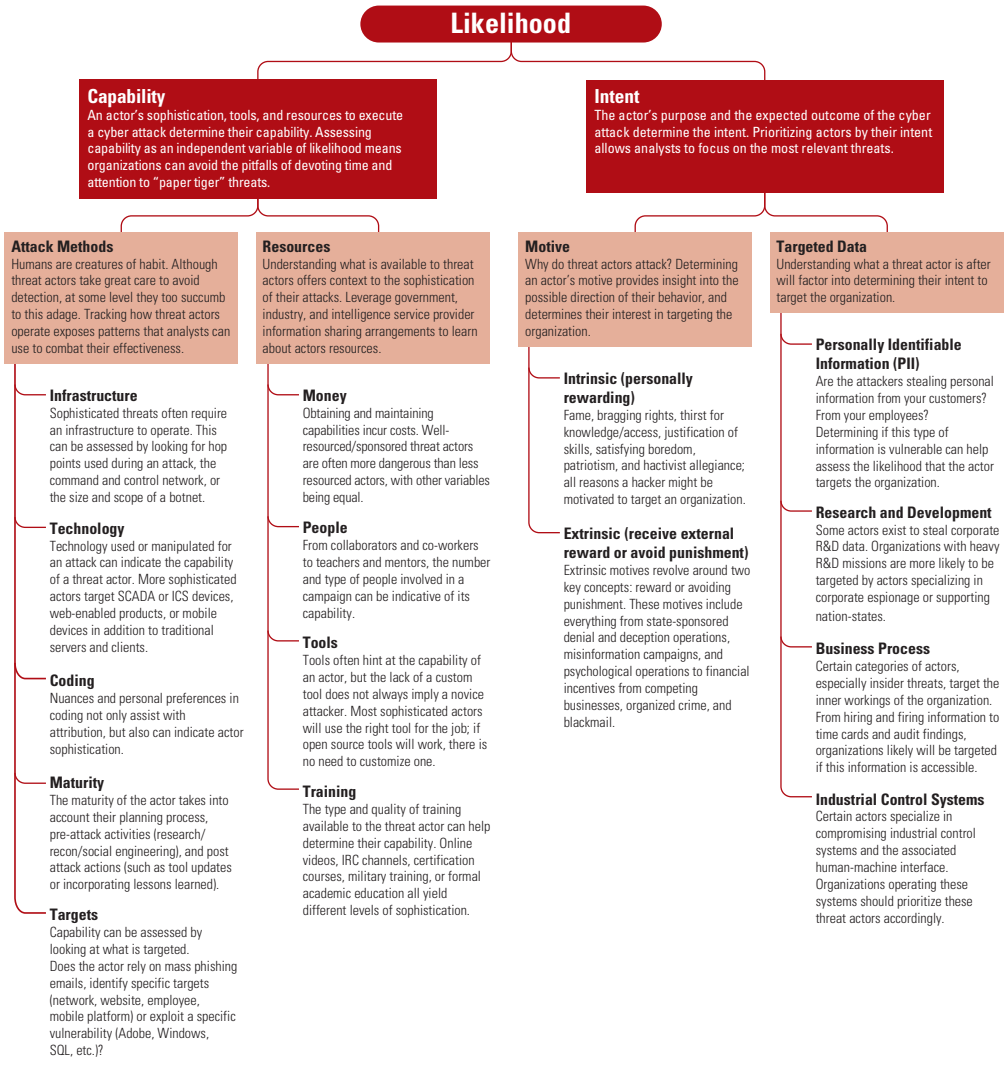
Likelihood

Understanding the capabilities and intentions of cyber threat actors determines the likelihood of them targeting an organization. To determine this likelihood, a CITP participant from industry monitored open source publications from an organization known to sponsor cyber threat actors who frequently targeted the organization. Analyzing this accessible data provided insight into the motivations of the sponsored cyber threat actors, allowing the CITP participant to narrow down the types of data likely to be targeted, and work with network security experts to create diversions, honey pots, and employ other measures to proactively defend against the threat.



Indicators of Success

- Analysts have a repository of current and historical threat actor tactics, techniques, and procedures (TTPs) to generate profiles that are fed into data collection platforms to separate known threats that automated defensive actions can mitigate from unknown threats requiring an analyst's attention.
- Analysts gain perspective on the tools threat actors use to assess how they access an organization or if they outsource tool development. A basic netflow analysis could show the majority of attacks come from well known, prepackaged scripts, which analysts can easily combat using remediation efforts posted on open source websites.
- Analysts realize that sophisticated actors use the lowest common denominator for attacks. If a threat actor can use an off-the-shelf tool to accomplish their goal, they'll wait to deploy customized tools on harder targets.
- Analysts understand that the targeting of Adobe or Windows software vulnerabilities usually equates to a threat of lower sophistication than one targeting Windows operating systems.
- Analysts understand threat actors' intentions well enough to assign them to different categories, such as nation-state, criminal, hactivist, recreational, or competitor; enabling them to identify the most likely threats their organization faces through profiling.
- Analysts realize that if a threat actor is targeting their organization for fame, the likelihood increases for the actor to choose a DDoS attack to the organization's website as the attack method.
- From their organization being the first result in a Google search to knowing over what holidays certain actors like to conduct attacks, analysts recognize the importance of timing when it comes to assessing the overall likelihood of a threat.