CERT.be
The Federal Cyber Emergency Team

MITRE ATT&CK at CERT.be

Trey Darley
CTI Strategist

EU ATT&CK Community Workshop
Dommeldange, Friday 25 October 2019

TLP:WHITE

Who am I?

- CTI Strategist, CERT.be
- OASIS CTI Technical Committee co-chair (with Richard Struse, father of STIX/TAXII)
- @treyka on the Twitters (and pretty much everywhere else…)
- trey.darley@cert.be

CERT.be and our constituents

- Operators of vital interest (NIS list) are key constituents.
- EWS: Belgian Early Warning System
- Capturing our constituents' intelligence requirements is key.
- MITRE ATT&CK is not a threat model, but it provides a framework and building blocks for developing threat models.

EWS: what problems are we trying to solve?

- Prevent bad stuff from happening (left of boom)
- Decrease MTTD/MTTR when incidents occur
- Inform tactical and strategic decision-making by building a mature sightings ecosystem at the sectorial and national level

How does ATT&CK help?

CSIRTs are at different levels

- Crawl, walk, run

Building feedback loops with our constituents

- It helps to know when things we do help and when they don't.

Building feedback loops with our peers

- Where is there room for improvement in how we tag CTI?
- Is there room for standardizing how we capture adversary behavior during IR?
- Capacity building between higher and lower maturity CSIRT teams

Harmonization of approaches

- Premature standardization is bad.
- Are we far enough along that it makes sense to begin harmonization yet?
- What would this (potentially) solve?

This slide intentionally left blank

- The future is not yet here, but it's coming…

Questions? Comments? Comments disguised as questions?