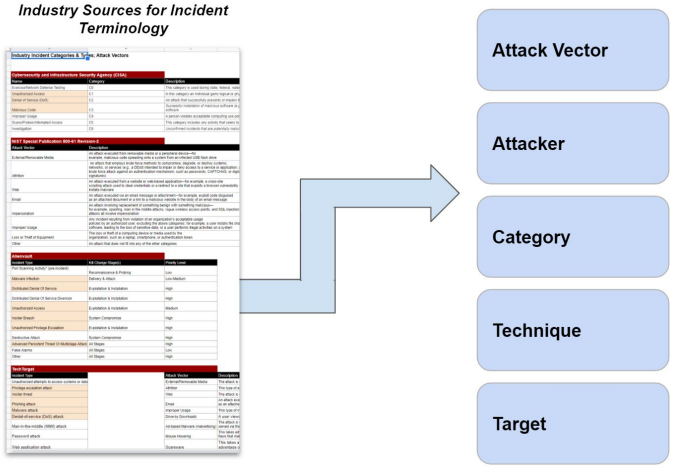
DAYBLINK

Threats, Risks, & Vectors - The Lexicon Problem

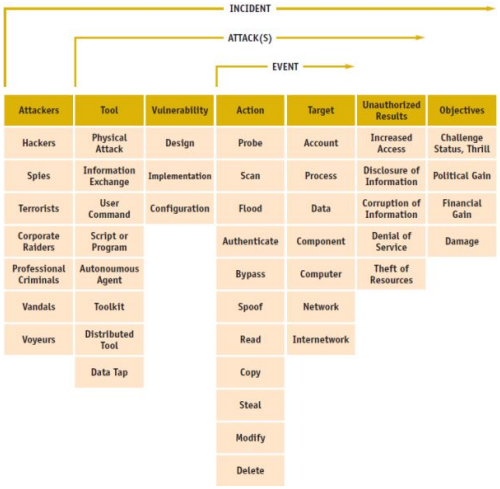
SOC & Incident Response teams need a well-defined incident classification system in order to quickly & consistently respond to cyber events, however:

- Most SOC platforms only offer a pre-defined incident type hierarchy and a predefined list of categorizations, except at the most customized enterprise service levels
- Industry, regulatory, and thought leaders all offer different types of incident classifications without one centralized authority leading to multiple types of terminology, taxonomy, and hierarchy
- Several “standard” threat classifications exist, but it isn’t clear that threats (i.e. pre-incident) may be a good model for Incident classification. For example, “threats” or “threat vector” should seemingly be a ***subset*** of any incident taxonomy

Industry Sources for Incident Terminology



A typical solution: Take an aggregation of all the industry frameworks and come up with a few vague categorizations without much definition



A (more) elegant solution: As developed by ENISA (1), this model leverages parent <> child relationships and builds along an attack lifecycle

Starting Point for a Solution

Although we may not have a universal solution - there are a few key pieces that can help Incident Response teams to more consistently categorize and react to security incidents in order to bring their products and operations back to BAU faster and stronger

1. **Identify a Minimal Viable Dataset -** Identify the key categories and metadata your SOC needs to action against
2. **Define parent-child relationships** - Consistency in action requires consistency in categorization
3. **Set a baseline - but stay flexible** - An incident taxonomy should have a standard framework, but is also allowed to change based on attacks, technology, or ecosystem

(1) Common Language Security Incident Taxonomy - as developed by ENISA (European Union Agency for Cybersecurity) in their January 2018 report

To learn more about DayBlink Cybersecurity or for additional insight into implementing the cybersecurity measures above, please visit www.dayblink.com or contact:
Jacob Armijo (jacob.armijo@dayblink.com), **Michael Morgenstern** (michael.morgenstern@dayblink.com), **Justin Whitaker** (justin.whitaker@dayblink.com)