Michael T **Moran**

PH.D. | SECURITY RESEARCHER | DATA SCIENTIST | HE/HIM

Brooklyn, NY 11201

248-885-3581 | mmoran0032@gmail.com | mmoran0032.com | mmoran0032 | mmoran0032 | in/mmoran0032

Experience

Duo Security *New York, NY*

SENIOR DATA SCIENTIST *June 2021—Present*

- Designed and developed an internal Python-based detection engineering platform to support rules-based and ML-based threat detection methodology on a single cohesive platform. Led efforts to unify existing detection point solutions across MFA, SSO, Passwordless, Mobile, and Administration teams on the new platform.
- Created and led the research program on malicious MFA device registrations and co-authored MITRE ATT&CK T1098.005. Organized engineering and design initiatives to include the detection outputs into Duo's SIEM product and improve the underlying log events.
- Expanded and standardized existing network-based detection methodology to use efficacious metrics and features and incorporate internet topology considerations (e.g., ASN, CIDR). Created a generalized large-scale PySpark feature generation pipeline to run across arbitrary entity combinations with limited code duplication.
- Provided incident response support on a number of internal and external incidents, including the 2022 Cisco breach. Collaborated with Cisco Talos and internal Duo teams to provide a full description of the phishing attack and created initial detection methodology to counter copy-cat threats.
- Created and maintained dbt-based threat intelligence feed and monitoring system within Snowflake data lake.

Human Security (née White Ops) *New York, NY*

SENIOR DATA SCIENTIST *September 2020—June 2021*

- Supported and trialed internal initiatives to integrate machine learning methods robustly into the threat detection life cycle, including interpretability methods (e.g., SHAP). Created an offline model reduction/distillation process as a transition system from pure rules-based detections to ML-based detections.
- Collaborated with Google and Roku to assess Roku's WATERMARK system in preventing device impersonation attacks.

TECHNICAL LEAD *March 2019—December 2020*

- Led an international team of threat researchers, security engineers, and analysts to develop brand new solutions to stop advertising fraud/spam on Connected TV platforms.
- Integrated team best practices (OKRs, retrospectives, code reviews) and championed improved documentation processes. Made the decision to fold the team into the existing Mobile team to improve the company's research and response capabilities.

DATA SCIENTIST *January 2019—August 2020*

- Created and led the research program on fraudulent ad activity in the Connected TV (video streaming devices and services) domain. Led counter-offensive against three large fraud operations and integrated statistical models based on the underlying TTPs into fraud detection and prevention systems.
- Expanded anomaly detection, device and IP classification, and device fingerprinting systems to Connected TV-related environments.

Gartner *Stamford, CT*

DATA SCIENTIST *October 2017—December 2018*

- Improved client engagement by 5% by integrating a session-based reading history recommender system into the search ranking model.
- Created pipeline (using SQL, pandas, XGBoost) and post-training analysis framework (based on SHAP) to assess search engine ranking result efficacy and avoid negative feedback loops in ranking outcomes.
- Ran and analyzed A/B tests to ensure that changes improved search KPIs (search abandonment, document engagement).

Education

University of Notre Dame *Notre Dame, IN*

PH.D. NUCLEAR ASTROPHYSICS *November 2018*
M.S PHYSICS *August 2014*

Michigan State University, Lyman Briggs College *East Lansing, MI*

B.S. ASTROPHYSICS, B.S. PHYSICS, MATHEMATICS (MINOR) *May 2011*

Volunteering

Section Leader

CS106A: **CODE IN PLACE**, OFFERED ONLINE BY STANFORD UNIVERSITY *Spring 2020, 2021, 2023*