Spanish (Native), English and Dutch (Advanced), French (Intermediate), German and Russian (Basic).

WORK EXPERIENCE

GOOGLE, *Netherlands* November 2022 – Present

Analysis Manager, Cyber-Physical and Information Operations

- Coordinate the strategic development of tools and processes for collections and threat hunting to develop threat intelligence related to cyber physical threats and information operations.
- Support the development of technical outputs to scale the reach of cyber threat intelligence analysis and implement analysis projects to promote thought leadership.

MANDIANT, *USA and Netherlands* June 2017 – October 2022

Senior Technical Analysis Manager, Cyber-Physical (ICS/OT)

- Lead the technical analysis team to develop methodologies to hunt for malicious ICS/OT samples (Snort/Yara), define mechanisms for automated intelligence processing and collections, and research on observed threat activity.
- Designed and coordinated the implementation of a software tool to integrate heterogeneous data into a comprehensive platform to support operational technology vulnerability assessments. The product has generated over one million dollars in revenue.
- Automated the creation of intelligence reports leveraging open and proprietary sources. The topics for these reports include anomalies in ICS network traffic, internet-exposed OT assets, malware distribution, and ICS vulnerabilities, among others. This involves restructuring intelligence production to automate data pipelines from collection to distribution of end products.
- Collaboratively created the cyber-physical team strategy to address customer needs and project thought leadership. This included conceptualizing on report topics, blogs and publications, and coordinating automation projects.
- Created a collection tool to retrieve information from public vulnerability disclosures and provided a systematic analysis.
- Coordinated the development of in-depth risk assessment reports for organizations across multiple industry verticals.
- Tested and analyzed methodologies for streamlining the training process of new entrants to OT/ICS cybersecurity.
- Volunteered to develop and provide trainings on a range of topics including: Introduction to OT Security, Cyber Threat Intelligence Foundations, Threat Actor Attribution, and Hunt Mission Workshops.

Speaker Engagements:
BRUCON 2022, Confidence 2022, EuskalHack 2022, FIRST 2022, S4 2022, No Hat 2021, BRUCON 2021, MRO 2021, RSA 2020, CS3STHLM 2020, ICSJWG 2018/2019, CYCON 2019, AFPM Operations & Process Technology Summit, IIoT World Days 2020, ICS Village Hack the Capitol 2019, Virus Bulletin 2019/2020, Summit Virtual U-Gob Lab 2020.

Additional Training:
SANS 612 ICS Security In-Depth, SANS 515 Active Defense, SEC488: Cloud Security Essentials , CISA ICS Cybersecurity 401 and 301, Mandiant Consulting 101, FireEye Binary Triage. Certified CISSP, CompTIA CSAP, and AWS Cloud Practitioner.

INTERNATIONAL TELECOMMUNICATION UNION (ITU) Jan 2016 – Dec 2017

Remote Consultant - *ITU is the United Nations specialized agency for Information and Communication Technologies*

- Conducted research about policies, social plans and projects pertaining digital inclusion and Girls in ICT.
- Achieved four times increase in the number of visits to the Digital Inclusion Newslog over 2016 and 2017.

UNIVERSITY OF WASHINGTON Jan 2017 – June 2017

Research Assistant – Technology and Social Change

- Researched services, practices, and programs that foster civic engagement in public libraries through technology. Wrote and delivered a report evaluating these programs' effectiveness.

- Performed research on case studies that measured the level of digital inclusion and technical capabilities across countries. Research supported a collaborator's report that was delivered to the United Nations.

PUGET SOUND ENERGY (PSE), *Seattle, WA* Jun 2016 – Sep 2016
Intern - IT Planning and Architecture
- Developed project deliverables for planning and implementation of Enterprise Architecture Software (Visio and SharePoint).
- Enhanced the Architecture Review Board's process and site based on data obtained from user surveys and main stakeholders.
- Produced Cloud Readiness Assessment Tool to assess the level of preparedness of IT projects before implementation.

THE COMPETITIVE INTELLIGENCE UNIT (CIU), *Mexico City, Mexico* Feb 2014 – Jan 2016
IT Business Analyst - *The CIU is a strategic consultancy specialized in ICT market research, regulation and Creative Industries*
- Led a team of ten analysts to survey local software and video game developers. Utilized this data to perform market analysis on the challenges and opportunities faced by local technology companies.
- Coordinated a team to elaborate the Digital Strategy for Yucatán state, providing a framework for IT development.
- Quantified the financial impact of large cultural venues to evaluate their relevance for the local economy.

EDUCATION

UNIVERSITY OF WASHINGTON, INFORMATION SCHOOL, *Seattle, WA* Sep 2015 – Jun 2017
Master of Science in Information Management- *Awarded: Fulbright Fellowship and Conacyt Scholarship*
- Technical foundations for cybersecurity and penetration testing (Kali Linux, Security Onion, Wireshark, etc.)
- Experience in compliance projects (PCI, HIPAA, FERPA & NERC-CIP) & information security frameworks
- InfoSec Capstone Project: Implementation and design of Anti-Phishing Awareness Strategy for UW Medicine
- Founding Member/Editor in Chief for ISACA UWC Student Group – Coordination of ISACA UWC Handbook 2016

INSTITUTO TECNOLÓGICO AUTÓNOMO DE MÉXICO (ITAM), *Mexico City, Mexico* Jan 2010 – Oct 2014
Bachelor of International Relations – *Awarded: Excellence Scholarship and Telmex Foundation Grant*
- Thesis paper: "Cybersecurity in the USA: An Approach to the New Global Threat"
- Exchange semester at Universität zu Köln, Germany, January 2012

PROJECTS & AWARDS

- ***International Liaison:*** for the Industrial Control Systems Joint Working Group (ICSJWG) Steering Committee from the U.S. Cybersecurity Infrastructure Security Agency (CISA)
- ***Virus Bulletin Research Publication (UK):*** Hello from the OT Side!
- ***Conference on Cyber Conflict (CyCON) 2019 Research Publication (Estonia):*** Call to Action: Mobilizing Community Discussion to Improve Information Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure.
- ***Virus Bulletin Research Publication (UK):*** Fantastic Information and Where to Find it: A guidebook to open-source OT Reconnaissance.
- ***Kaspersky Talent Lab 2017 (Russia):*** Won contest through design of "Personal Security Trainer" for cybersecurity awareness.
- ***Microsoft Big Idea Design Challenge 2016:*** Honorable mention for design of "Home Abroad" application.
- ***Future Challenges Blogger:*** Written assignments funded by Deutsche Welle, Bertelsmann Stiftung, Siemens Stiftung.
- ***Policy Publication:*** Multilateral Cyberspace Regulation text for the book ¨México y el Multilateralismo del Siglo XXI.¨