# ARUN KUMAR

❑ Cybersecurity ❑ Analytics ❑ Engineering Leadership ❑

+44 77563 78761
career@arunkumar.uk
www.arunkumar.uk
United Kingdom

Security-focused technologist with 18+ years of experience designing, building, and securing complex distributed systems. Expertise spans threat detection, mitigation, and research, with strong leadership of global, multi-disciplinary teams. Driven by a passion for learning, mentoring, and continuous innovation.

## WORK EXPERIENCE

### Sr Security Researcher (Anti-Automation & Fraud) — Fastly, Remote UK | 2022 - Present

As the lead researcher for the anti-automation (bot management), anti-abuse and anti-fraud security domains, responsibilities include research strategy, roadmap, design, prototyping, evaluation, and SME for client/analyst engagements.

- Developed techniques and tools to detect automated attacks by bots, such as account takeover (ATO) through credential stuffing/cracking, L7 DDoS, etc, without blocking benign bots and humans.
- Published research reports and blog posts on threat landscape trends, attack techniques, best practices, and mitigation strategies often in collaboration with marketing, PR, legal, CISO and product teams.
- Developed early warning techniques to identify internet-wide mass exploitation attempts through analytics, and deploy suitable mitigations for customer endpoints.
- Worked with engineering organisation to take prototypes to production, review designs, measure efficacy of security products, and provide product security guidance.
- Proactively identified platform security misconfigurations and worked with relevant teams to resolve them.
- Represent Fastly in W3C anti-fraud CG, working on emerging standards to combat cyber enabled fraud, collaborating with organisations across industries.
- Contributed to client consulting, product marketing, industry analyst engagements, with threat landscape, thought leadership and security strategy briefs.

### Threat Hunt Analytics & Engineering Lead — Morgan Stanley Fusion Center, UK | 2022 - 2022

Delivered the next generation of scalable data processing platforms for real-time threat detection, correlation and alerting.

- Conceptualized and designed a DAG centric real-time data processing platform, focused on ease of use and computational efficiency using memory mapping and zero copy techniques.
- Built tools for automated statistical summarization of large data sets for the purpose of data exploration and continuous monitoring of data fidelity.
- Build and mature the platform for adoption within the wider team of analysts.

### Threat Hunt Lead - Payment Systems — Morgan Stanley Fusion Center, UK | 2020 - 2022

Delivered threat detection and hunting solutions for payments systems across the firm including institutional and wealth, over a number of channels including SWIFT, ACH, TCH, Check processing, etc.

- Stood up a team of high-performing technologists to deliver solutions to a critical security function, in response to escalating attacks on payment systems.
- Surveyed the landscape of systems, conceptualized an analytics solution that can scale and be versatile to address the variety of risks and attack vectors in payment systems
- Developed and operationalized a detection strategy, and delivered a effective suite of analytics to significantly reduce risks to payment systems.
- Collaborated with fraud analytics teams to effectively hand off detections of cyber risk to mitigate fraud risk.
- Matured the platform and introduced tooling to make it accessible to the wider set of cyber analysts for use in their domains.

## EDUCATION

**M.Tech - Naval Arch & Ocean Engg**
Indian Institute of Technology Madras
2002 - 2007

**B.Tech - Naval Arch & Ocean Engg**
Indian Institute of Technology Madras
2002- 2007

## SKILLS

### Technical

Python/Go/Rust/Java/C#

Kafka/NiFi/Spark/Airflow

Ceph/Arrow/Parquet

Jupyter/Elasticsearch/Splunk

Fluentd/Prometheus/Grafana

Docker/Kubernetes/Helm

Terraform/GCP

Typescript/Angular/Bootstrap

CXF/Spring/WCF/Websockets

DB2/MySQL/Sybase/Redis

Fastly/Akamai/Cloudflare

HAProxy/Envoy/NGINX/F5/A10

WAF/mod_security/mod_proxy

Sysmon/auditd/Zeek/Arkime

MITRE/OWASP/NIST-800-53

### Professional

Leadership and Strategy

People Management

Program Management

Stakeholder Management

Effective communication

Strong problem solver

**Insider Threat Analytics Lead** — Morgan Stanley Fusion Center, UK | 2019 - 2020

Delivered a fit-for-purpose renovated insider threat analytics platform and analytics suite to detect threats to the firm and clients from insiders.

- Designed and delivered a scalable and maintainable analytics platform, with several customer self-service features.
- Delivered a suite of analytics to detect data leakage through various channels such as email, web, print, etc. Leverage data and capabilities from several security controls in the firm, to effectively deliver visibility and insights to incident responders.
- Transitioned a team staffed entirely with consultants to employees, and handled their training and career advancement.

**Cyber Analytics Research & Prototyping** — Morgan Stanley Cyber Fusion Center, NYC | 2018 - 2019

Responsible for developing and implementing a strategy to prevent and detect threats to the firms public facing web infrastructure, which includes over 400 web domains, 1000s of origin servers, across the globe.

- Rapid prototyping of detection analytics during cyber events, as well as coordination with control infrastructure teams in deploying emergency mitigation solutions.
- Developed a number of analytics to detect account takeover attacks such as credential stuffing, phishing kits, and validating user credentials against stolen credentials dumps.
- Developed a strategy to catalogue and harden the firm's external web surface, and built tailor-made analytics for each web property leveraging its distinctive characteristics.
- Develop new data sources for collection to continuously improve visibility in the network and leverage them to build threat intelligence driven analytics.
- Evaluate vendor and open source solutions for adoption into the firm's security posture, as well as assess existing critical controls deployed in the network for their effectiveness.
- Collaborate with BU cyber teams, offering support in areas such as analytics development, subject matter expertise and security policy deployment, with the goal of improving security posture of business apps.

**Senior Engineering Manager - Business Process Security Program Lead** — Morgan Stanley Prime Brokerage Tech, NYC | 2016 - 2018

Responsible for the ensuring the confidentiality, availability and integrity of Prime Brokerage assets, business processes and client services. Responsible for conceptualizing the road map for the program, prioritizing initiatives with PB non-market risk, and executing them to completion. I'm also responsible for managing the careers and work streams for my team. A selection of key projects is listed below

- Centralized implementation of 2FA for all/any internal PB apps using DUO/SecurID.
- A centralized 'client anonymity' feature enabling fully anonymous client onboarding to PB.
- Centralized app-wise IP whitelisting for client access to Morgan Stanley Matrix.
- Email Safety Catch solution to prevent accidental client data leakage. Tight control on client data while aliasing clients during support sessions.
- Automated alerting for changes in sensitive client attribute and contact information.
- Security training for IT on topics such as OWASP, and for the business on topics such as phishing, malware, etc

**Engineering Manager - Centralized Entitlements Platform** — Morgan Stanley Prime Brokerage Tech, NYC | 2015 - 2016

Responsible for the renovation and consolidation of the centralized entitlements platform in use by more than 60 systems including client and internal apps. Consolidated multiple GUIs into a single web GUI using AngularJS and Bootstrap. Modern client libraries in .Net and Java for use by apps to query entitlements.

**Cloud Integrations Developer** — Morgan Stanley Prime Brokerage Tech, NYC | 2015 - 2016

Responsible for evaluating and integrating cloud products requested by PB for suitability in the firm environment, including necessary security controls, legal, sourcing, etc.

- Products include VDR (Intralinks), client surveys (Qualtrics), and file sharing (Box).

Research and innovation

Lead and delivered complex software systems

Team player

## INTERESTS

Volunteering, Education

Travelling, Photography

Open Source Software

Protocols, Standards

Kayaking, Curling

- SSO for users using SAML/OAuth2. Backend integration using PKI, JWT, OAuth, REST API, FTP, etc.

---

**Client Web and Mobile Apps Lead** — Morgan Stanley Prime Brokerage Tech, NYC | 2012 - 2014

Designed, developed and delivered a number of application on the client facing MATRIX platform for multiple business lines including Equity Prime Brokerage, Equity Swaps, Listed Derivatives, OTC Clearing and FX Prime Brokerage.

- Worked with various teams for security architecture review, penetration testing, UX, legal, and risk.
- SME on client connectivity aspects such as global app delivery, authentication, entitlements, network routing, latency, edge caching, origin protection, DMZ deployment, etc.

---

**Employee and Conf Mobile Apps Lead** — Morgan Stanley Prime Brokerage Tech, NYC | 2012 - 2014

Developed mobile applications (Blackberry/MobileIron/iPad/iPhone) for clients and business users.

- A iPad based conference app for clients with geofencing, registration and messaging features. An app to schedule and send SMS messages en mass to client attendees.
- Email based CRM query/response system for use by PB Sales, Consulting, Client Service and Cap Intro.
- An iPad application for Sales, which indexes and correlates public data sets (regulatory filings, News, etc) and provides a search engine to find insightful information on prospective clients.

---

**Client Platform Framework Developer** — Morgan Stanley PB Tech, Mumbai | 2009 - 2012

Developed the foundational framework components (Flex) and libraries (Flex, Java, JS) for Matrix, a client-facing platform with research, operations, and reporting capabilities. The framework components developed include navigation, inter-app communication, real-time data feed channel, web based telephony, and task management. Handled support for clients in Asia until a dedicated support team was setup. Handled training for the new hires in the team.

---

**Business Apps Developer** — Morgan Stanley PB Tech, Mumbai | 2007 - 2009

Developed a number of applications primarily in C# .Net (desktop) and Java (JSP, Spring) to support the Prime Brokerage team in scaling client servicing. These applications helped them migrate off emails to task/exception management systems. The outlook based plugin helped to migrate a conversation off email to the CRM/WORKQ systems. A business intelligence PoC built with Google motion charts was later adopted by the business in their client selection process.

---