Michael Galde

Cybersecurity Researcher & Educator

Tucson, Arizona, United States

consult@michaelgalde.com | www.michaelgalde.com | linkedin.com/in/mgalde | github.com/mgalde

SUMMARY

Innovative cybersecurity researcher and educator with a decade of experience in cyber operations, reverse engineering, malware analysis, and industrial control system security. Proven expertise in developing hands-on curriculum, leading applied research projects, and conducting technical assessments across IT and OT environments. Recognized speaker and contributor to cybersecurity publications and conferences. Holds a Master's in Cybersecurity and advanced GIAC certifications (GICSP, GRID).

EXPERIENCE

Assistant Professor of Practice | University of Arizona | Jan 2020 - Present

- Lead instruction for courses in Malware Analysis, Network Defense, ICS Security, and Reverse Engineering
- Created hands-on malware exam challenges and co-led ICS SOC research with ELK + Wazuh integration
- Built VICE virtual instruction platform and developed 'The Packet' publication

Cybersecurity Engineer II | Nebraska Applied Research Institute | May 2017 - Jan 2020

- Conducted vulnerability research and reverse engineering on IT/OT protocols (DNP3, BACnet)
- Developed protocol fuzzers and packet replay tools for ICS exploitation simulations
- Presented findings at DEFCON and authored internal technical white papers

Consulting Specialist | SaguaroSec | Jan 2022 - Present

- Lead analyst for advanced threat scenarios and custom security tooling for private sector clients

Intelligence Analyst | The Buffalo Group / US Army / USSTRATCOM | 2005 - 2016

- Supported classified analysis missions on Middle East, Iran, DPRK, and extremist networks

- Contributed intelligence products to Congress and interagency defense efforts

EDUCATION

Master of Science in Cybersecurity - University of Nebraska at Omaha, 2019

Bachelor of Science in Political Science - University of Nebraska at Omaha, 2013

CERTIFICATIONS

GICSP - Global Industrial Cyber Security Professional

GRID - GIAC Response and Industrial Defense

Ethical Hacking | Wireshark Forensics | Malware Analysis (LinkedIn Learning)

TECHNICAL SKILLS

Reverse Engineering, Malware Analysis, ICS/SCADA Security, Python, KVM, Yocto, ELK, Wazuh, C/C++, Wireshark, Ghidra, IDA Pro

SELECTED PUBLICATIONS & MEDIA

- 'One Year of Russia's Cyberwar in Ukraine' (Military Times)

- Cybersecurity features on local news, CactusCon workshops, and university panels