NEW CONTEXT

Borderless Cyber Asia

STIX – Lessons Learned

BACKGROUND

- We are a Digital Garage Company and New Context was founded 3 years ago to build stronger Industry Internet through its Lean Security practice.
- New Context has been working with the US energy sector for the last 2 years to represent Operational Technology threats within SCADA infrastructure
- Contributors to STIX/CYBOX through Oasis CTI Committee
- Partners with Soltra for deployment and integration of intel into enterprise systems and operational environments.

CHALLENGES TODAY

- Building the CTI sharing network and building adoption
- A lot of reliance still on F2F
- Significant weight on any PDF & Emails the need to translate these into STIX in a more sharable portable format.
- As you look at products, make sure that those products that advertise STIX/TAXII actually implement the model well.
- Support the adoption, and not underestimating the effort for your IT organization
- Legal getting in the way of progress. A parallel approach, give IT the ability to implement while you figure out the legal challenges. Don’t wait till the very last minute hoping IT will be able to just quickly deploy STIX into their ecosystem

LETS TALK ABOUT THE FUTURE

- Lessons Learned from Research & Development of Using STIX to describe the future
- We come from the machine automation side looking out how do we describe threats, that haven’t materialized yet.
- Patterning, and Temporal Challenges
- Complexity is the enemy, working to continually simplify for scalability
- Translating Use Cases into real Indicators – Being aware of false positive, false negatives, building in appropriate testing and automation

TO INFINITY AND BEYOND

- We are at the beginning of the journey
- The stronger we build our infrastructure the more we can innovate