FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

ASSESSMENTS

TLP:AMBER

ASSESSMENTS DEFINE THE PROGRAMS WE NEED

- **Vulnerability Assessm**ent: Looks at the *avenues* of attack; identifies weaknesses that can be exploited, and how.
- **Threat Assessment**: Looks at the *likelihood* of an attack. Who has the capability and intent? Who has necessary skills to overcome the target's defenses, or exploit its vulnerabilities? and how might an attack unfold, unfold based on the group or individual's capabilities and Modus Operandi?
- **Risk Assessment**: Looks at the *consequences* of an attack: "What's the worst that could happen?" "What would it cost, in terms of lives and assets?" *or* "What have you got to lose?"

VULNERABILITY ASSESSMENT

- **Vulnerability Assessment** looks at your facility through the eyes of the adversary
- Looks for the weak spots through which the adversary could attack
- By identifying and mitigating the vulnerabilities, you can remove/ resolve myriad threats. It's a good starting point.

THREAT ASSESSMENT

- **Threat Assessment** identifies *who* in the environment has the *capability* and *intent* to harm you.
- If they don't have the capability to harm you, or the ability to exploit your vulnerabilities or overcome your defenses, they're no threat.
- If they have the capability to harm you, but neither the intent nor desire, they're no threat.
- Each threat actor presents a unique combination of capability and intent. The role of intelligence is to identify the actors who have the intent to harm you… and determine their capabilities.
- Once you know their capabilities, you can see if you are vulnerable to an attack from them.

THREAT = *f* (Actor, Access, Intent, Capability)

- ***Inter alia***, if you have already hardened your target, you can determine if potential adversaries **have the capability to overcome your defenses.**
- **Know Your Barriers And What They Do**: If the adversary doesn't possess the requisite skills / resources to overcome your barriers, they don't pose a threat.
- If they DO possess the skills and resources, you must strengthen or upgrade your defenses, but at least *now you know who and what you're protecting against*.
- ***Perceived vs Actual Threat*****:** Without a threat assessment, you may be protecting against nothing, the wrong thing, and buying hardware or developing skills you're unlikely to need.

RISK ASSESSMENT

RISK = f (Vulnerability x Threat x Consequence)

- Risk assessment looks at the *probability* and *consequences* of an attack
  - How *likely* is an event to occur?
  - What are the *possible* and *probable consequences* if it were to occur?
- Risk Assessment is important because you don't want to spend more on protecting an asset than it's worth – *nor do you want to skimp on protecting something whose loss would be incalculable*.

ROLE OF INTELLIGENCE

Intelligence

- Reveals whether new actors have appeared in your environment
- Identifies their intent and capabilities
  - Whether old actors are saying things that would indicate a change in their intentions
  - Whether they have developed new skills that now render you vulnerable

Each news item, each new reported action, each **S**uspicious **A**ctivity **R**eport (*SAR*) provides information about threat

- Does the SAR indicate anything new? Reflect a new interest? A new intent? A new capability or skill?
- Does the SAR indicate you have a new vulnerability?
  - If yes, mitigate
  - If no, carry on, but keep looking.