Daniel Kapellmann Zafra

Dora Tamanaplein 10, 1074 JM, Amsterdam | kapellmann@google.com
(+31) 06 1185 8915| www.kapell.tech

SUMMARY OF QUALIFICATIONS

- Main focus on Technology & Strategy with operational experience leading cyber threat intelligence teams.
- Subject matter expertise in Applied AI for Cyber Threat Intelligence (CTI), engineering AI-centric workflows, and navigating adversarial AI landscapes, built upon a strong foundation in OT/ICS and Information Operations.
- Success in operationalizing AI to solve complex engineering challenges, rapid prototyping (POCs), and delivering scalable intelligence.
- Frequent speaker on cyber threat intelligence topics at international conferences with a robust history of top industry-led cyber security and threat intelligence training.
- 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, Dutch (Advanced), French (Intermediate) German and Russian (Basic).

WORK EXPERIENCE

GOOGLE THREAT INTELLIGENCE GROUP, *Amsterdam, Netherlands* November 2022 – Present

Security Engineer, Applied AI | *Mar, 2026 – Present*

- **Engineer AI-centric workflows:** Redefining cyber threat intelligence by building and testing hypothesis-driven proofs-of-concept (POCs) that automate complex cyber threat intelligence (CTI) processes and accelerate intelligence delivery.
- **Redefine Threat Intelligence:** Drive the evolution of CTI into an autonomous, AI-first ecosystem by applying large language models (LLMs) and advanced AI tooling to solve complex engineering challenges.
- **Adversarial AI Research:** Actively track and navigate the evolving adversarial AI threat landscape, maintaining subject matter expertise on the ecosystem of threats using AI to scale threat activity and target AI models.
- **Bridge Strategy & Execution:** Turn analytical expertise into production-ready action by translating high-level executive objectives into deep, scalable engineering systems.

Technology Prioritization Lead, Operations Enablement | *May, 2025 – Mar, 2026*

- **Strategic Prioritization:** Strategic technology leader and advisor focused on translating complex security and engineering challenges into actionable executive strategy and high-impact business outcomes.
- **Prioritization Framework:** Designed and operationalized a framework for Technology prioritization, acting as the strategic bridge between GTIG operational teams and Engineering to translate complex intelligence needs into precise, scalable technology requirements.
- **AI Integration & Enablement:** Led cross-functional initiatives (such as the Prompting Guild and Agentic GTI efforts) to initialize the safe and effective adoption of AI capabilities into existing intelligence workflows.
- **Process Automation:** Spearheaded the development of novel tools and processes to keep the organization ahead of emerging threats and improve the scale of intelligence collections.

Security Engineering Manager, OT/ICS & Information Operations (IO) | *Nov, 2022 – May, 2025*

- **Operational Leadership:** Led world-class operational teams specializing in cyber-physical security (OT/ICS) and Information Operations (IO) threat intelligence.
- **Team Consolidation:** Successfully consolidated diverse multidisciplinary teams, translating highly complex technical topics into clear, actionable strategies.
- **Foundational Intelligence Delivery:** Coordinated the strategic development of tools and collections processes for threat hunting, laying the rigorous analytical foundation necessary for intelligence-led action and process automation that later evolved into AI-centric CTI workflows.

MANDIANT, *USA and Netherlands* June 2017 – October 2022 ***Senior Technical Analysis Manager, Cyber-Physical (ICS/OT)***

- Co-created and led the cyber-physical team strategy to address customer needs and project thought leadership. This included conceptualizing automation projects and analytic products.
- Designed and coordinated the implementation of software tool to integrate heterogeneous data into a comprehensive platform to support operational technology vulnerability assessments. The product 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.
- Led the technical analysis team to develop methodologies for threat hunting malicious ICS/OT samples (Snort/Yara), implemented mechanisms for automated intelligence processing, and delivered in-depth risk assessments for organizations across multiple verticals.
- Collaborated with Go-to-Market teams by serving as a frequent external speaker on cyber threat intelligence (ICS/OT) at 15+ international conferences (RSA, Virus Bulletin, CODE BLUE, CyCON, S4, etc.), enabling Sales/Partner teams with intelligence-led narratives and thought leadership.
- Streamlined internal training processes for OT/ICS cybersecurity and trained customers on a range of topics including: OT Security, Cyber Threat Intelligence Foundations, Threat Actor Attribution, and Hunt Mission Workshops.
- Accomplished a variety of training in different domains SANS 612 to sustain actualized multidisciplinary capabilities. This includes for example 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
- Enhanced 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 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

OTHER PROJECTS & AWARDS

- ***Adversarial AI and Agentic Google Threat Intelligence:*** "Operationalizing Google Agentic Threat Intelligence: Transforming Defense Workflows" & Beyond source code: The files AI coding agents trust — and attackers exploit
- ***Virus Bulletin Research Publications (UK): '***Hello from the OT Side!' & 'Fantastic Information and Where to Find it: A guidebook to open-source OT Reconnaissance.'
- ***Conference on Cyber Conflict (CyCON) 2019 Research Publication (Estonia):*** Call to Action: Mobilizing Community Discussion to Improve Information Sharing About Vulnerabilities in ICS and CI.
- ***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.¨