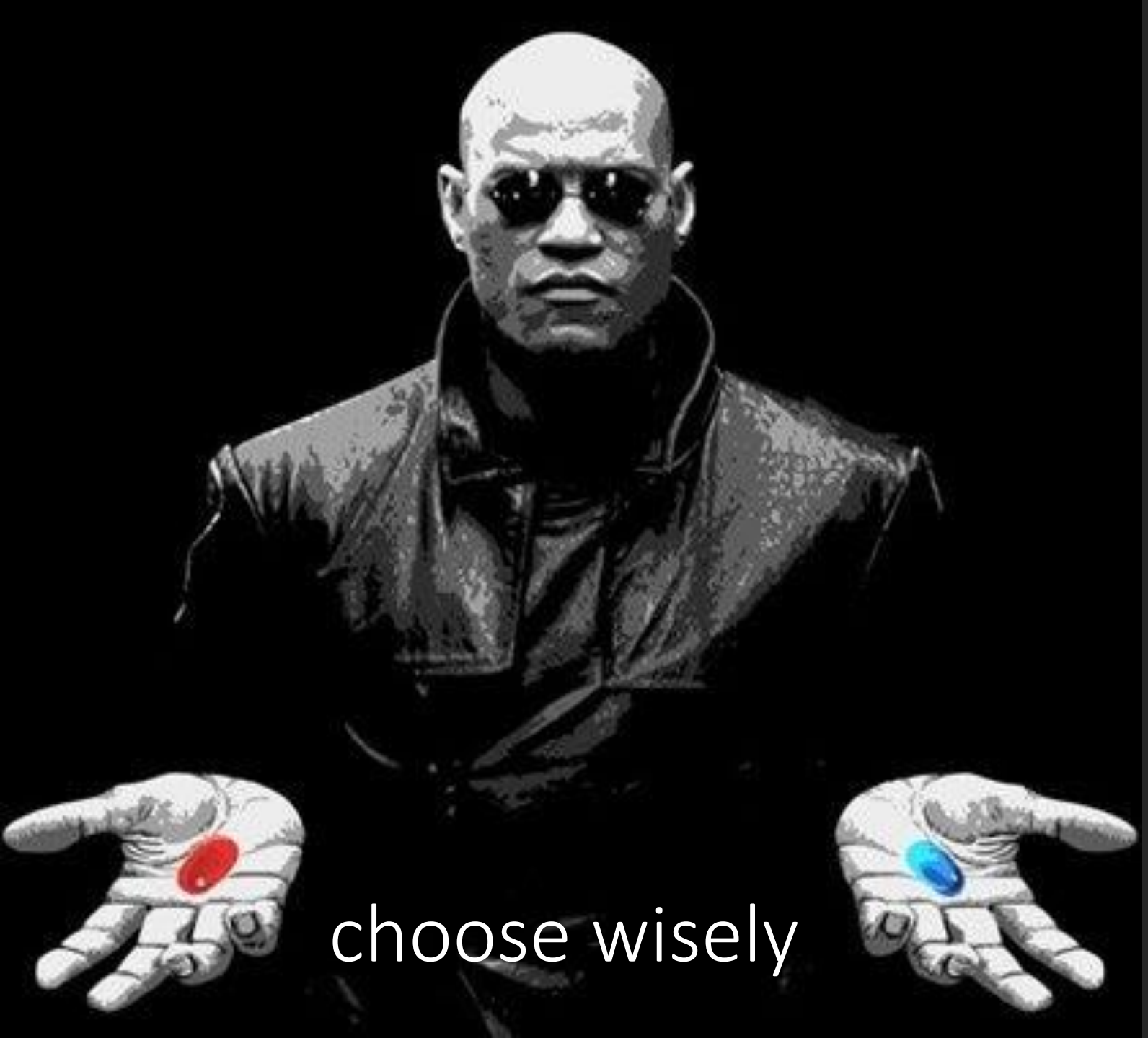
BSIDES Dublin 2022

Cyber Cluedo: using threat intelligence to defend & respond to cyber threats

Kevin Jones

Group CISO – Airbus

@CyberKevinJones



What can we do to stop cyber threats?

BSides Dublin

What is a modern enterprise?

- **Hyper-connected**
- **Complex**
- **(Big) Data Driven**
- **Mobile**
- **Cloud Integration**
- **Automation**
- **AI & Machine Learning**

… and in most cases; a bunch of stuff 10+ years old !

BSIDES Dublin

Cyber Security Transformation – what's new?

- **Connectivity Security**
- **End Point Protection**
- **Cloud Security**
- **Network Security**
- **Monitoring**
- **Red Team**
- **Human Centric Cyber Security**
- **.. and the 10 year old stuff !**

BSIDES Dublin

How’s that working out for you?

BSides Dublin

Who are these hackers anyway?

Dublin BSIDES

Cyber Threat Intelligence

Strategic

- Broader trends
- Organizations threat landscape & business risks
- Threat Anticipation

Operational

- Tactics, techniques, procedures (TTPs)
- Threat Actor Tracking
- Attack vectors, tools, infrastructure, etc
- Geopolitical events / conflicts

Tactical

- IP addresses, domains, hashes, etc
- Deep / Dark Web Monitoring
- Compromission lists
- Generally: technical in nature & machine readable

STRATEGIC

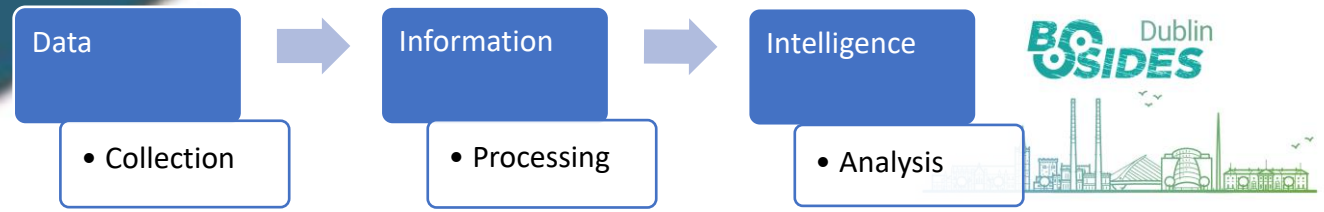
Identify the *Who* and *Why*

OPERATIONAL

Address the *How* and *Where*

TACTICAL

Focus on the *What*



Where is **TI** used in cyber security?

- Anticipation
- Risk Management
- Red Team
- Detection - SOC
- Incident Response / CERT
- Threat Hunting

BSides Dublin

Flaws and Misconceptions of Threat Intel

- We focus mostly on the tactical + a bit of operational. The strategic is often overlooked!
- Commercial & community feeds are best used together
- You can't (fully) automate … and don't believe the vendors who say they can!
- Threat Intelligence MUST
  - Have situational awareness
  - Be timely
  - Be actionable
- Sharing of intelligence is more common than you think! Aviation-ISAC, CERT to CERT, suppliers

BSides Dublin

The End Game Attribution

Threat Intelligence != Attribution

Tracking, Understanding, and Using attacker TTPs makes us better – but most organizations don’t (and shouldn’t do) attribution

Thank you

Questions?