

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



A Common Cyber Threat Framework: A Foundation for Communication

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N



Goals of a Common Approach

- Key Attributes: a model that is ***hierarchical, structured, transparent and repeatable***, tied to ***explicit definitions***
- An optimized cyber threat framework
 - Is focused on empirical and often sensor-derived data; serves as the foundation for subsequent analysis and decision-making
 - Supports analysis and the characterization and categorization of cyber threat information through the use of standardized language
 - Accommodates a wide variety of data sources, threat actors and threat activity
 - Information arranged hierarchically and organized in increasing “layers” of detail
 - Can be tailored or customized to meet individual needs



Common Cyber Threat Framework

Threat Actor Objectives within the “Threat Lifecycle”

Layer 1

Layer 2

Layer 3

Layer 4

The progression of cyber threat actions over time to achieve objectives

Stages

Preparation

Engagement

Presence

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Plan activity

Conduct research & analysis

Develop resources & capabilities

Acquire victim specific knowledge

Complete preparations

Deploy capability

Interact with intended victim

Exploit vulnerabilities

Deliver malicious capability

Establish controlled access

Hide

Expand presence

Refine focus of activity

Establish persistence

Enable other operations

Deny access

Extract data

Alter data and/or computer, network or system behavior

Destroy HW/SW/data

Actions and associated resources used by an threat actor to satisfy an objective

Actions

Discrete cyber threat intelligence data

Indicators



Common Cyber Threat Framework

Current Status

- Used in threat products by multiple US Government agencies and some Allies
- Adoption across the Executive Branch high priority for 2018
- Under consideration by NATO and Asian allies to facilitate a common operating picture and enhance information sharing
- Being taught to new US Government cyber analysts
- Included in curricula and research at multiple universities
- Evolution continues based on use and ongoing outreach to industry, academia, government, and international partners

Framework materials available at DNI.GOV