

arcX Cyber Threat Intelligence 101 part 3

Day 16/365

Black hat hackers

'The unholy trinity'

- Nation Stated backed (or APT)
- Cyber Criminals
- Hacktivists

Motivation<

- NSB
 - Stealing intellectual property/information that can further a political aim
- Cyber Criminals
 - Directly stealing money or data that can be monetised
- Hacktivists
 - Further political goals or just causing chaos

Capability

The actor's ability to achieve their intent

Order according to capabilities

- NSB
 - CS
 - Hacktivists

Resources dictate this distribution

CIA Triad model

Confidentiality, availability and integrity

'CIA triad' stands for Confidentiality, Integrity, and Availability. It is a common model that forms the basis for the development of secure systems.

- **Confidentiality** - Confidentiality is to do with keeping an organisation's data private. This often means that only authorised users and processes should be able to access or modify data.
- **Integrity** - Integrity means that the data can be trusted. It means that it should be maintained in a correct state, kept so that it cannot be messed around with, it should be correct and also needs to be reliable.
- **Availability** - It's all well and good maintaining confidentiality and integrity but the data must be available to use. This means keeping systems, networks and devices up and running.

Being aware of these 3 concepts and how they overlap is important and as Stewart mentioned in the video, some organisations may lean more towards Confidentiality whilst others focus more on Availability depending on what their system or platform is being designed to do.

maps closely to intent

Intent

When an actor seeks to hack a system it does so with an intent

How is intent different from motivation?

Motivation is the why of the actor, intent is the end goal
