Axel Hoehnke
Virtual CISO · Governance Advisor · EU Cybersecurity Specialist

Case Study: OSINT Investigation — Mystery Box Supply Chain

Investigative TV Documentary, Germany

SECTOR	CLIENT	BRIEF
Broadcast journalism / Investigative media	Independent TV production, Germany	Supply chain intelligence for documentary
ENGAGEMENT	**DURATION**	**OUTCOME**
Vendor-neutral OSINT research	4–8 weeks investigation	Documentary broadcast, Dec 2025

The Brief

An investigative journalist at a German television production company was developing a documentary on mystery boxes — the consumer trend of buying packages of unknown, returned e-commerce goods. The story needed more than shopper interviews. It needed to show the infrastructure: who controls the supply chains, where the goods originate, how distribution networks are structured, and whether systematic consumer fraud could be documented.

Investigative intuition is not evidence. The documentary required verifiable, source-documented intelligence that could withstand editorial and legal scrutiny before broadcast. I was brought in to build that evidence base.

What I Did

Phase 1 — Digital Infrastructure Mapping

Using Shodan and Censys, I identified server networks associated with mystery box operators. DNS analysis via crt.sh and DNSlytics traced relationships between domains that appeared independent but shared infrastructure, registrar patterns, or SSL certificate chains — indicators of coordinated operation behind separate-looking storefronts. This phase produced a map of operator clusters and geographic distribution, primarily Polish warehouses routing into German retail.

Phase 2 — Actor Profiling

Using Sherlock, WhatsMyName, and OpenCorporates, I correlated usernames across platforms and traced corporate relationships between operators. TgStat and MaveKite provided analysis of Telegram and TikTok promotional channels — identifying influencer networks being paid to create unboxing content and how those channels connected back to the supply chain operators.

The investigation also incorporated physical intelligence: AirTag tracking to document actual product flows, and forensic address recovery — chemical treatment and specialised lighting to restore redacted shipping labels and reconstruct supply chain origin points deliberately obscured by operators. A whistleblower with direct industry access provided corroborating evidence of systematic fraud, documented and anonymised per journalistic protection standards.

The Findings

METRIC	FINDING
Mystery box articles in circulation annually	15+ million
CO^2 impact from returns logistics alone	240,000+ tonnes per year
Primary supply chain routing	Polish warehouse network → German distribution
Operator structure	Coordinated networks presenting as independent sellers
Consumer harm documented	Systematic fraud: fake labels, adulterated contents
Physical verification	AirTag tracking + forensic address recovery
Whistleblower evidence	Insider documentation of systematic fraud practices

The Outcome

The research formed the evidential backbone of a prime-time documentary broadcast on a major German public broadcaster in December 2025. The documentary exposed both the consumer harm and the environmental consequences of the mystery box ecosystem at industrial scale. It remains available on the broadcaster’s media library and YouTube channel.

This is the standard I hold OSINT work to: not interesting intelligence, but broadcast-ready evidence. Every finding documented, every source archived, every chain of custody traceable.

What the Client Said

> *“Super thanks — forwarding it. Results coming Friday.”*
>
> **— Lead Investigative Producer, German Television**
> (Personal reference available upon request)

What Made This Engagement Different

Regulatory compliance work produces audit files. Investigative OSINT produces evidence for public accountability. The discipline is the same — structured methodology, documented sources, defensible conclusions — but the stakes are different. A finding that cannot be verified to broadcast standard is not a finding.

The combination of digital infrastructure analysis, cross-platform actor mapping, physical tracking, and whistleblower corroboration is what separated this from surface-level web research. The supply chain operators had deliberately obscured their connections. Making those connections visible — and documenting how — is the work.

Relevant for Your Organisation If:

- You are an investigative journalist or documentary producer needing OSINT research to broadcast evidential standard
- You are a law firm or legal team requiring open-source intelligence for litigation or regulatory proceedings
- You need supply chain due diligence — mapping who is actually behind a distribution network
- You require vendor-neutral intelligence with documented methodology and full source archives
- You need digital infrastructure analysis combined with physical verification methods