Cyber Threat Intelligence (CTI): Automating information sharing with STIX, TAXII, CybOX

Increasing Importance of Awareness of Data

Takahiro Kakumaru, CISSP
NEC Corporation
t-kakumaru@ap.jp.nec.com

OASIS Borderless Cyber Asia (November 1-2, 2016 @Keio Univ.)
NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow. We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs. Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.
Topics

Increasing importance of awareness of data in order to enhance current security posture

I. What could CTI change security posture?

II. Data handling is important to carry forward CTI

Takahiro Kakumaru, CISSP
NEC Corporation
Cyber Security Strategy Division
- Member of OASIS CTI-TC
- Advocate of CTI adoption
What could CTI change security posture?

Enhancing awareness of data is key to make security possible

1. **Large amount of data generate new intelligence**
   - Quantity turns to Quality by processing large amount of data and analyzing it.
   - What data should we collect? What information should we transform?

2. **Make security mechanisms more efficient if we share information**
   - CTI provides platform to exchange between organizations for better security controls.
   - How should we connect information newly? Reforms to our attitudes as well.

3. **Whether good or bad of AI would be depend on collected data**
   - CTI provides platform to collect data and information about cyber threat.
   - Quality of intelligence source need to be looked after if we leverage AI.
II. Data handling is important to carry forward CTI

To handle data properly, we should be aware of ...

1. **Ensuring a variety of intelligence sources**
   - It is also important to utilize what we monitor, observe, and sight by ourselves in real time.

2. ** Clarifying ownership of shared data**
   - How to protect ownership of shared data? Taking on a contract is considerable.

3. **Ensuring quality of data, information, and intelligence**
   - There are noise on data, bias on information, and morality on intelligence.

4. **Ensuring security of data we treat**
   - Security include devise security, system security, and vulnerability of human.

5. **Understanding and adapting to legal systems of each country**
   - Legal systems are different for each country, e.g. EU Data Protection Directive.
I. What could CTI change security posture?

- CTI provides platform to exchange, collect, and analyze.
- CTI requires not only technology, but also change of mind.

II. Data handling is important to carry forward CTI

- A variety of intelligence sources, and ownership of data.
- Quality of data, security of data, and aware of legal systems.