MARK J. BRUNO

Den Haag, Netherlands | mark@itsbruno.xyz | linkedin.com/in/markjbruno
U.S. Citizen | Netherlands Permanent Resident | Open Work Authorization

Cybersecurity Professional | Threat Intelligence · Security Risk & Compliance · Security Testing

PROFESSIONAL SUMMARY

Cybersecurity professional working across threat intelligence, security risk and compliance, and security testing. Published analyst at the New Lines Institute for Strategy and Policy, with authored work on PRC-linked telecommunications infrastructure operations (Salt Typhoon) and illicit finance networks in Southeast Asia. Founder and editor of The Moloch, an independent threat intelligence research publication covering APT activity, cybercrime ecosystems, and critical infrastructure threats, with analysis cited by U.S. Army publications and Halcyon Threat Intelligence.

Background spans SIEM administration and incident response, ISO 27001 policy development, OSINT and adversary TTP profiling, and vulnerability assessment. Holds CompTIA Security+, CySA+, PenTest+, ISC² CC, and Microsoft AZ-900. MA in International Relations & Security Studies; MSc in Cybersecurity & Information Assurance. U.S. Army veteran with prior TS/SCI clearance. Netherlands-based with full right to work.

CERTIFICATIONS

CompTIA Security+ | CompTIA CySA+ | CompTIA PenTest+ | ISC² CC | Microsoft AZ-900

In Progress: ISACA CISM | CompTIA SecurityX (CASP+) | EC-Council CCSE | EC-Council CASE | HTB CDSA

PROFESSIONAL EXPERIENCE

Security Risk & Compliance Contractor 2025 – Present
Freudiger IT Security B.V. | Netherlands

- Produce threat intelligence and risk advisory products for clients across healthcare, manufacturing, and medical supply sectors, mapping adversary TTPs to client-specific attack surfaces and delivering prioritized intelligence findings to technical and executive stakeholders.
- Conduct OSINT-driven threat actor research, dark web monitoring, and sector-specific threat landscape analysis, integrating findings with MITRE ATT&CK to produce structured intelligence products and control gap assessments.
- Support client vulnerability assessment engagements using Nmap, Nikto, Burp Suite, and OWASP ZAP; translate technical findings and regulatory exposure (GDPR, NIS2, DORA) into operational remediation guidance for management.

Contributing Analyst — Tech Sovereignty & Cyber Security 2025 – 2026
New Lines Institute for Strategy and Policy | Washington, D.C. (Remote)

- Research and analyze state-sponsored cyber operations, digital infrastructure threats, and geopolitical risk for a senior policy-oriented audience, integrating OSINT and technical threat intelligence with systems-level analysis.
- Authored published analysis on telecommunications infrastructure security and PRC-linked state cyber operations (Salt Typhoon); published manuscript on financial crime and illicit finance networks in Southeast Asia.

Information Security Officer 2023 – 2025
Dyami Security Intelligence | Utrecht, Netherlands

- Deployed and administered Wazuh SIEM across organizational endpoints, configuring detection rules, monitoring alert queues, and triaging security events to identify indicators of compromise and anomalous behavior.
- Developed and implemented the organization's information security policy framework, including incident response, access control, data classification, and acceptable use policies aligned with ISO 27001.
- Produced 50+ threat intelligence reports covering cybercrime trends, sector-specific attack vectors, and state-sponsored operations for aviation and other high-priority sector clients.

- Administered Google Workspace and GCP IAM, managing user provisioning, MFA enforcement, role-based access controls, and audit logging to maintain least-privilege posture across the organization.

Combat Medic (68W) / Public Affairs Representative 6 Years of Service
United States Army

- Operated within NATO joint-force and coalition environments requiring rigorous information assurance, documentation integrity, and structured accountability frameworks; held U.S. Top Secret/SCI security clearance.
- Managed sensitive records using DoD-networked systems in compliance with military IA standards; operated tactical CIS including encryption key management devices and coalition-networked endpoints.

EDUCATION

MA, International Relations & Security Studies — Webster University Leiden, 2026
MS, Cybersecurity & Information Assurance — Western Governors University, 2024
Graduate Certificate, Information Assurance — University of Maryland Global Campus, 2021
BS, Communication & Media Management — State University of New York at Fredonia, 2014

TECHNICAL SKILLS

Security Operations & Detection: SIEM administration (Wazuh, The Hive, Security Onion), alert triage and investigation, detection rule development, threat hunting, incident response, IOC analysis
Threat Intelligence: Adversary TTP profiling, MITRE ATT&CK mapping, OSINT, dark web monitoring, threat actor tracking; MISP, OpenCTI, Maltego, Feedly TI, FalconFeeds, Shodan, ANY.RUN, Recorded Future
Vulnerability Assessment & Testing: Nmap, Nikto, Burp Suite, OWASP ZAP, Metasploit, Kali Linux; red team / blue team / purple team methodology
Cloud & Infrastructure: GCP IAM, Microsoft Azure (AZ-900), Docker/Podman, Linux (Fedora, Debian, Kali, Parrot OS), TCP/IP, DNS, firewalls, IDS/IPS, VPN
Automation & Scripting: Python & BASH (workflow automation, data processing; LLM-assisted development); SOAR familiarity (coursework); GitLab; SIEM detection rules
Regulatory Frameworks: GDPR, NIS2, DORA, PCI DSS, ISO 27001, NIST CSF

LANGUAGES

English: Native | **German:** B1 | **Dutch:** Developing