ATT&CK for ICS Update

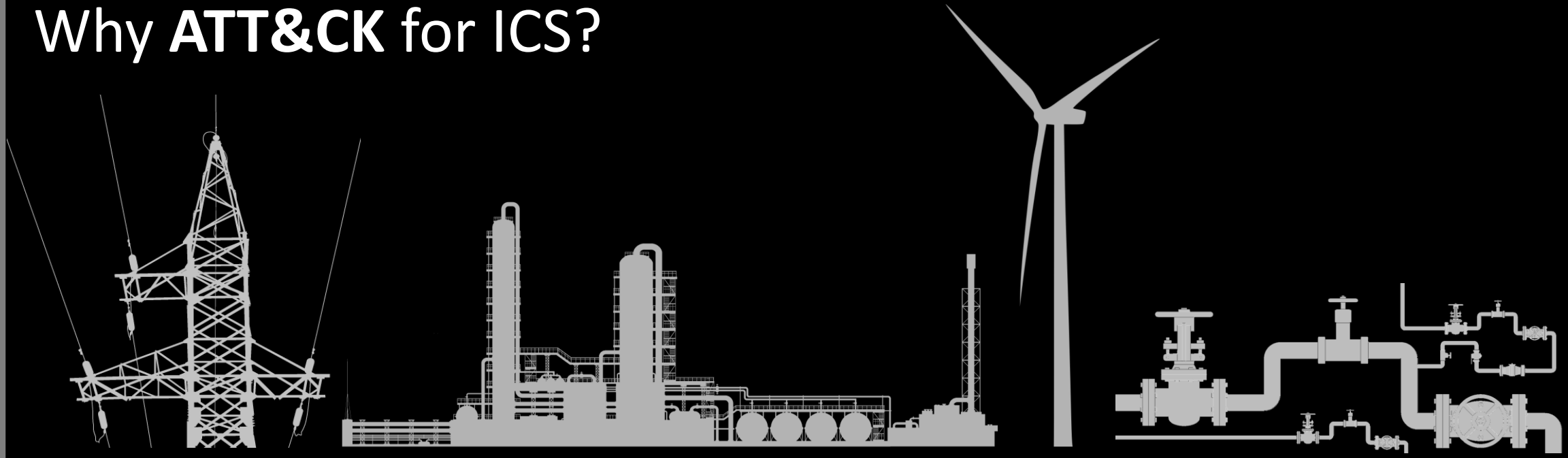
Otis Alexander
@ojalexander

@MITREattack

#ATTACKcon

MITRE

Why **ATT&CK** for ICS?



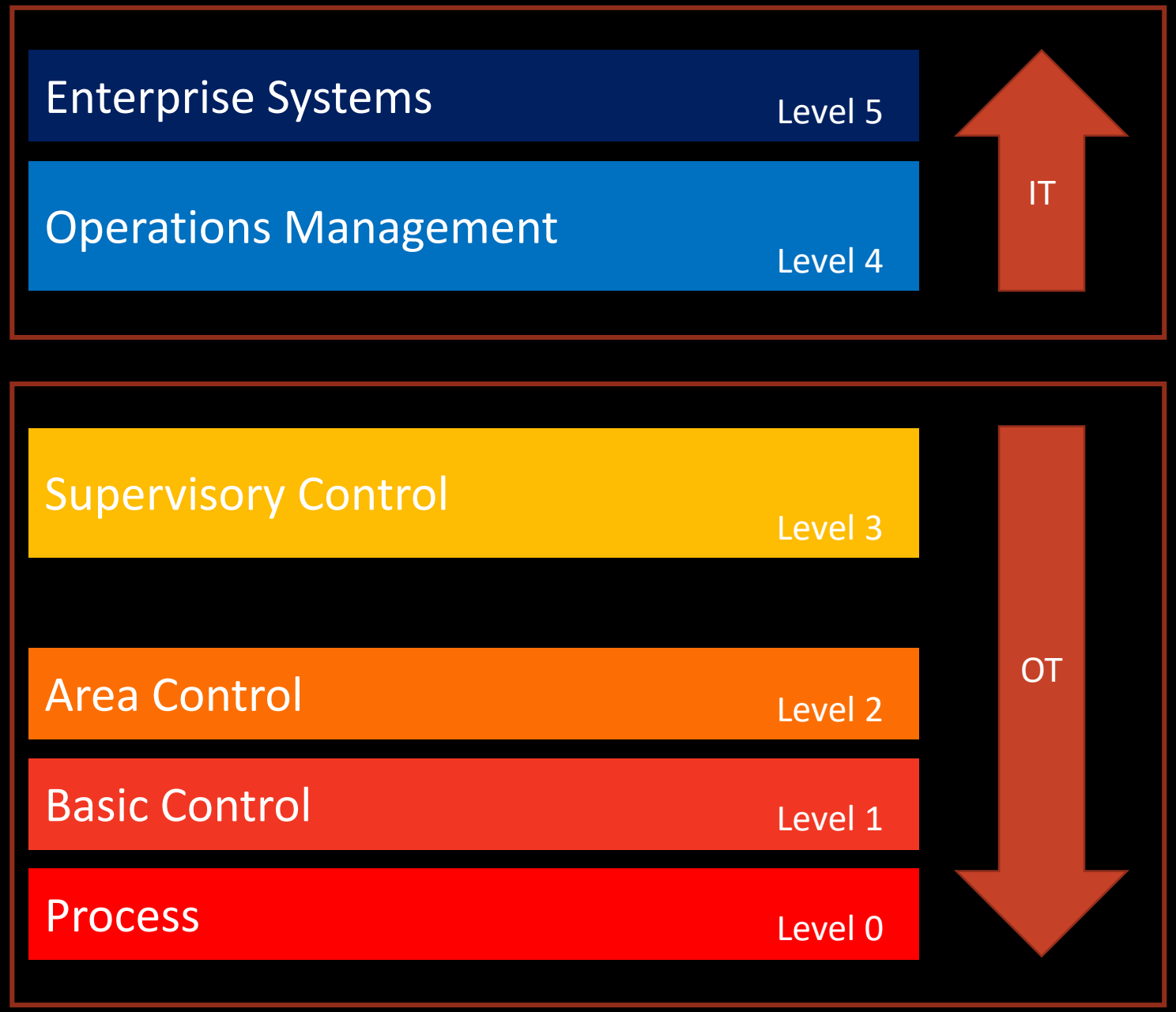
Unique Adversary Goals

Technology Differences

Different Defenses

ATT&CK

MITRE



Enterprise ATT&CK

ICS ATT&CK

A Sampling of Use Cases

Current

- Standardized Information Sharing
- Hunt and Incident Response Playbooks
- Analytic Development
- Adversary Emulation
- Criticality Analyses
- Analyst Training

Future

- Threat Modelling at the Design Phase
- Security Engineering
- OT SOC assessments

ATT&CK™

MITRE

Challenges

- **Lack of real world data**
- **Immature information sharing**
  - Lack of requirements or incentive
- **Non-standard data source interfaces**
- **Immature detection capabilities**
- **What's the proper level of abstraction**
  - Multiple domains
  - Diverse set of vendors
  - Many protocols
- **Scope**
  - Should we be including a broader scope of domains?

New Tactics Based on Feedback

Initial Access	The adversary seeks to access operational environments
Evasion	The adversary evades operators and defenses
Collection	The adversary collects artifacts to enable their operation
Inhibit Response Function	The adversary inhibits safety, protection, and quality assurance functions
Impair Process Control	The adversary seeks to manipulate, disable, or impair physical processes
Impact	The adversary's ultimate goal

ATT&CK™

MITRE

Status

- Currently in the 3rd major revision
- 83 individuals from 28 organizations have access as early reviewers
- Range of public and private participation
- Planned for release around December 2019
- Independent release initially to facilitate rapid response to feedback
- Currently available for review through an NDA

Otis Alexander
@ojalexander

ATT&CK™

attack@mitre.org
@MITREattack
#ATTACKcon

MITRE