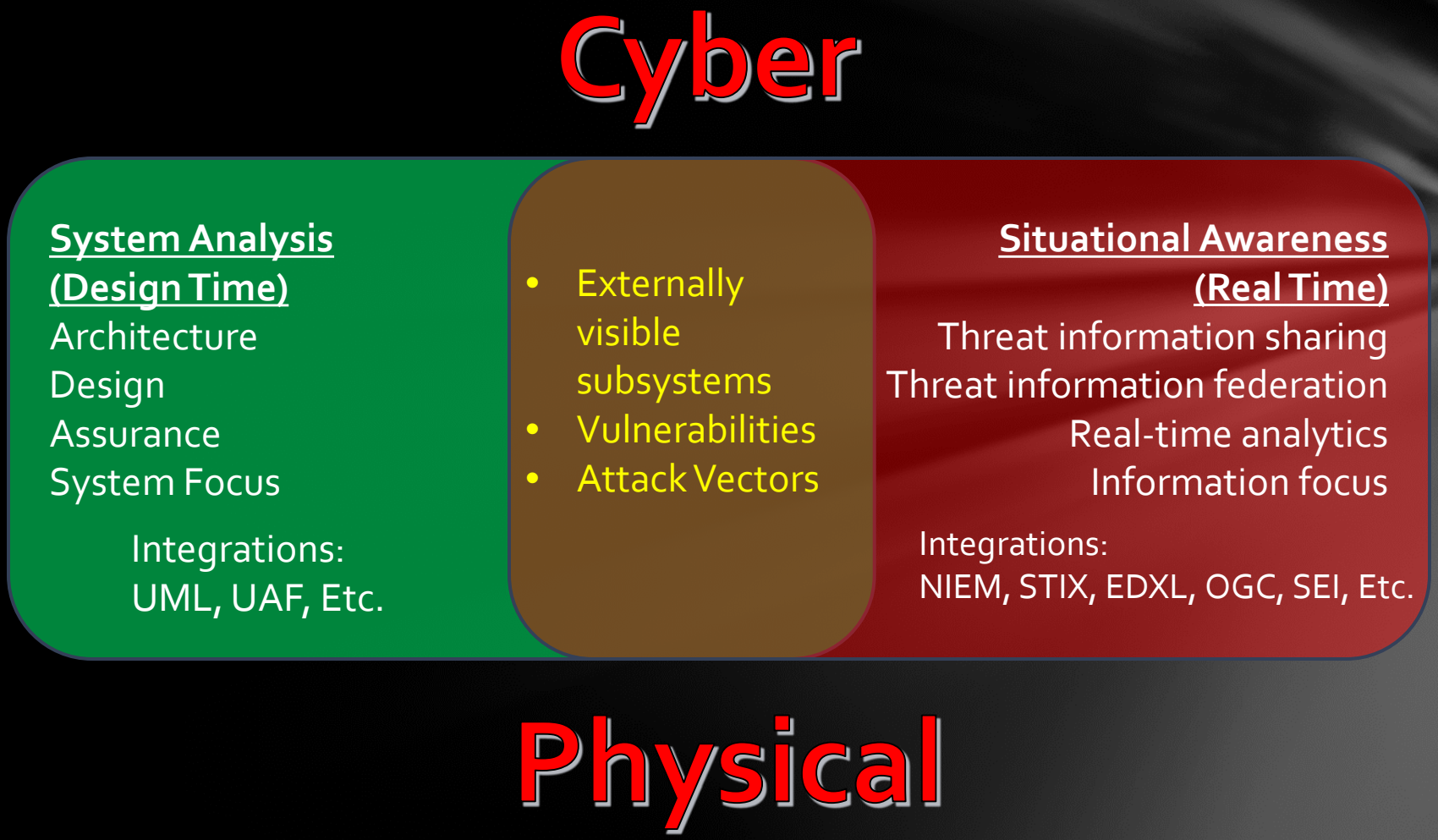
Operational Threat & Risk Information Sharing and Analytics

TEAM Threat

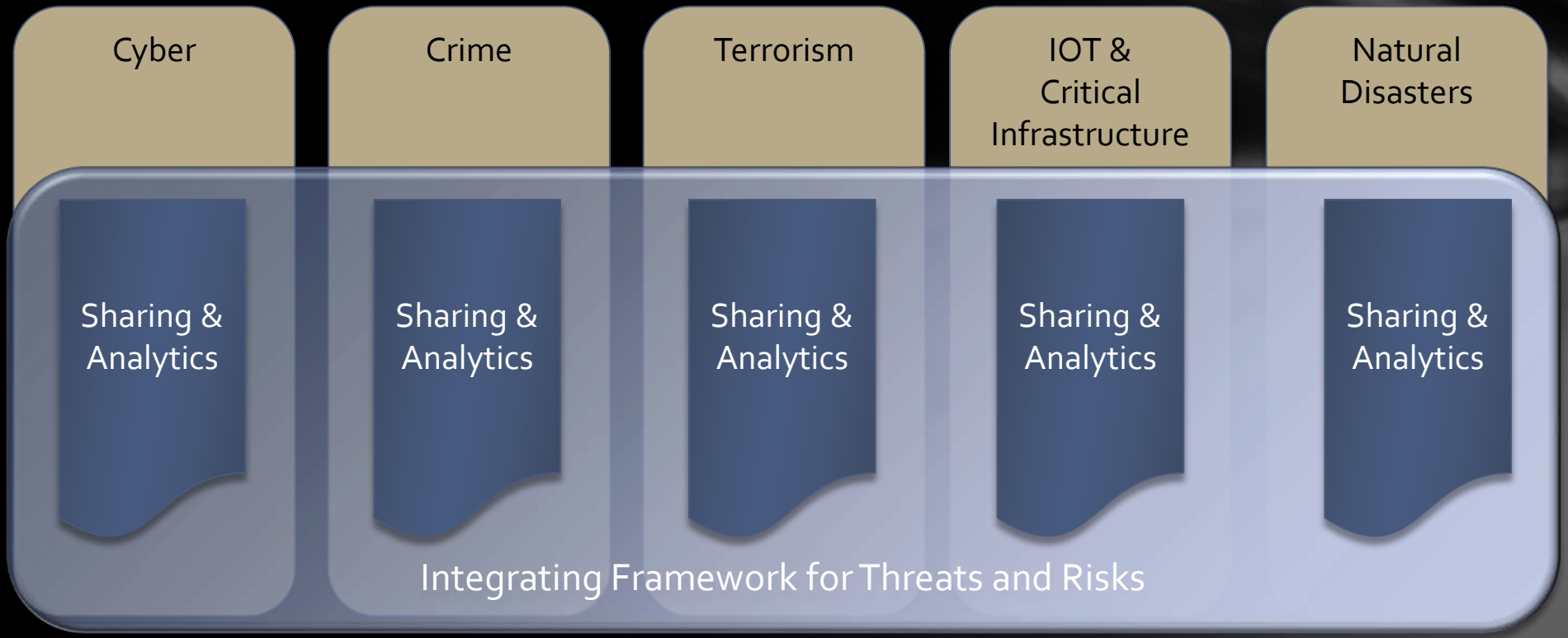
OMG
WE SET THE STANDARD®

ISE
ORACLE
IBM
demandware
move faster, grow faster.
Model Driven Solutions
Where Business Meets Technology
U.S. Department of Defense
DEFENSE SECURITY SERVICE
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CAL OES
KDM Analytics
FUJITSU
RSA
INTELLIGENCE DRIVEN SECURITY
NIST
LOCKHEED MARTIN

Situational awareness across cyber/physical threats and risks



What we need is an integrating framework that supports automated data mapping



An integrating framework that helps us deal with all aspects of a risk or incident

A federation of risk and threat information sharing and analytics capabilities

Our reality today is thousands of systems, interdependent

The problem is less building systems, it is the interoperability and interdependence of systems

- Of data
- Of processes
- Of missions

Welcome to the white space

The methods, processes and standards developed for system building, are not serving us well for this new reality.

But the information, processes and content in "other systems" are critical for each systems mission.

Our new reality is the white space between systems – how they work together

Conceptual Model Packages

Generic Concepts

Abilities

Actors

Assessment

Contact Information

Containment

Control

Credentials

Cyber

Enterprise

Entities

Events and Activities

Identifiers

Intent

Location

Objectives

Observations

Generic Concepts

Organizations

Patterns

Persons

Physical Entities

Places

Policies

Predictions

Processes

Quantities and Units

Resources

Responsible Performers

Rules

Situations

Time and Temporality

Vendors and Producers

Threat and Risk Specific Concepts

Attack/Defense Trees

Campaigns

Danger

Danger Categories

Danger Sources

Incidents and Failures

Indicators

Risk

Risk Treatment

Threat Actors

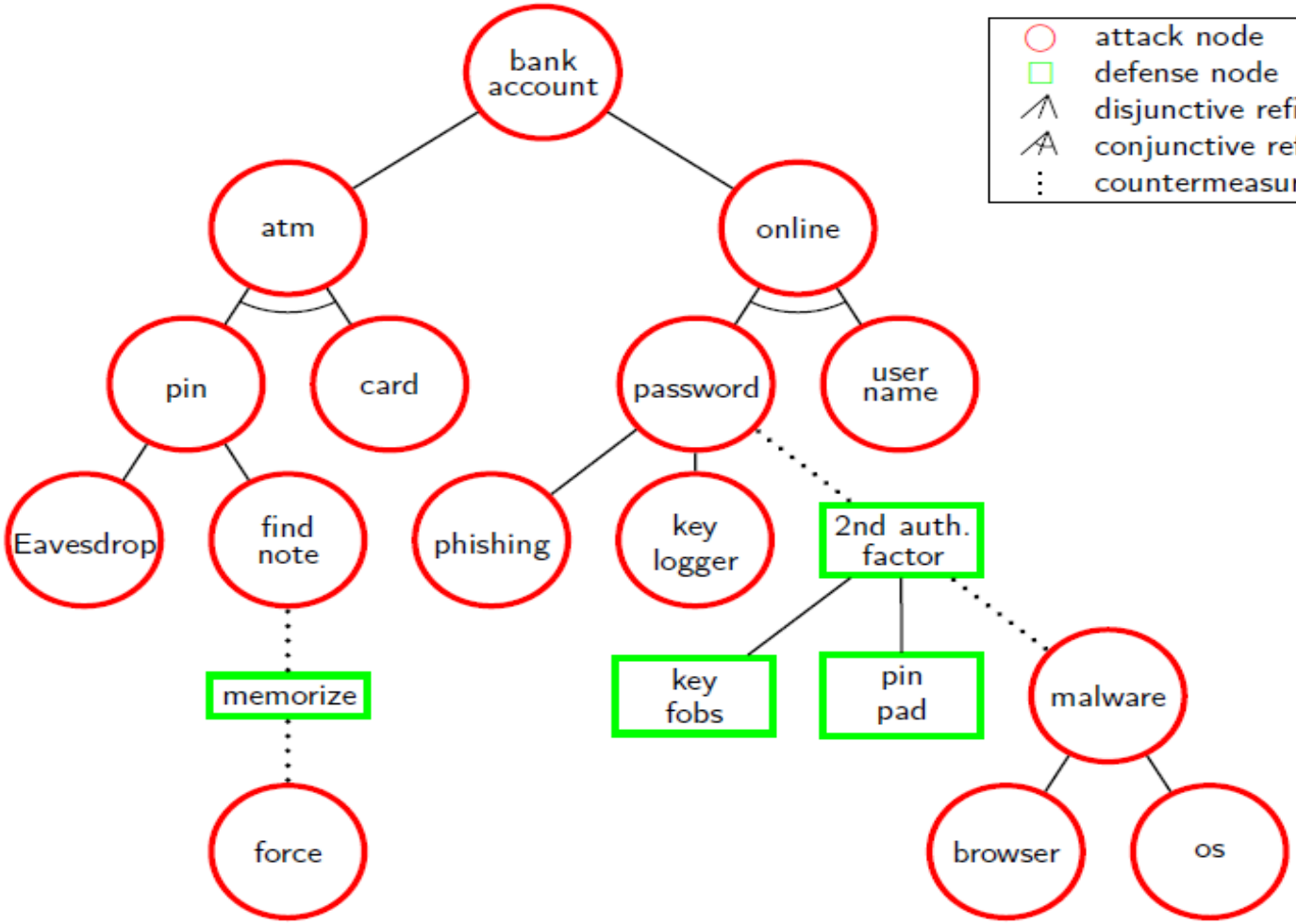
Undesirable Situations

Vulnerabilities

Weapons

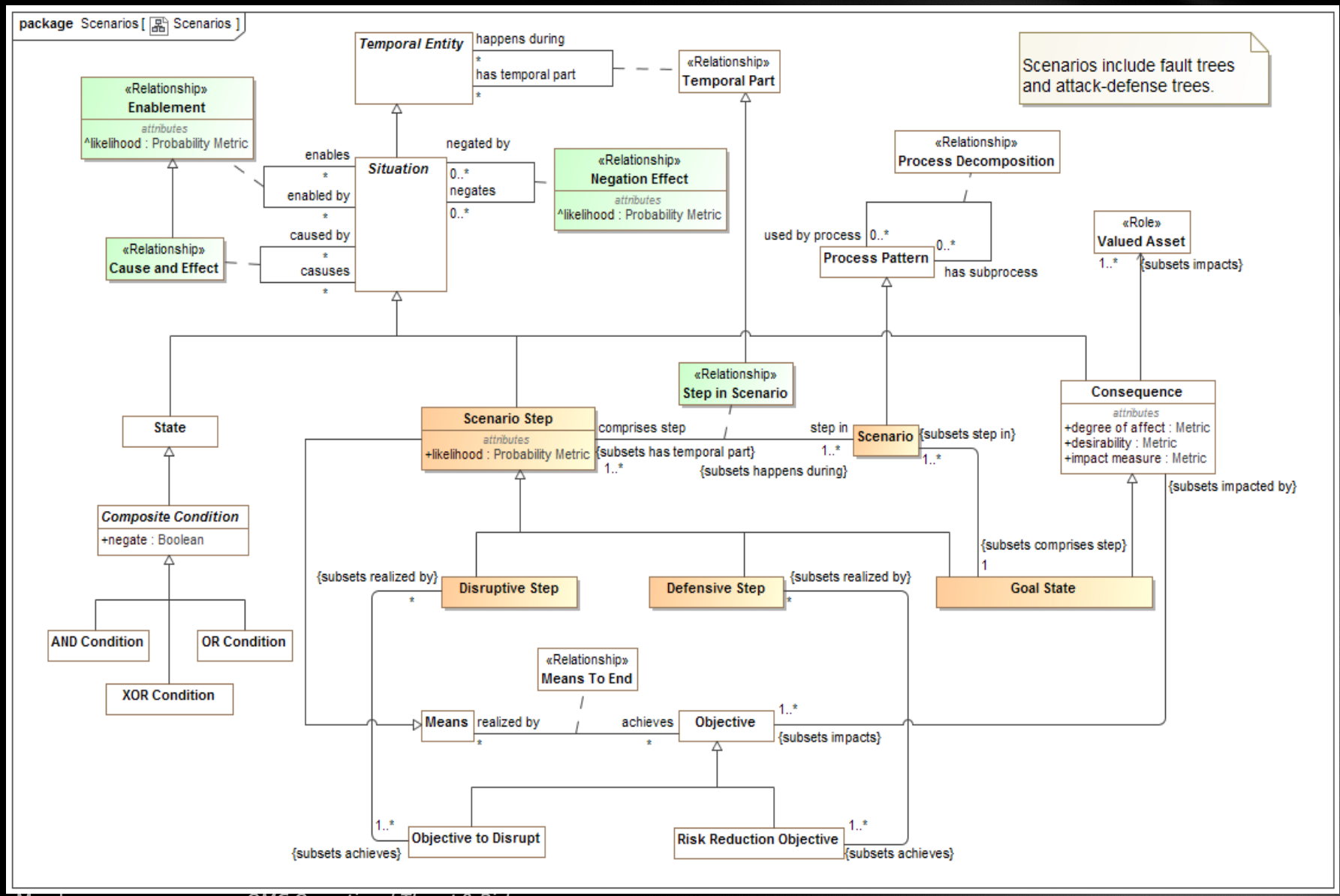
Attack Defense Tree Example

Example: attacking and defending a bank account

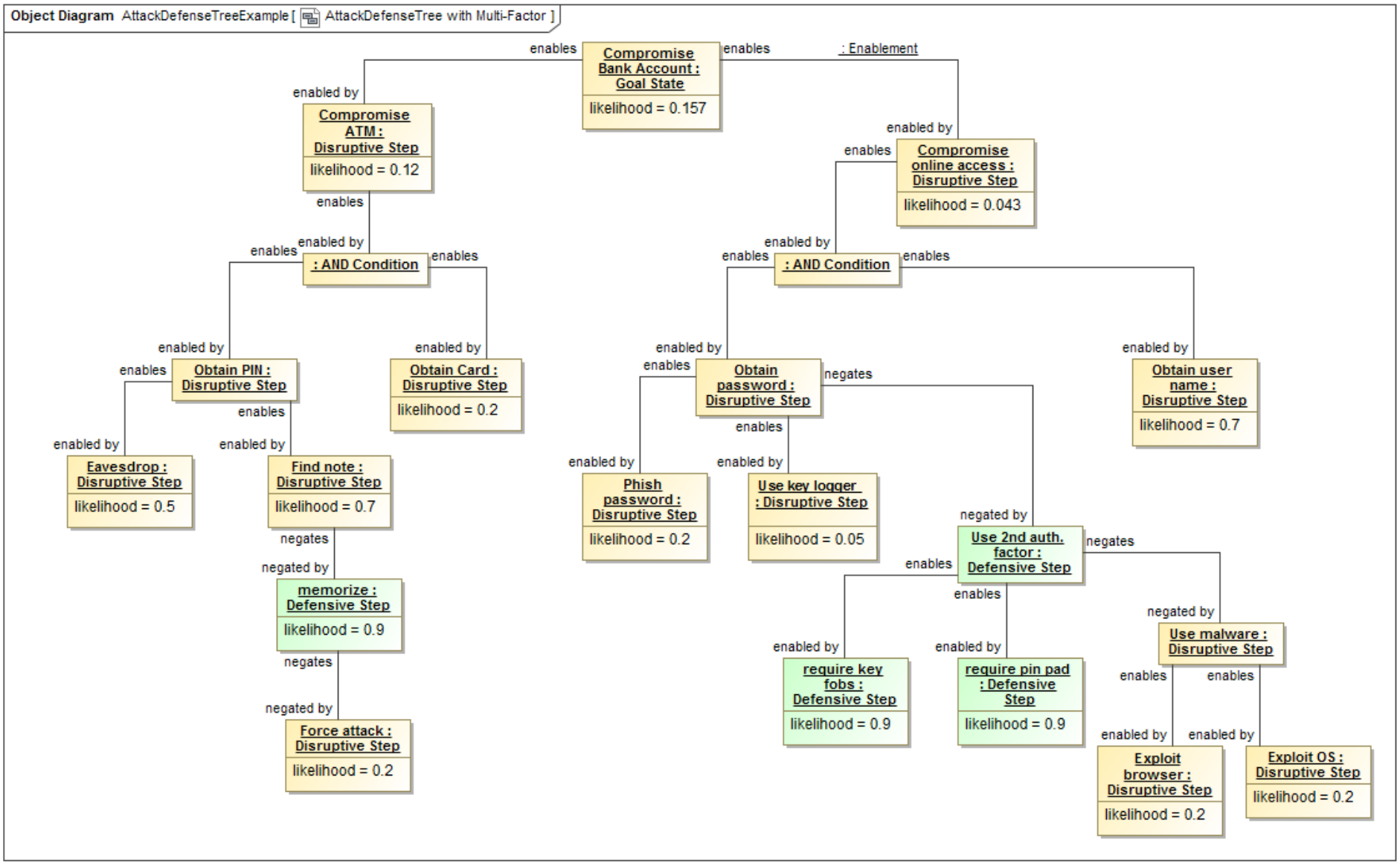


Barbara Kordy, UL ATREES project funded by National Research Fund CORE grant No. C08/IS/26 8

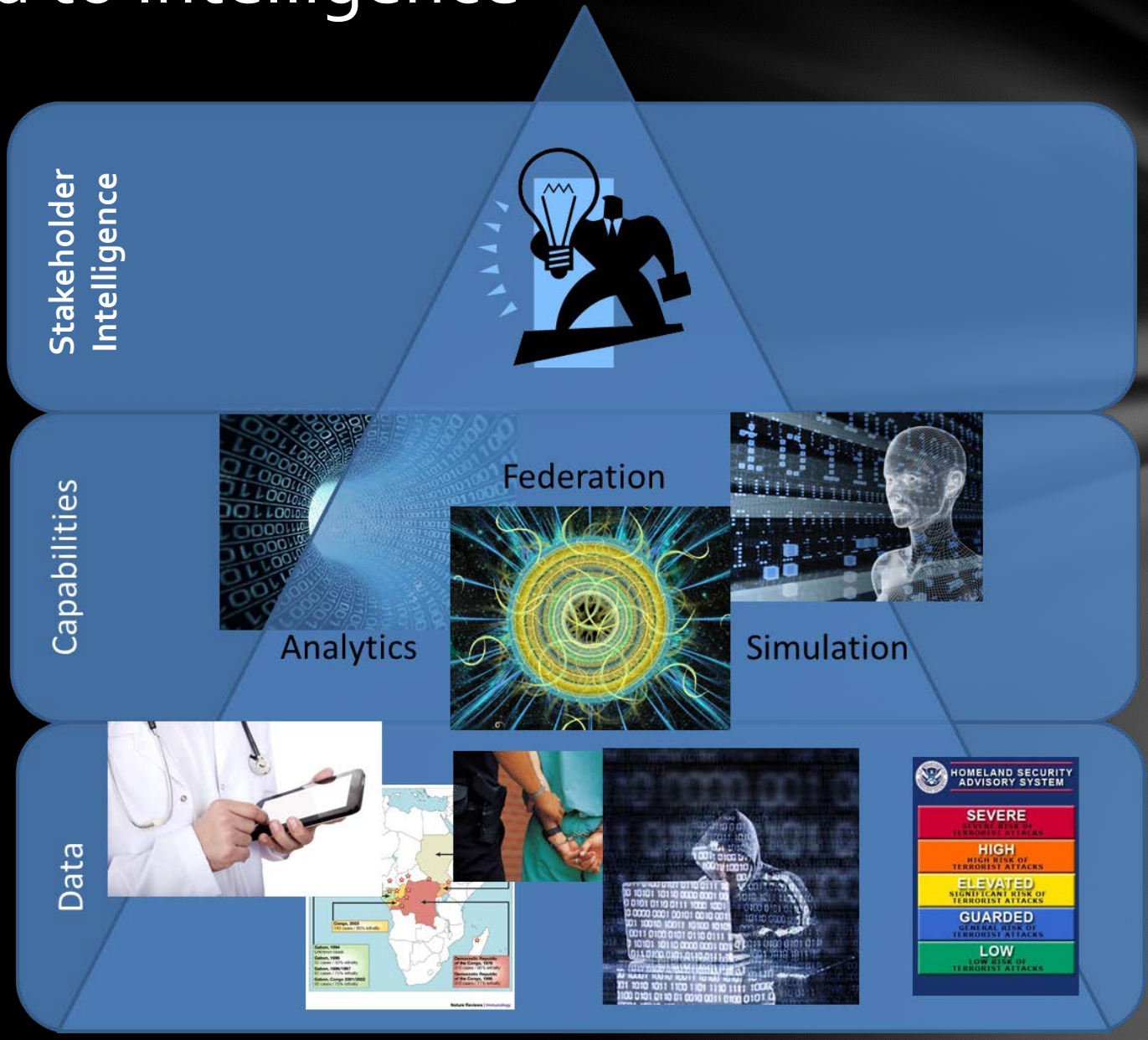
Model Supporting Attack/Defense Scenarios



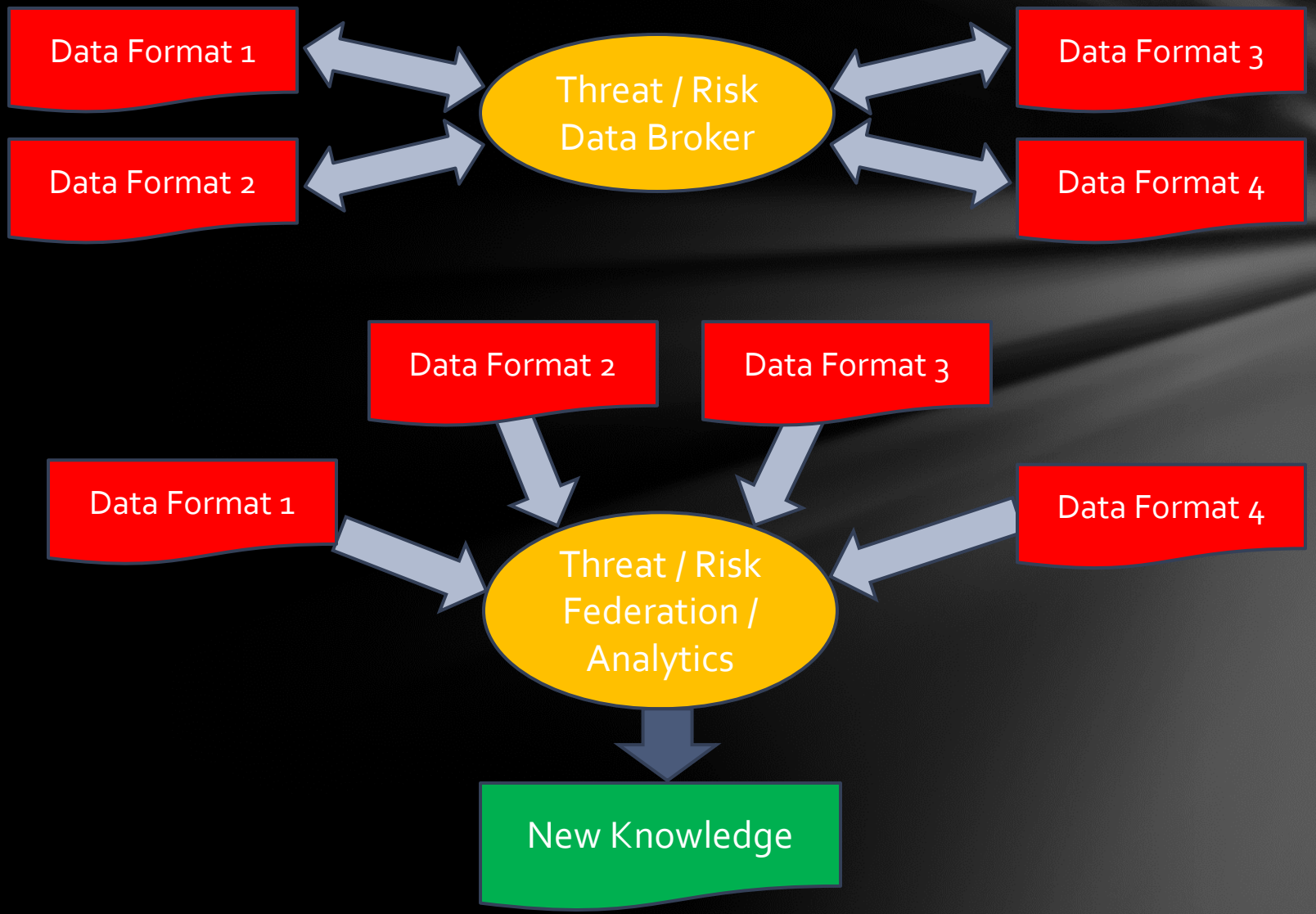
How example is mapped to concepts



Data to Intelligence



Primary Use Cases



It takes a community!

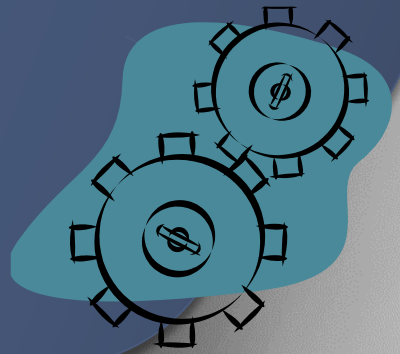
Leadership

Information Sources

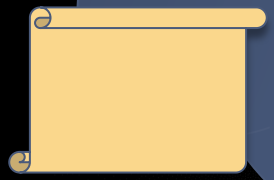
Policy

http://www.ThreatRisk.org

Threat & Risk Information Sharing Community



Tools & Services



Standards

Information Analysts & Consumers