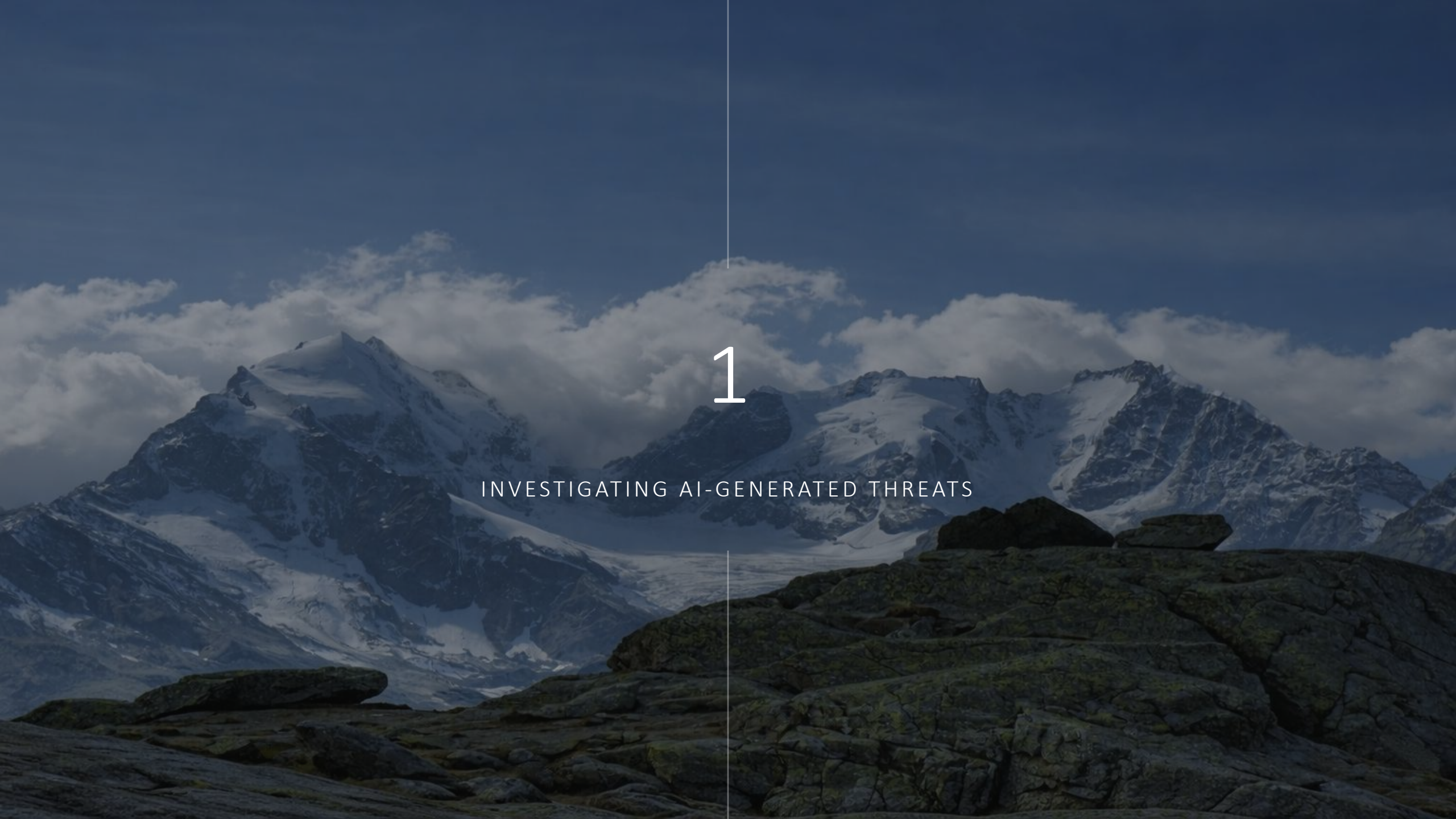




AI-POWERED CYBER-ATTACKS AND CROSS-BORDER INCIDENT RESPONSE

WORKSHOP



1

INVESTIGATING AI-GENERATED THREATS

Investigating AI-Generated Content & Deepfakes

New threats require new playbooks

- Rapidly evolving threats — playbooks quickly outdated; new forensics needed
- Hard to detect — no typos, no red flags; deepfakes can bypass voice/facial authentication
- Attribution nearly impossible — AI obscures identity, mimics legitimate users





2

CROSS-BORDER BREACH RESPONSE

Multi-Jurisdictional Data Breaches

One breach, 77 countries, dozens of rules

- Different triggers of reporting obligation — risk-based (EU) vs. data elements (US) vs. no threshold (Asia)
- Jurisdictional complexity — different applicability triggers in various statutes. Decisive criteria for reporting obligations: server location? Countries where individuals are located?
- Multiple regulators — DPAs, state AGs, sector regulators across regions
- Conflicting obligations — disclosure requirements vs. privilege & confidentiality
- Operational challenges — different forms, languages, tight deadlines (AI can help!)



3

ENFORCEMENT

Enforcement: Global Trends & Local Surprises

Same breach, different outcomes

- Common focus — response times, pre-breach security, vendor/supply chain oversight
- Significant inconsistencies — same breach: no response (most DPAs), acceptance (ICO/Hesse), or €5k fine (Bulgaria)
- Practical takeaway — plan for the strictest jurisdiction; expect the unexpected





THANK YOU!