Threat Modeling Control Ontology

Asset-level controls to prevent, detect, and respond to a threat

A Control Ontology allows device manufacturers to map to its threat vectors to identified loss scenarios (risk) and document their mitigating Prevent, Detect, and Response controls.

- Ontology branches represent control functions specific to its associated tree
  - Vulnerability Tree
    - Threat Event Detection
      - **Visibility** of Threat actions (logging)
      - **Recognition** of logged actions
      - **Reporting** (escalation) of recognized actions
        - Triggers to **Response**
    - Threat Event Response
      - Controls that Limit **Contact**
      - Controls that limit **Actions** to reduce spread of the threat
- An Ontology allows a device manufacturer to:
  - Map controls to ontology branches to identify a specific risk scenarios controls
  - Map Ontology branches to NIST CSF subcategories
  - Perform control gap assessments and;
  - Communicate shared control responsibilities with end users
- Ontologies meet Section B: Risk Management Documentation of Premarket Guidance
  - Section B-1: *List all cybersecurity risks considered in the design of your device… [likelihood of] exploitability*
  - Section B-5: *…Matrix that links actual controls to the risks that were considered in your security risk and hazard analysis*

Example of a Threat Ontology

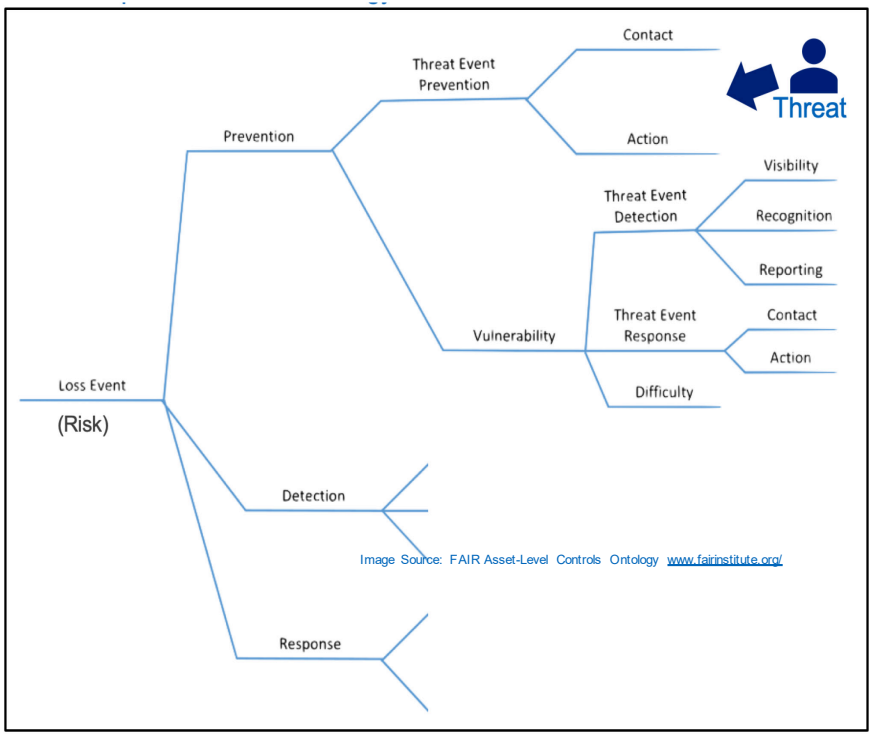

Image Source: FAIR Asset-Level Controls Ontology www.fairinstitute.org/

Jason Tugman, Axio VP Cyber Risk jtugman@axio.com
www.Axio.com | 2019-01-29 FDA Threat Modeling Panel