

Technologies and Languages

- Languages: Python, Ruby, Ruby on Rails, Botmaker (Java/Scala Hybrid)
- Technologies: MySQL, Postgres, GCP, Big Query, Looker ML, Tableau, Kafka, SOAR, Splunk, IAM, Git, CI/CD
- Other: CISSP, GDPR, Anomaly and Intrusion Detection (Insider Threat, Internal Abuse), Threat Modeling

Work Experience

Senior Security Engineering Manager Data Misuse Detection (1 EM, 7 ICs)	Twitter Durham, NC (Remote)	Jan 2021 - Present
<ul style="list-style-type: none">• Led design/deployment of scalable detection platform using the latest technologies of Kafka, Splunk, Kubeflow, GCP, Dataflow, Big Query, and Looker ML that normalized, processed, and actioned 100M+ events/month• Led development of several end-to-end advanced detectors using unsupervised ml techniques (e.g., autoencoder, anomaly detection, clustering), automation, data-driven decorators, and custom dashboards to identify and action abuse on internal systems, social engineering, and Twitter verification; meaningful detections reduced human hours in the loop by more than 300%• Automated from the ground up rule-based detection platform written in custom Botmaker language (Java/Scala hybrid) with novel new features: stateful events support, Kafka streaming events, and expanded detection coverage with unique capabilities: direct messaging access abuse and failed access attempts• Directed company-wide Privileged Access Detection Workstream to regain trust post-2020 data breach by addressing monitoring, and investigation gaps for sensitive customer data access through internal admin tools		
Senior Security Engineer (team lead) Detection and Response Team	Twitter Durham, NC (Remote)	Mar 2018 – Jan 2021
<ul style="list-style-type: none">• Led five critical severity company-wide security incidents and provided technical direction, coaching, and career advice to detection and response members; as a team lead, grew the organization from two to fifteen• Developed automated adversary emulation platform (GCP, Jira, Carbon Black, and Slack APIs) based on ATT&CK framework and TTPs; matured capabilities resulted in the creation of a dedicated detection pipeline and team• Drove GDPR and FTC incident response regulatory readiness; full compliance with all audits and requirements		
Security Engineer Office 365 Security	Microsoft Seattle, WA	2012 –2018
<ul style="list-style-type: none">• Led multi-quarter project to move dedicated email hosting workload into Azure Cosmos DB based security analytics platform; reduced time to detect advanced threats by 19.5%• Enriched signal data by integrating interflow's threat intelligence platform's telemetry; facilitated correlation of security events and early detection capabilities across office properties: Exchange, Lync, Skype, Yammer, Teams• Developed internal tools in Python and PowerShell to improve investigations and data acquisition• XFN team member for tracking Russian-speaking determined human actors; led targeted breach investigations		
Cyber Security	U.S. Air Force Multiple Locations	2000- 2007
<ul style="list-style-type: none">• Optimized software and infrastructure vulnerability and risk assessments using Nessus, and Nmap tooling		

Education

- **B.Sc. Computer Science**, University of Illinois at Champaign-Urbana **2008 - 2011**