Cloud App Security & Microsoft Defender ATP

Why they are better together.

"There's two types of organizations: those who have been hacked, and those who don't know it yet…"
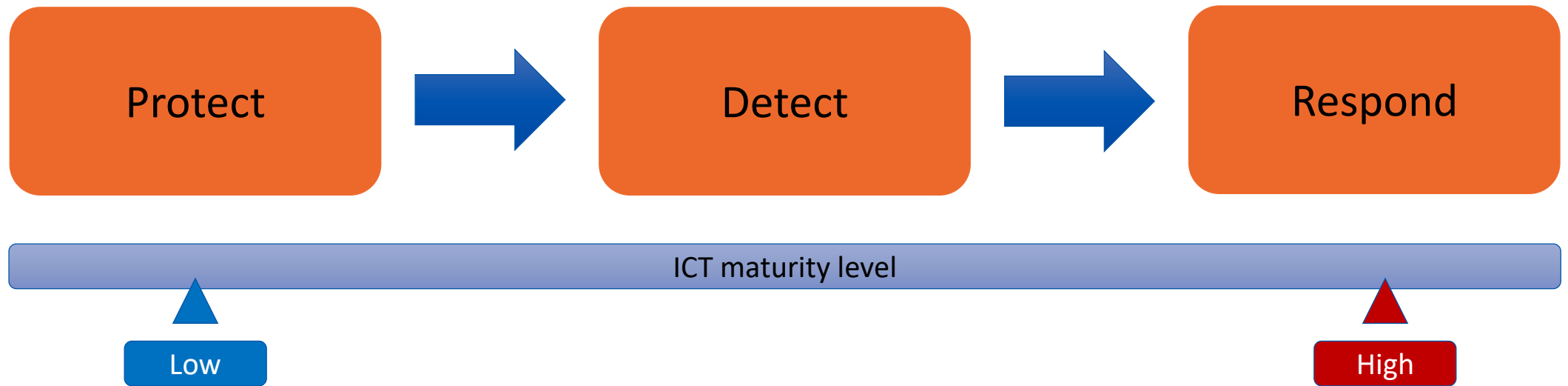
John T. Chambers

Threat landscape

- Data Theft / Data Loss
- Malicious software (malware, ransomware)
- Phishing
- Regulations
- …

Framework?

Various frameworks exist to aid developing a security strategy. Choose which one fits you best (if any). Ideally, combine them.

What to focus on?

Depending on your current security posture, you might want to first spend (most) efforts on developing a good/thorough **defense strategy** (protect)

Why use Cloud App Security?

Why use MDATP?

What is Threat Hunting?

The act of (proactively) searching for elements (e.g. activities) that previously weren't picked upon by existing automated detection (and correlation) systems.