Protecting the last sunny corner of the internet

Adrian McAlister

TikTok

March 2022

Adrian McAlister

- Industry expert with 25 years' experience across the IT industry and 17 years focused primarily on security
- Part of TikTok's CSPO team, based in Dublin
- Previously part of the computer Security Incident Response Team (CSIRT) at Salesforce, led security operations in APAC and EMEA for AECOM, and founding member of the CSIRT at Caterpillar

Agenda

- ❏ Threat actors
- ❏ Prioritising security
- ❏ Defence in depth
- ❏ Introducing our Dublin Fusion Centre
- ❏ Growing remotely
- ❏ The path to trust and transparency

Inspire Creativity, Bring Joy.

TikTok Can Be A Target for Bad Actors

To match our exponential growth, we're building a **world-class, converged security program**

Our Ambition

Ensure we Remain the Premier Platform for Happiness

Defend our Billion Strong Community of Creators

Comply with Global Regulations & Set the Standard for Industry

Position Security as a Business Enabler & Differentiator

What we're up against

State Sponsored Actors

- Motivation: Geopolitical gain by sowing discord and distrust
- May use coordinated inauthentic behavior (CIB), mis- and disinformation

Organized Crime

- Motivation: Financial gain
- Seek to exploit sensitive information from TikTok users

Terrorists

- Motivation: Social, economic, and/or political disruption
- Interested in causing civil unrest to advance a particular cause

Hacktivists

- Motivation: Activism / Advancing reputation
- Bringing awareness to a cause or causing damage to competing causes

TikTok

Prioritising Security, Based on our Principles

Instill a Security Culture to Enable our People as our 1st Line of Defense

People are the foundation of any organisation. Our security team is comprised of industry experts with decades of experience in the public and private sector to accelerate our security ambitions.

Expand our Capabilities & Reach Globally

Dramatically ***grow our footprint*** in innovative hubs like Washington, D.C., Mountain View, CA, Singapore & Dublin, Ireland to ***attract & nourish*** the best talent.

Build State of the Art Monitoring, Response & Investigative Fusion Centers

Our best-in-class Fusion Centres ***actively detect & respond*** to critical incidents globally in real-time.

Enable Partnerships with the World's Leading Cybersecurity Firms

Leverage ***partnerships & external expertise*** to ensure and validate our program delivers best-in-class security infrastructure and capabilities.

**We adhere to security standards like NIST, CSF, ISO 27001, & SOC2*

Defence in Depth

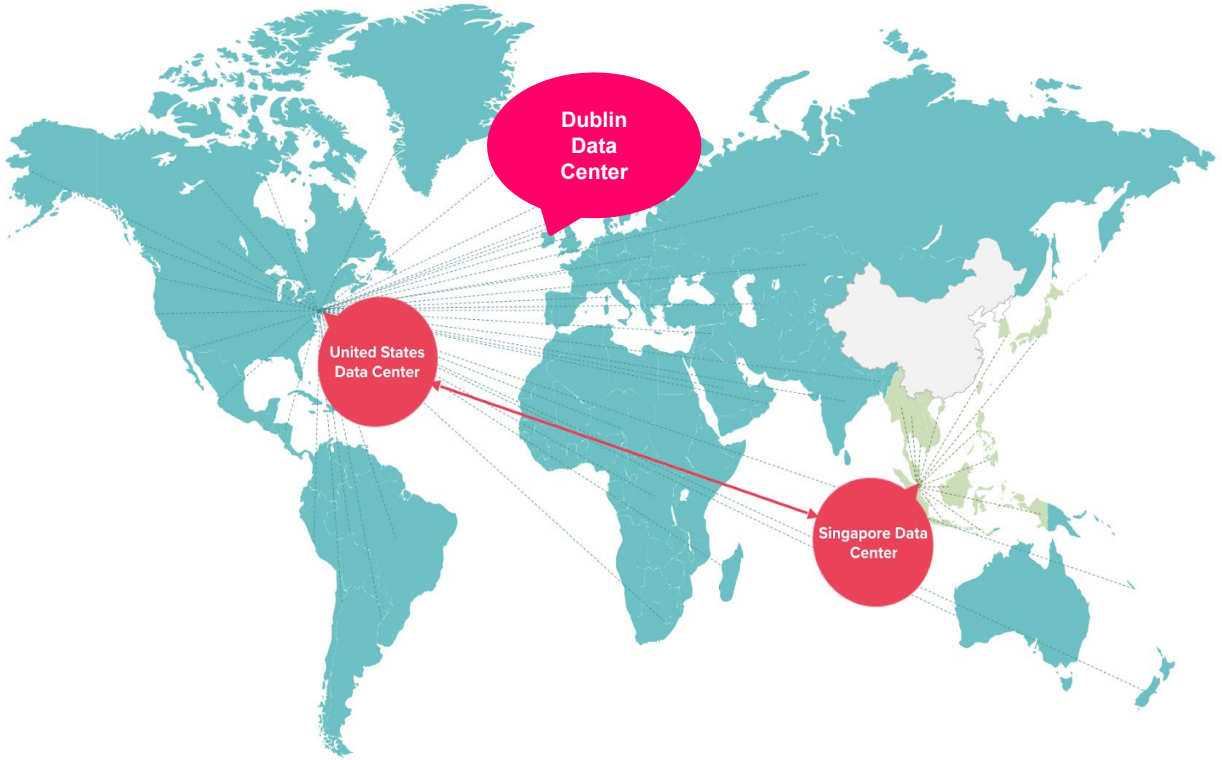
On Platform Defense	**Machine learning & automated monitoring** tools to track anomalous & inauthentic user behavior
ByDesign	Integration of security & privacy best practices & controls into **product development lifecycle**
Platform Controls	Security controls like **over the horizon threat defence** & global platform monitoring
Data Controls	**Define**, **implement** & **measure** controls to protect data including IAM/IDM
User Data	The hardened center of our defense in depth model focuses on **protecting user data** that we're entrusted to keep safe

TikTok Data Storage & Localisation

TikTok Users Serviced by the US Zone

TikTok Users Serviced by the Singapore Zone

Synchronizations Between Data Centers



TikTok

Introducing our Dublin Fusion Centre

We're growing our CSPO presence in Dublin through a **best-in-class Fusion Centre**

Communication & Coordination

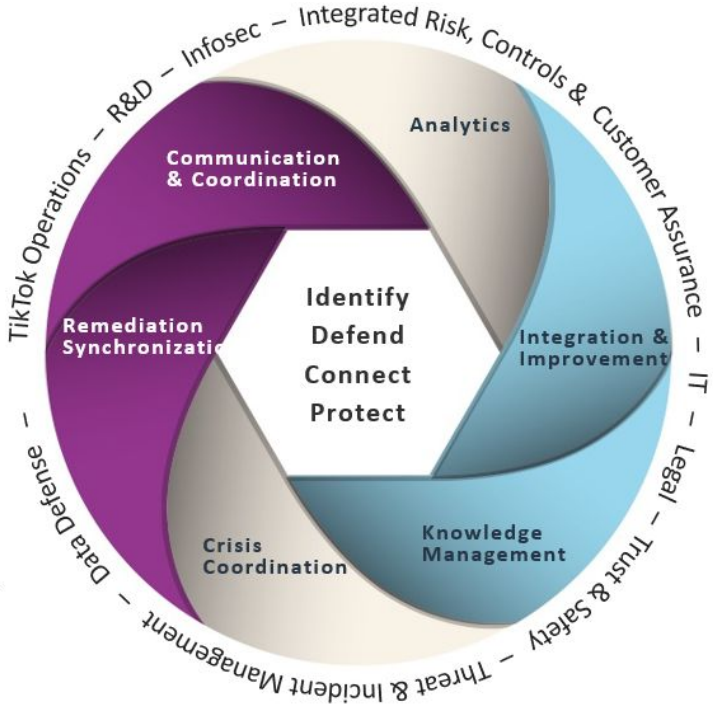
Engage with internal and external stakeholders

Remediation Synchronisation

Organise activities and ensure long-term strategic goal alignment

Crisis Coordination

Facilitate crisis training exercises and lead crisis coordination during response efforts



Analytics

Design metrics and contextualise data for reporting

Integration & Improvement

Break down silos across your organisation and build holistic enterprise risk solutions

Knowledge Management

Maintain change control and integrated process documentation

Detect & Respond

TikTok's state-of-the-art monitoring, response, & investigative **Fusion Response Centres** increase collaboration, helping us to actively **detect** & **respond** to critical incidents in real-time.

- Fusion Centres help us achieve:
  - Next-generation cyber-threat monitoring
  - Private & public cyber investigations & digital crime groups
  - Advancement of our on-platform threat discovery to protect our community
  - More efficient operations

Regional centres of excellence

Our Global Fusion Centres operate a **follow the sun** approach

We set out to build three simultaneous converged All Hazards Fusion Centres around the world (branded as FUSE)

Since early 2021, we've been building monitoring, response and investigative Fusion Centres to detect and respond to critical incidents in real-time, in Singapore, Dublin, and Washington D.C

Taking a virtual approach

XFN expertise	Specialised professionals with a **diverse skillset** across cyber, physical, misuse, environmental, social, and error-related risks and incidents
Common operating model	**Common tools and processes** include: advanced machine learning platforms to automate manual functions; detection and response controls for event monitoring, incident handling, remediation and forensic support; and platforms, dashboards and analytics to better contextualise both investigations and reporting
The impact of COVID	This group of cross-functional talent came together to build an All Hazards Fusion Centre during a pandemic, **virtually**
Taking a hybrid approach	Fusion Centre team has representation from across the business including **R&D, legal, privacy operations and trust and safety**

Product Security

Internal Detection Experts

Dedicated teams regularly test our code, identify vulnerabilities, and close them before the code is released

Partner with Leading Independent Assessors

Engage leading multinational service providers, experts, and contractors to provide an independent viewpoint & surge resources as necessary

Bug Bounty Program with HackerOne

By encouraging white hat hackers to identify bugs in our code and network, we benefit from independent security testing to better prepare ourselves for black hats that may target us

Anomalous Activity Detection

Threat intelligence is our force multiplier, driving decisions about what anomalous behavior looks like

Advanced Threat Library

Organized, categorized library of threats based on our converged intelligence philosophy all stored in a single repository; sources include our internal tools, feeds, and external providers

Converged Intelligence

We employ an abstraction layer for all threat intelligence that maps each threat, risk, or observation against 9 identifiers for indexing and correlation

Threat Informed Defense Capabilities

Countermeasures

We use a set of playbooks and use cases to rapidly respond to and remediate threats, leveraging state of the art detection and response tools

Security Automation

We have a team dedicated to automation, identifying resource intensive processes and applying machine learning and AI to reduce manual workloads

Our ***vision*** is to leverage threat intelligence platform to make better ***business decisions & protect our community***

A foundation of safety

*We are committed to **earning the trust** of our community.*

Quality
Delivering a quality product & experience to users globally

Communication & Education
Collaborating with security, law enforcement, & privacy experts to protect our global community

Choice
Empowering users with choices about their privacy, data sharing, & security practices

Access
Providing access to code & systems to validate security controls by third parties

Consistency
Continuously keeping users informed of updates to enhance privacy & security

5 Point Path to Trust & Transparency

A foundation of safety

- TikTok offers a wide range of **privacy & security settings** that users can activate during account setup or at any time
- We **actively educate users** about their options through in-app safety & security videos
- We offer **resources & tools for parents** to better oversee their child's online experience
- We frequently **update our security & privacy hub** with tips & resources

Empowering Community with Security & Privacy Choices

Inspire Creativity, Bring Joy.

TikTok is focused on protecting our users & scaling a global team of security experts to deliver *best-in-class capabilities.*
This important work is a job that's never "done."

Thank You!

TikTok