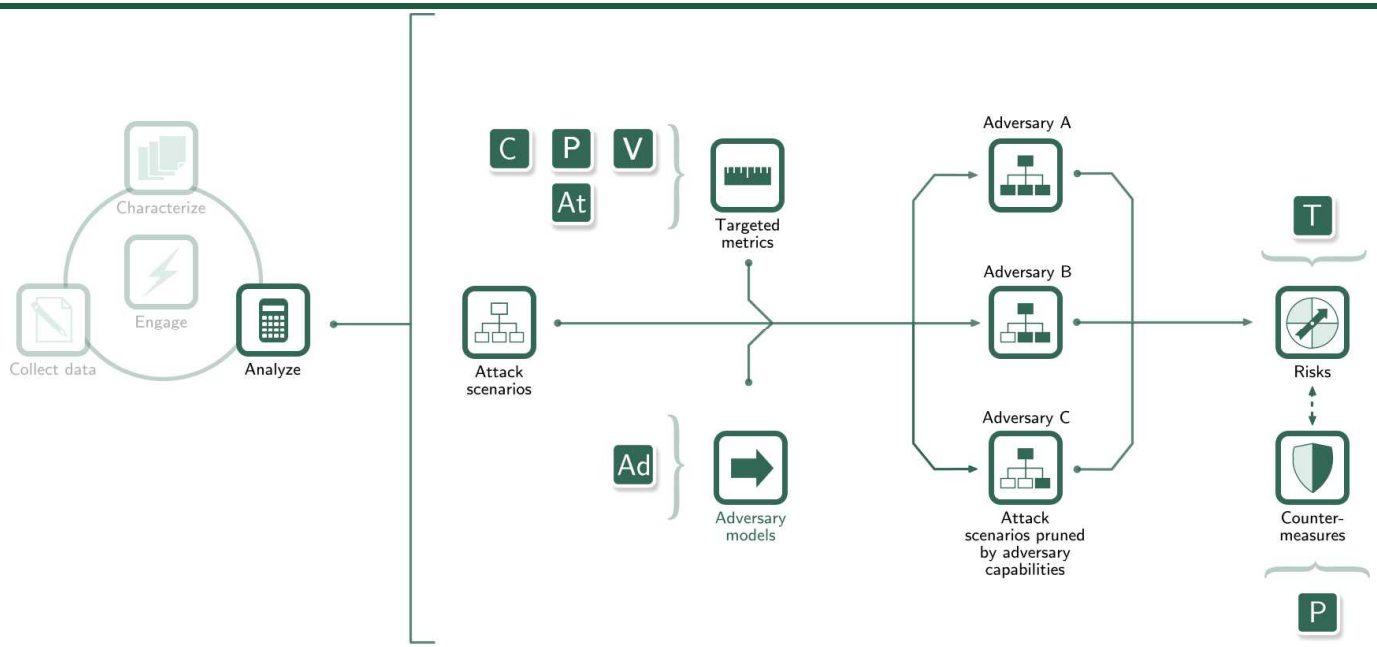
SAND2008-7993P

Analyze Risk Associated with the Target Metrics

Analyze Risks



- In this process, the RED TEAM
  - models possible attack scenarios,
  - analyzes the risks associated with each scenario by comparing the capabilities required to achieve the scenario with the capabilities the posited adversaries possess, and optionally
  - models effectiveness of notional countermeasures (in “what-if” style).

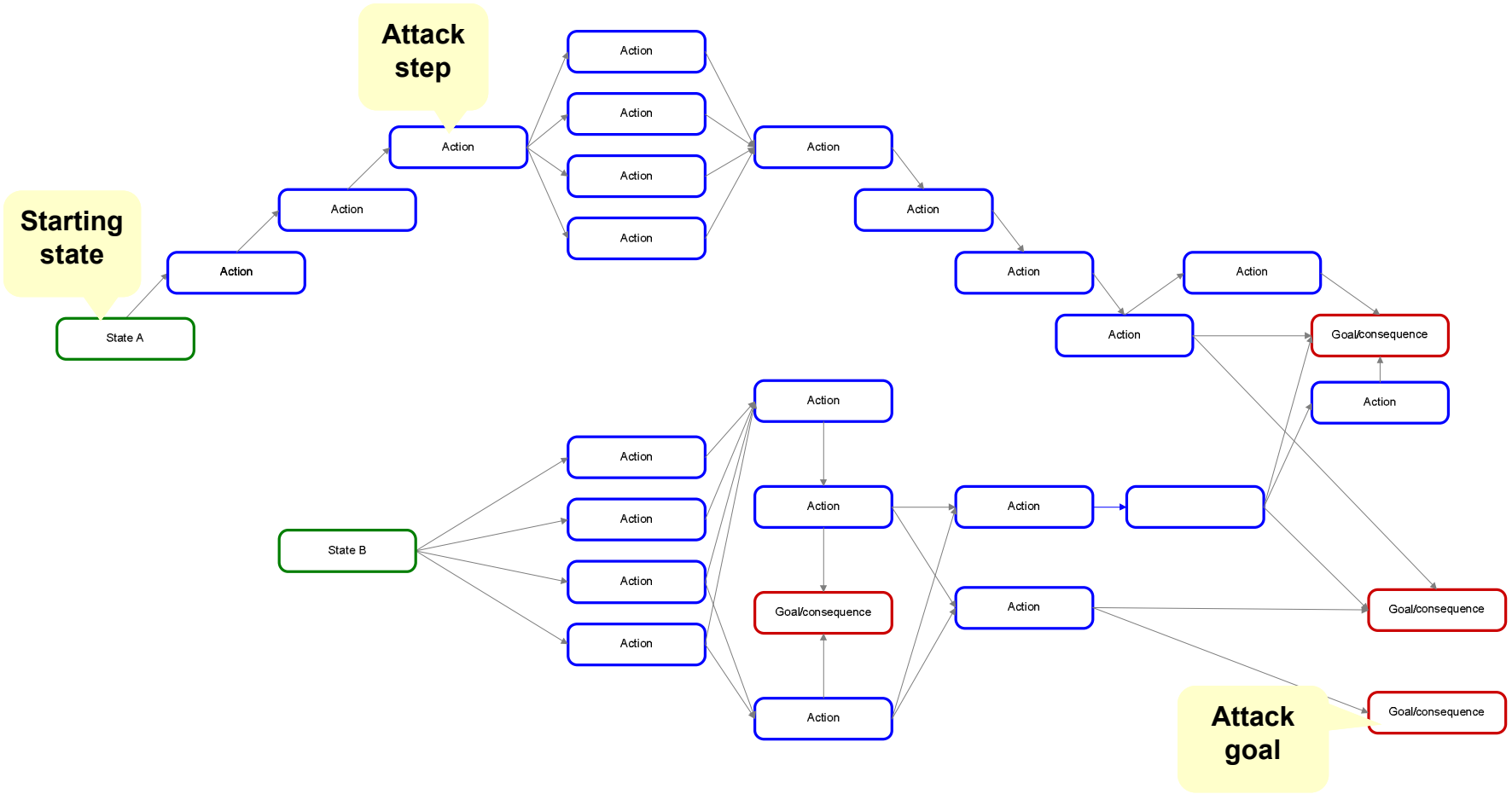
Generalized Process

- Model attack scenarios as collections of discrete actions
- Determine the cost and benefit of each attack scenario from the red team's perspective
  - associate metrics with the discrete actions, and
  - assign values to each action's metrics.
- Compare the attack scenarios
  - assess the adversaries' ability to achieve attack scenarios, and
  - rank the scenarios based on a more detailed assessment of consequences, capabilities, and preferences.

Using Graphs to Model Attack Scenarios

- Attack graphs
  - are a useful communication tool,
  - highlight common elements,
  - eliminate redundancy seen in attack trees,
  - communicate attack sequences,
  - identify end states or attacker goals,
  - show entry points to the goals using attack steps, and
  - reveal paths that represent attack scenarios.

Example Attack Graph



Attack Tree Analysis

- Attack trees
  - circumvent the need to define a probability of attack,
  - force adoption of the attacker's perspective,
  - are conceptually straightforward and analytically transparent,
  - models are flexible and reusable, and
  - the tree building process encourages collaboration and learning.

Section Three Exercise

(Active Demo of SecurITree)

- To analyze risk, the red team uses SecurITree to model attack scenarios and analyze risk of different adversaries

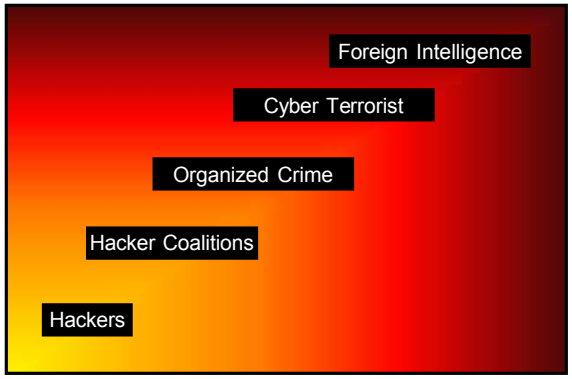
(Analyze risks associated with the target metrics)

- **Exercise: as we walk through a demo of SecurITree, identify additional metrics to use as indicators**

(Hint: review metrics that were discussed in Exercise One)

Adversary Models

- Original IDART™ models lacked adequate structure and definition, and included
  - *Outsider category*
    - *Nation-State*, *Cyber Terrorist*, …
  - *Insider category*
    - *Application Designer*, *Network Administrator*, …



- Newer IDART models employ generic categories with a better defined structure and basis
  - focusing on threat levels not adversary names, and
  - providing a range of capability and resource factors.

Attributes of Generic Threat

Commitment Family

- Intensity
- Stealth
- Time

Resource Family

- Technical Personnel
- Knowledge:
  - Cyber
  - Kinetic
- Access

Generic Threat Matrix

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Goal Commitment Intensity

- How committed is this adversary?
- H – willing to expend life of group member(s), highly motivated to achieve goals no matter the obstacle
- M – willing to have group member caught, captured, or go to prison
- L – group is not willing to risk being caught or captured, won't put themselves at risk

Stealth

- Adversary's required level of stealth necessary to achieve goal
- If required level is not maintained, goal will not be achieved
- H – loss of stealth cannot be tolerated
- M – loss of absolute stealth can be tolerated, or total stealth cannot be achieved due to other restrictions
- L – stealth is not required prior to execution, or stealth is not considered important to group

Physical Access to Cyber Assets

- Insider component to threat profiles
- H – has access through employment or turned insider, long-term commitment and local presence
- M – short-term physical access available through blackmail, coercion, or breaking & entering
- L – access available only through unscheduled opportunity, if at all

Cyber Skills

- Level of cyber skills contained within the adversary organization
- H – all levels of knowledge and skills, maintains a training program or R&D program in infosec
- M – mix of practitioners, low-level internal education capability, some limited R&D skills
- L – minimal skill with IT, limited coding, no training or R&D program

Implementation Time

- Adversary time available for planning, developing, and deploying a cyber attack
- Decades/Years – lots of lead time available, they're in it for the long haul
- Years – several years available
- Months – only months are available, possibly due to technology turnover
- Weeks – little time devoted to planning, development, and implementation; more likely to be "off-the-shelf" in nature

Cyber Organization Size

- Size and social networking ability of the cyber portion of the organization
- Hundreds – large-scale, with good communications
- Tens of Tens – many small groups with loose communication, limited relationship between groups
- Tens – small workgroups working independently
- Ones – individuals working independently

Countermeasure Analysis

- Indicator values of select nodes can be changed to model notional countermeasures
  - a task that requires a skill level of 3 might increase in difficulty to a skill level of 5 when the defender implements a countermeasure at that point in the tree
- Allows the analyst to find the likely points for the most effective countermeasures
- Can use attack graphs to identify optimal points in adversary attacks for countermeasures and trees to model impact on risk

Questions?