

# Andrew VAGLIANO

andrew.vagliano1@gmail.com | Washington, DC | (860) 806-3910

 [andrew-vagliano](#)

## SUMMARY

Security software engineer experienced in analyzing and mitigating highly sophisticated threats to global-scale networks. Passionate about designing user-centric security solutions and skilled at bridging technical and non-technical expertise. Seeking fast-paced work environment with high growth and product ownership opportunity.

## SKILLS

<b>Languages</b>	Python   PHP / Hack   Javascript / Typescript   Haskell   Rust   SQL
<b>Technologies</b>	React   GraphQL   Dataswarm / Airflow   AWS   Docker   Linux
<b>Areas of Expertise</b>	Data Engineering   AI Solutions   Full-Stack Engineering   Data Analysis   Threat Intelligence
<b>Personal Interests</b>	Motorsports   Jazz & Bluegrass Guitar   College Football   Home Automation & Self-Hosting

## EXPERIENCE

### Meta Platforms, Inc.

Sep 2021 - Sep 2024

*Security Engineer, Integrity Investigations & Intelligence (i3)*

*Washington, DC*

- Served as engineering lead on trust & safety intelligence teams across multiple problem spaces; prototyped bespoke tools, standardized workflows across teams, and advocated investigator needs to external engineering teams to influence scaled solutions.
- Created a classification system to define malicious behavior; directed alignment of subject matter expert decision making, defined performance metrics with policy teams, built infrastructure to aggregate technical and manual decisions, and managed deployment to human review teams.
- Developed an AI system to detect and modify egregious content to minimize psychological impact on content moderators, improving employee retention and review speed; led cross-functional collaboration with design, legal, product, and review operations teams to align on requirements, execution, and deployment.
- Defined analytical requirements and collaborated with our human reviewer operations team to design a testing procedure for identifying miscalibration in an updated sexual exploitation policy; conducted statistical analysis of results, delivering insights to refine policy wording and improve precision.
- Led migration of file processing system for critical actor tracking pipelines to modern infrastructure, improving performance and interoperability with investigative tooling.
- Triaged and resolved technical incidents and reputational escalations across an ecosystem of hundreds of legacy data pipelines, tools, and systems, balancing rapid fixes with long-term systemic solutions.
- Mentored new hires by curating onboarding tasks and facilitating connections with key teams; conducted coding interviews to evaluate applicants and promote team growth.

### Meta Platforms, Inc.

Summer 2020

*Security Engineer Intern, Threat Discovery*

*Remote*

- Adapted an account clustering system to surface and classify decentralized conspiracy networks, enabling one of the company's then-largest takedowns of a dangerous conspiracy movement.
- Integrated OSINT sources and vendor data with internal tooling to improve situational awareness and off-platform investigative coverage; collaborated with vendor-management teams to secure data access.

### American University

Summer 2019

*Summer Research Assistant*

*Washington, DC*

- Developed an ML pipeline for a model leveraging NLP techniques to predict and identify malicious sequences of system calls in continuous network traffic, addressing the challenge of unstructured and variable call patterns.

## EDUCATION

### Northwestern University, McCormick School of Engineering

2017 - 2021

*Computer Science, B.S. | International Studies Minor | Pi Kappa Alpha Fraternity*

*Evanston, IL*

### The Hotchkiss School

2013 - 2017

## PUBLICATIONS

### Feature Extraction Based on Word Embedding Models for Intrusion Detection in Network Traffic

2020

*Journal of Surveillance, Security, and Safety*