OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Cyber Threat Framework (version 4)

How to Use

LEADING INTELLIGENCE INTEGRATION

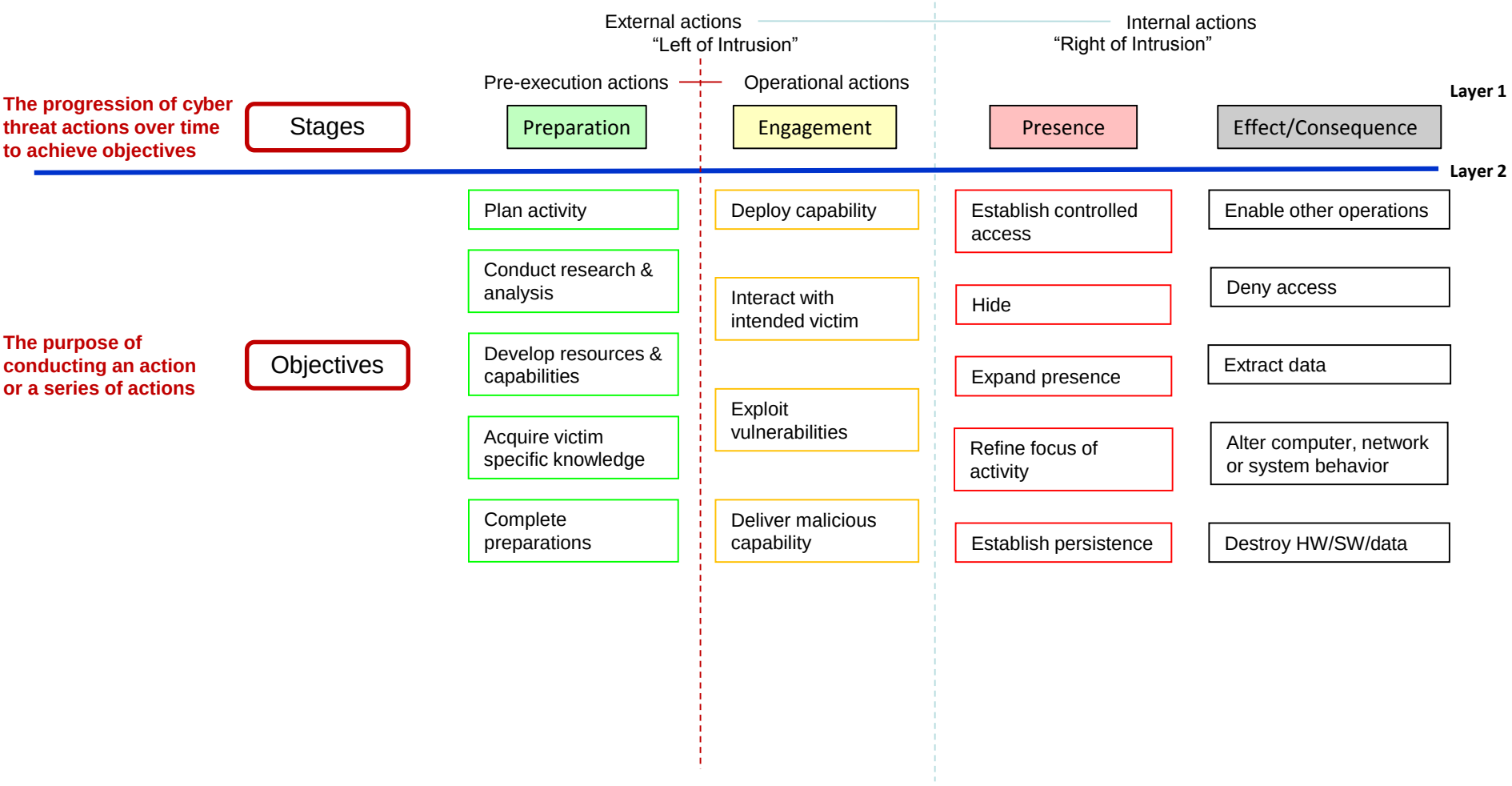
What You Need to Know

- Recognize and understand how to interpret data tagged to the Cyber Threat Framework (CTF)
- Understand how to tag reporting to the Cyber Threat Framework
- Understand how CTF-tagged reporting can be used in analysis

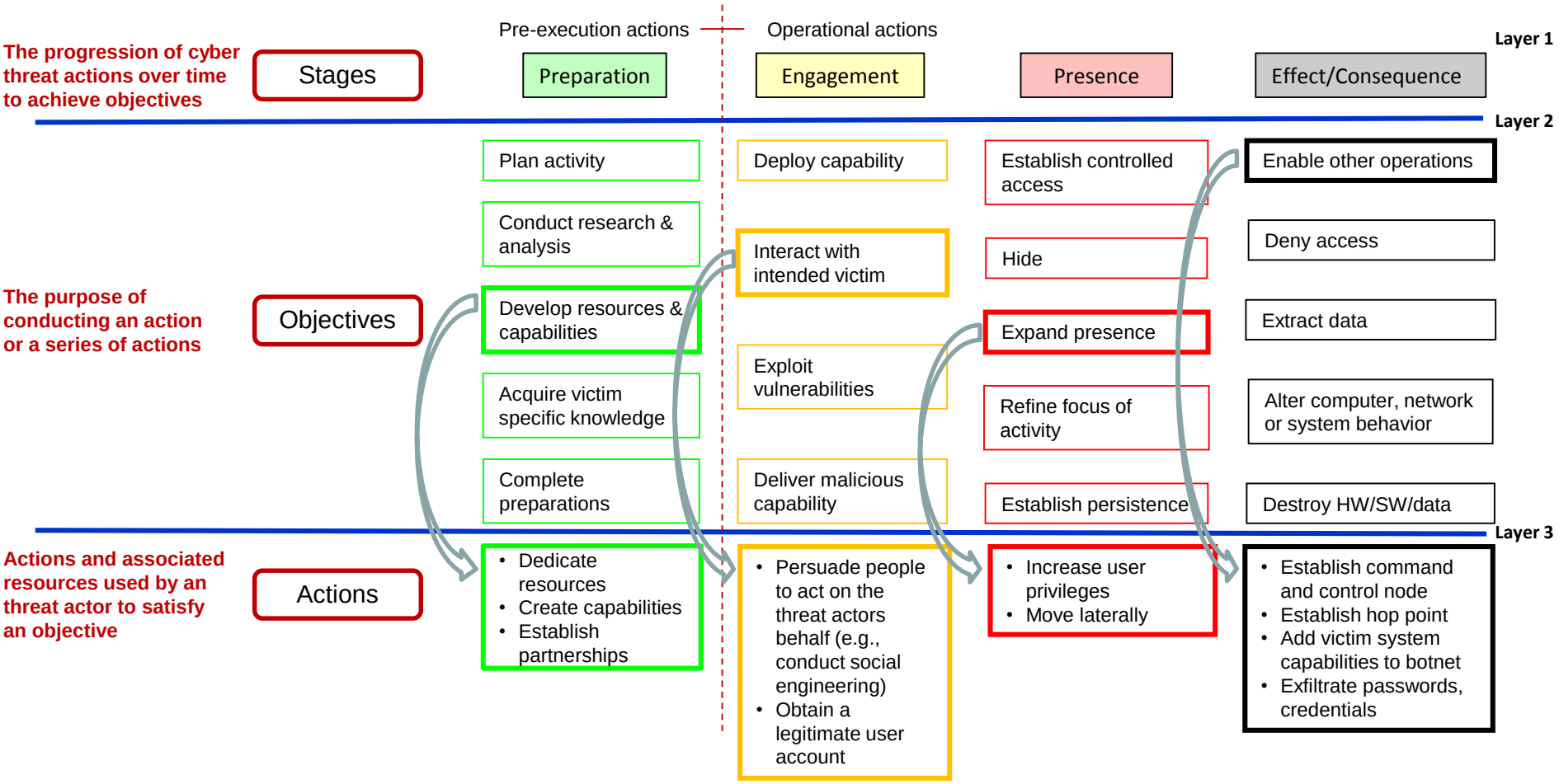
Cyber Threat Framework (CTF) Overview

The Cyber Threat Framework was developed by the US Government to enable consistent categorization and characterization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The framework captures the adversary life cycle from (a) “PREPARATION” of capabilities and targeting, to (b) initial “ENGAGEMENT” with the targets or temporary nonintrusive disruptions by the adversary, to (c) establishing and expanding the “PRESENCE” on target networks, to (d) the creation of “EFFECTS and CONSEQUENCES” from theft, manipulation, or disruption. The framework categorizes the activity in increasing “layers” of detail (1- 4) as available in the intelligence reporting.

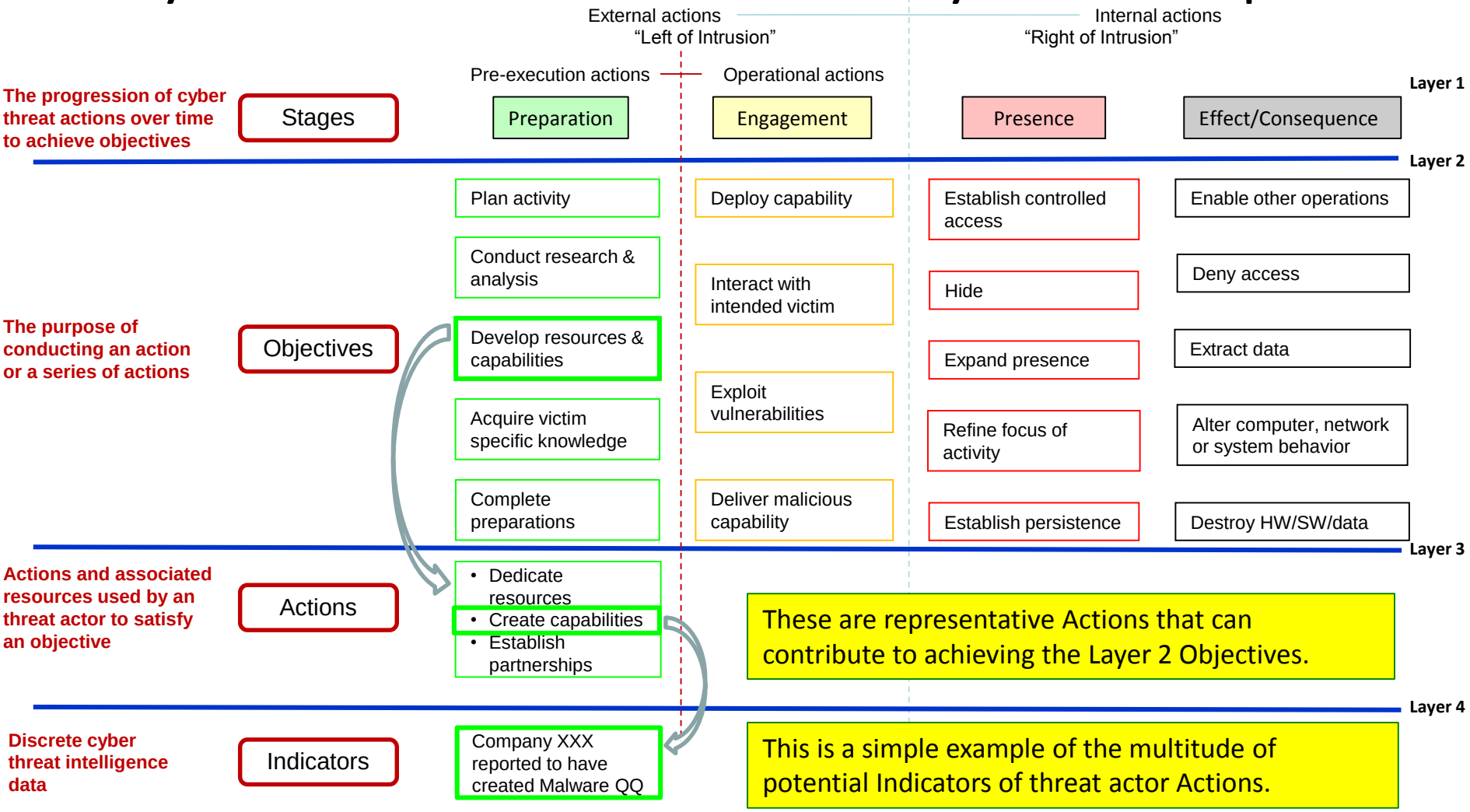
Cyber Threat Framework (v4) Layers 1 and 2



Cyber Threat Framework (v4) Layer 3 Exemplars



Cyber Threat Framework (v4) Layer 4 Exemplar



Cyber Threat Framework Representations

- The Cyber Threat Framework's presentation can be adjusted to include only the information of most interest to an intended audience.

(U) Cyber Threat Framework		
Executive	Layer 1	Stages
Executive	Layer 2	Objectives
Tactical	Layer 3	Actions
Tactical	Layer 4	Indicators

Reading the Framework

- Products tagged to the Cyber Threat Framework may represented in a variety of ways on products. Presented layers can be adjusted to fit the intended audience.

Example 1

(U) Cyber Threat Framework	
Layer 1	**Layer 2**
Preparation	N/A
Engagement	**Deliver Payload**
Presence	N/A
Effect/ Consequence	N/A

Example 2

(U) Cyber Threat Framework	Layer 1	Layer 2
	Engagement	Deliver Payload

Example 3

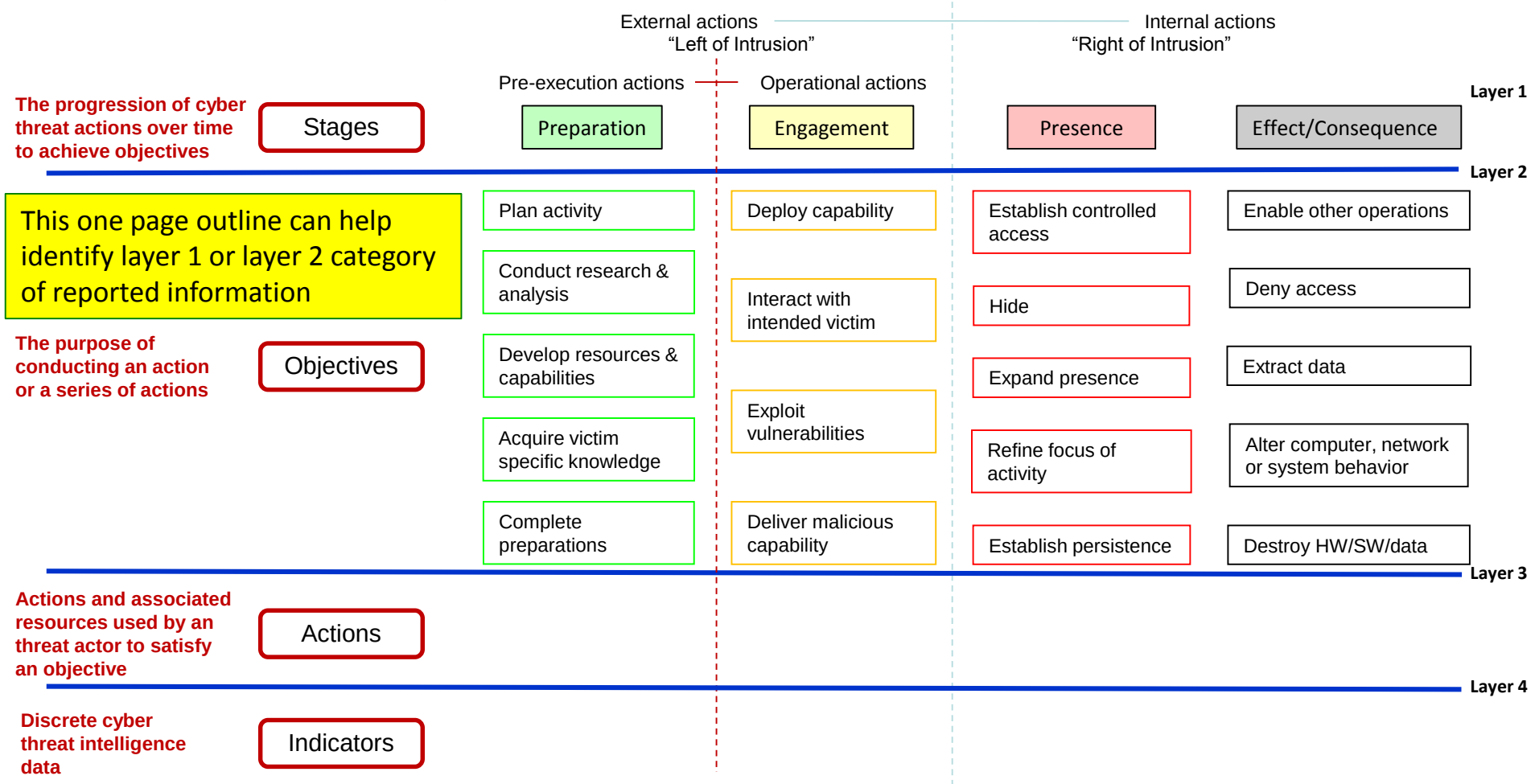
(U) Cyber Threat Framework	
Layer 1	**Stages**
Layer 2	**Objectives**
Layer 3	**Actions**
Layer 4	**Indicators**

Tagging Information to the Cyber Threat Framework

Tools to help you

- Cyber Threat Framework one page overview
- Cyber Threat Framework Lexicon outline
- Cyber Threat Framework Lexicon

Cyber Threat Framework (v4)



Cyber Threat Framework (v4) Lexicon Outline

- The outline provides a multilayer view of a segment of the entire framework.

Enable other activities	
Deny access	
	Disrupt/degrade communication links
	Conduct Denial of Service (DoS) and/or Distributed Denial of Service (DDoS) attack
	Disrupt/degrade the network
	Execute ransomware
Extract data	
	Relocate and store data on victim's computer, information system(s), network(s), and/or data stores.
	Exfiltrate data/information
Alter computer, network, and/or system behavior	
	Change process run-state on victim system(s)
	Change decisions
	Change machine-to-machine (MtM) communications
Destroy hardware/software/data	

Cyber Threat Framework (v4) Lexicon

Terms				Definitions
Layer 1 Stages	**layer 2 Objectives**	**Layer 3 Actions**	**Layer 4 Indicators**	
stages				The progression of cyber threat actions over time to achieve objectives.
	objectives			The purpose of conducting an action or a series of actions.
		actions		Activity and associated resources used by a threat actor to satisfy an objective.
			indicators	Exemplars of discrete, measurable, cyber threat data, i.e., presence of malicious software, named Malware, and/or reported instances of malicious actions or activities, that connotes a threat actor's attempt to take or having taken an action, or to achieve an objective.
Preparation	Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities.			
	Plan activity			Steps taken by a threat actor before conducting malicious cyber activity to: define intent; establish policy limitations; identify funding; coordinate intended activities; establish initial objectives and parameters for measuring progress/success towards meeting them; and the steps taken to update plans, activities, and requirements based upon insights gained during the eventual victim engagement.
		Identify intended target(s) and the purpose for the malicious cyber activity		The initial step in the planning process that produces a list of intended victim(s), and defines the intent for and desired outcome of the malicious cyber activity.
		Outline where and how the malicious activity is to be conducted		Actions taken by a threat actor (individual, team or government-sponsored agency), their sponsor and/or leadership to establish the overall strategy for, policy limitations of, and the requisite resources and capabilities needed to conduct the intended malicious cyber activity, (e.g., information needs, resources and capabilities, and partnerships), along with the criteria for evaluating the eventual success/failure (measures of performance, merit, and effectiveness [MoP/MoM/MoE]) of the activity.
		Establish a projected timeline for the malicious activity		The last step in the initial planning process in which the threat actor establishes a projected time for executing the planned malicious activity.

Includes definitions of exemplar terms to aid in accurate data classification; as a living document, the number of terms will increase based on user input.

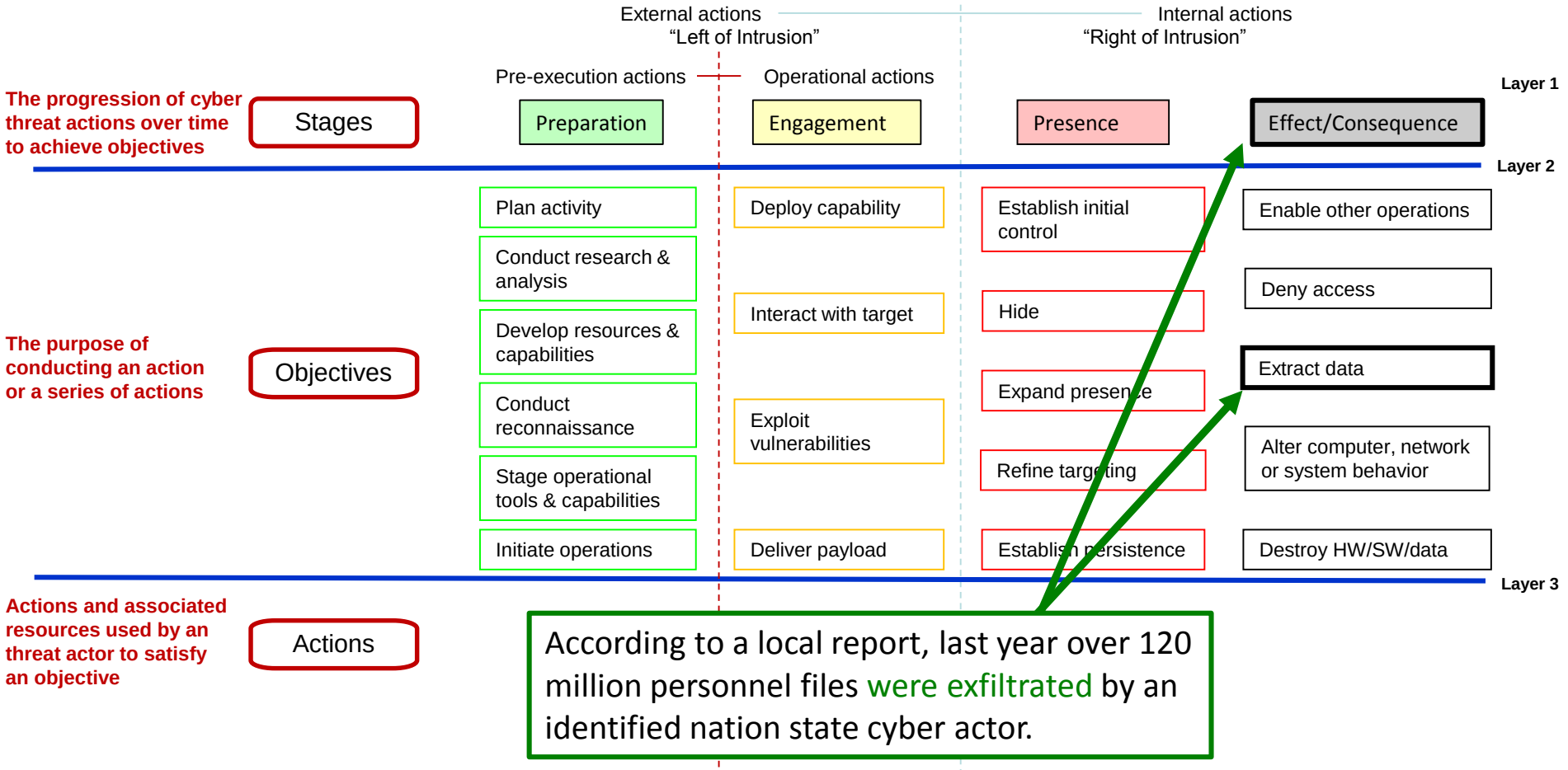
Sample Report #1

- According to a local report, last year over 120 million personnel files were electronically exfiltrated by an identified nation state cyber actor.

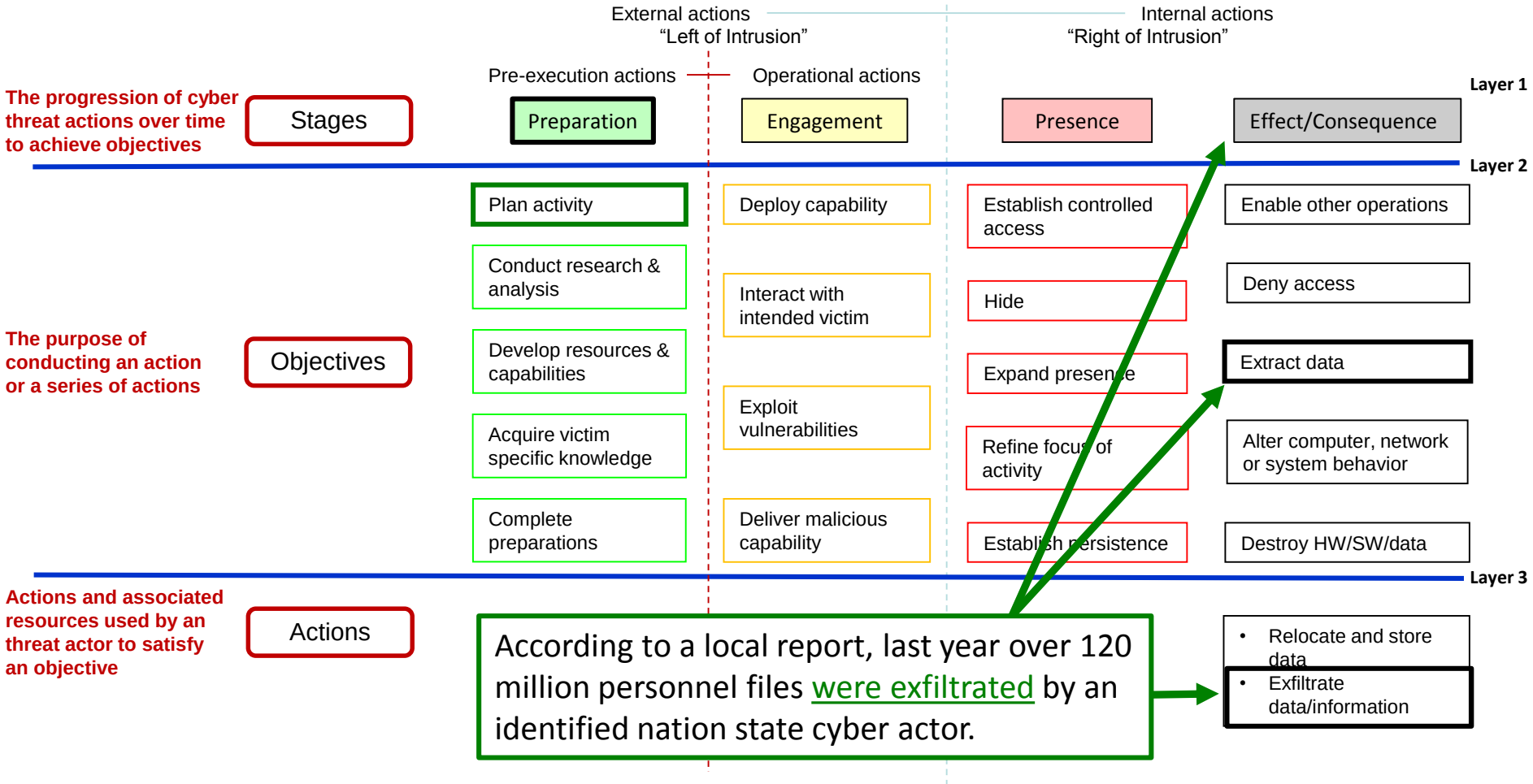
Sample Report #1 Highlighted

- According to a local report, last year over 120 million personnel files were electronically exfiltrated by an identified nation state cyber actor.

Sample Report #1 Tagged to Layer 1 and 2



Sample Report #1 Tagged to Layers 1, 2, and 3



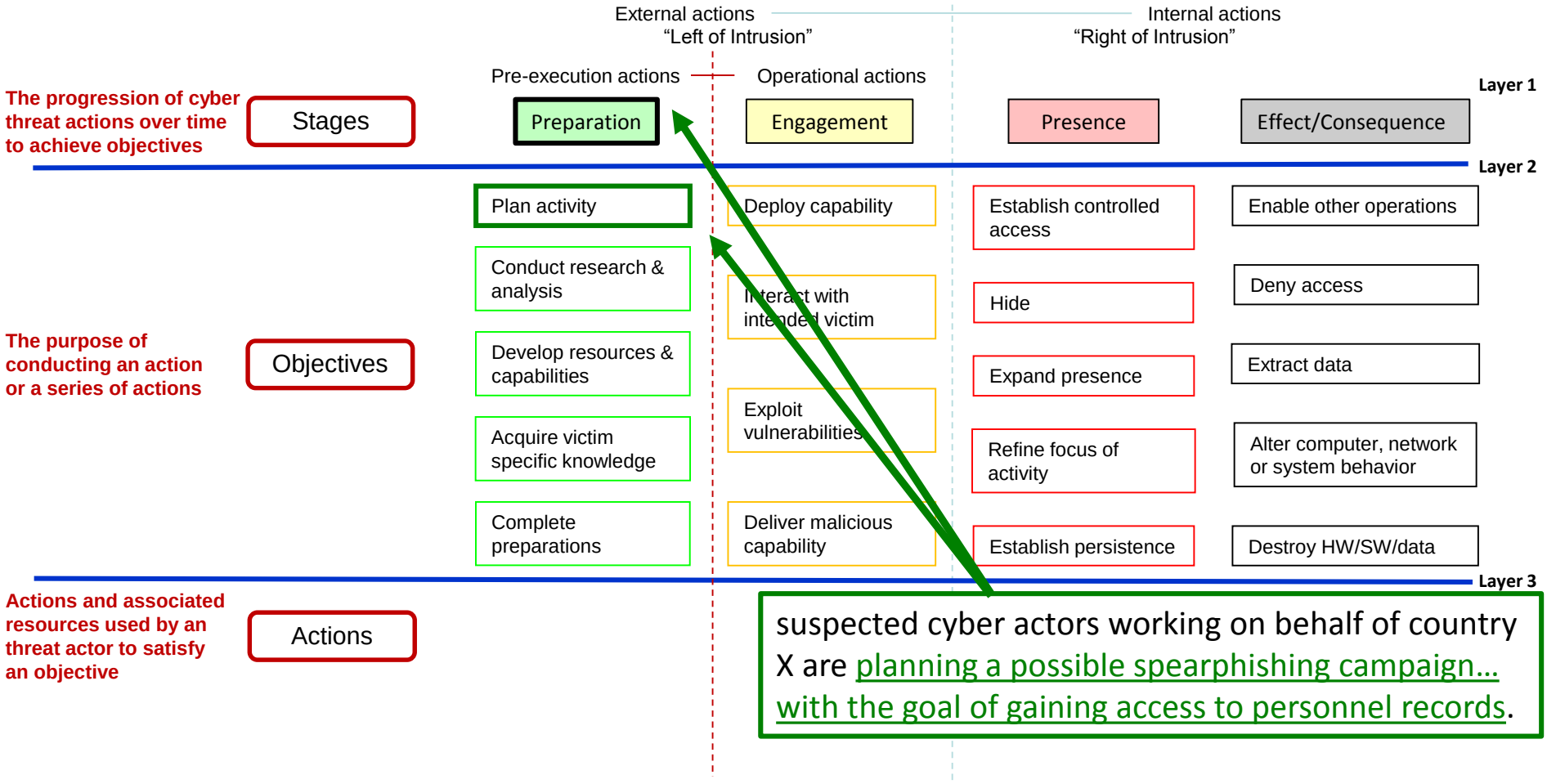
Sample Report #2

- Recent reporting indicates suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign against the US Government, with the goal of gaining access to personnel records.

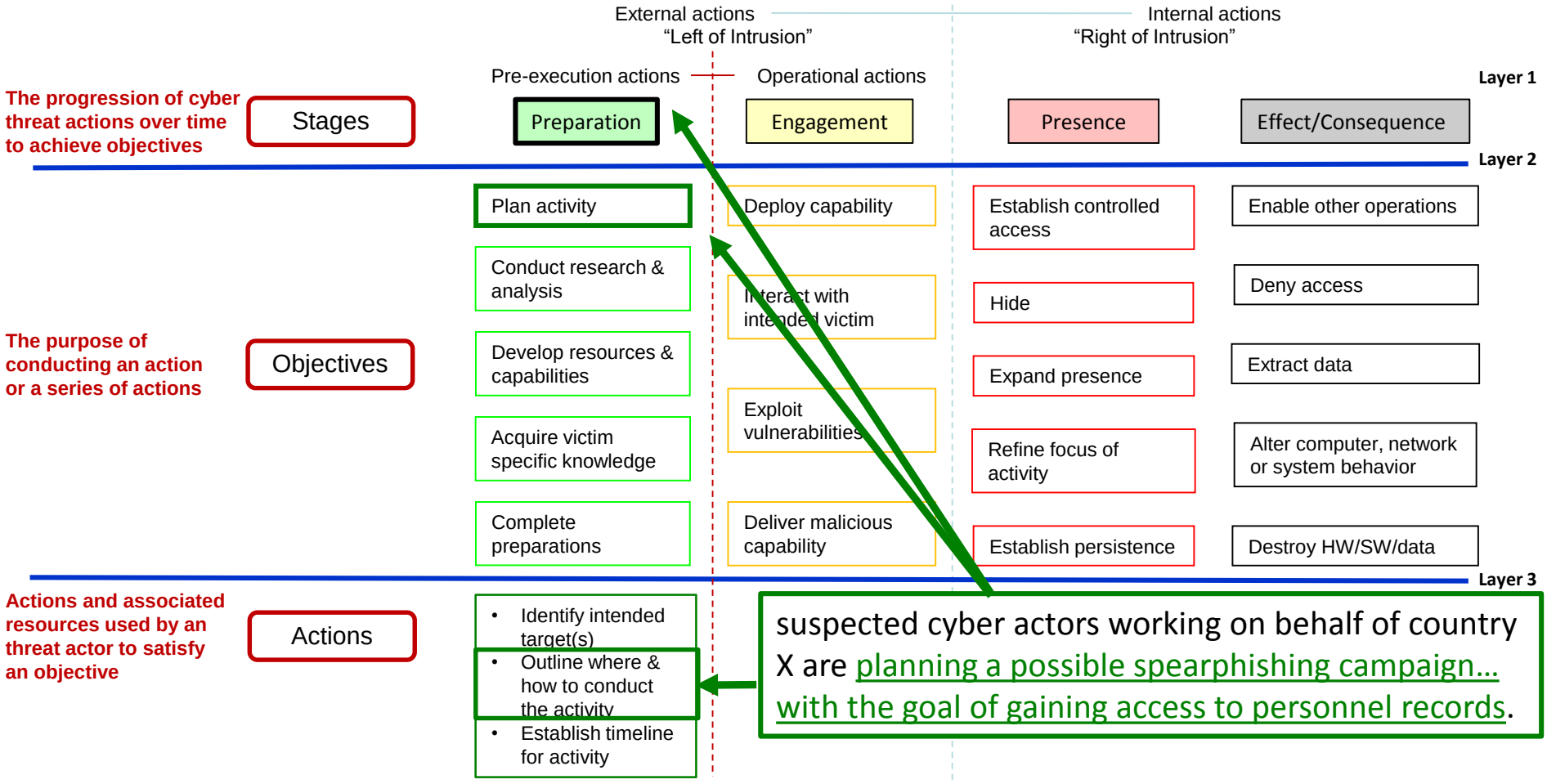
Sample Report #2 Highlighted

- Recent reporting indicates suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign against the US Government, with the goal of gaining access to personnel records.

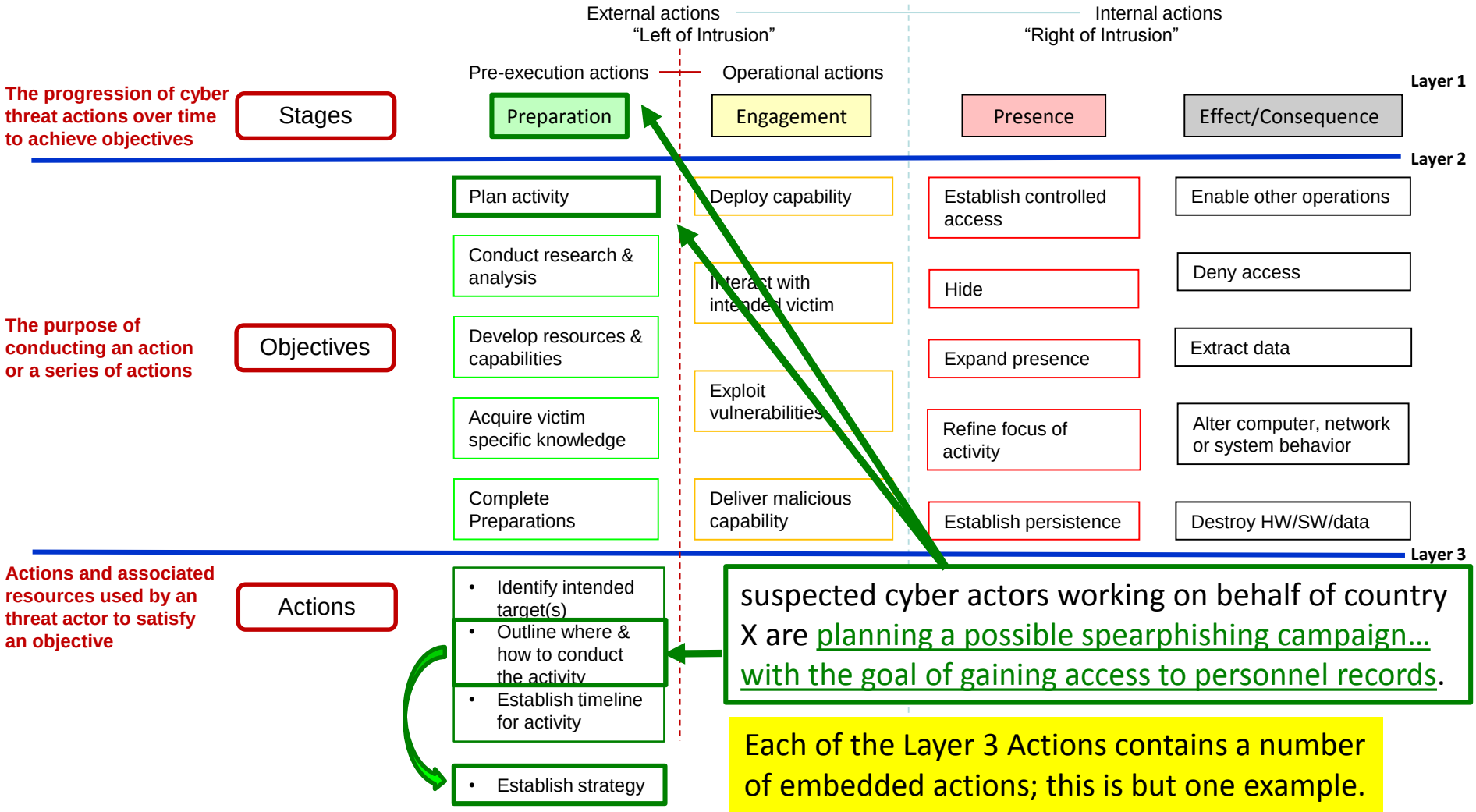
Sample Report #2 Tagged to Layers 1 and 2



Sample Report #2 Tagged to Layers 1, 2, and 3



Sample Report #2 Tagged to Layers 1, 2, and 3



Sample Report #3

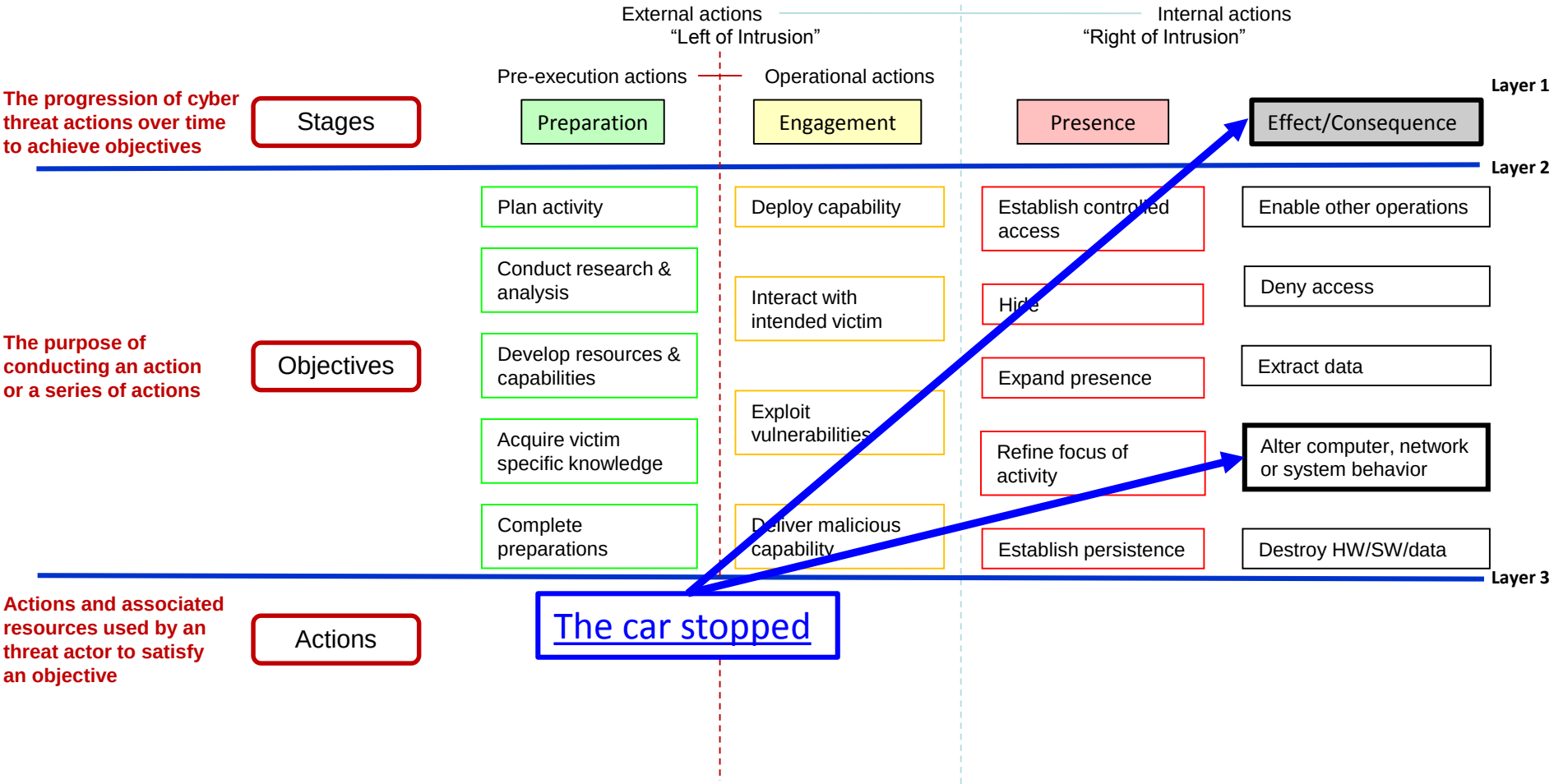
- Hackers attacked a self-driving car, bringing the car to a complete stop. Investigation showed that the hackers targeted the laser ranging system, spoofed thousands of objects, and overwhelmed the system's ability to process information.

Sample Report #3 Highlighted

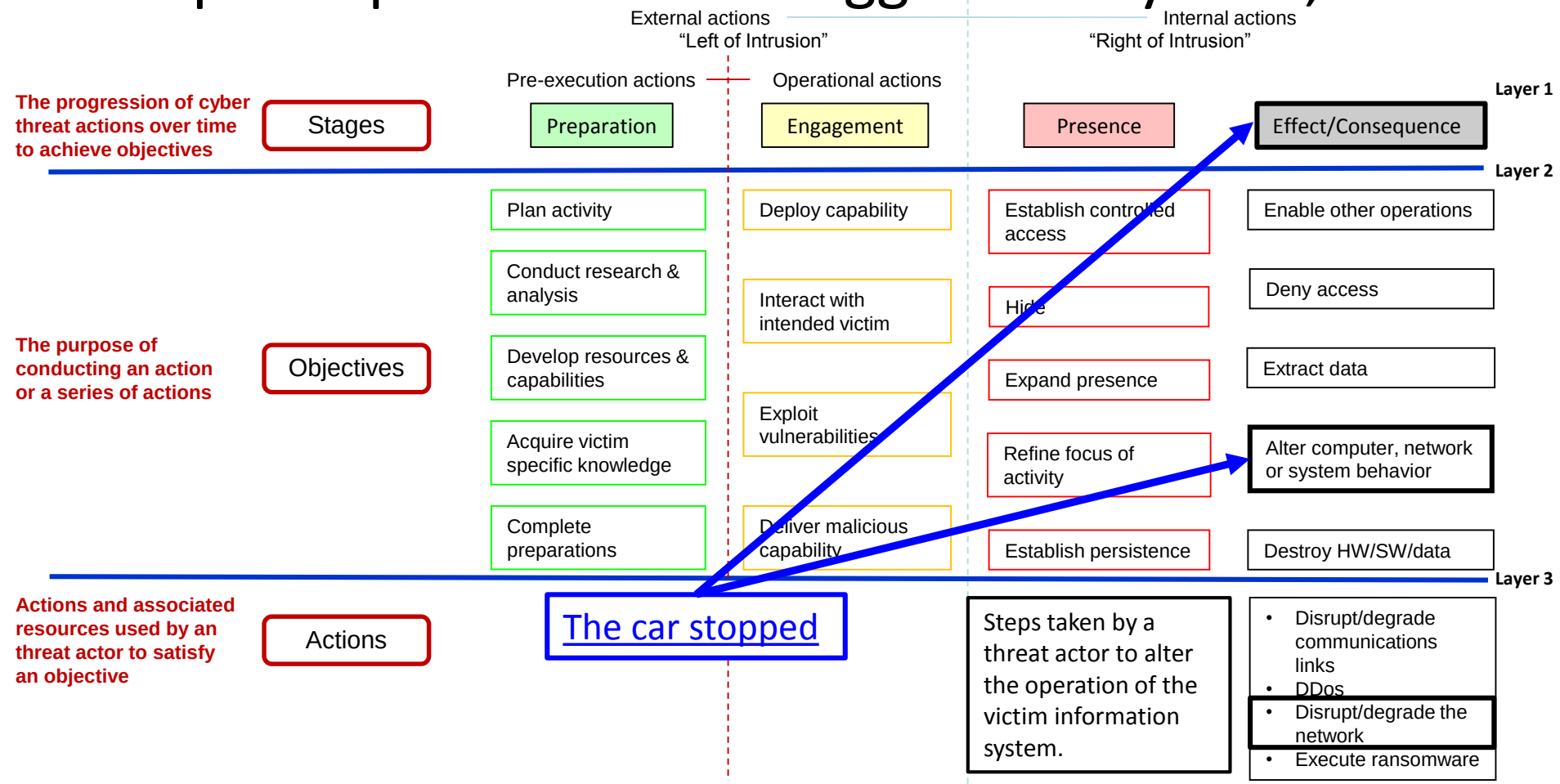
- Hackers attacked a self-driving car, bringing the car to a complete stop. Investigation showed that the hackers targeted the laser ranging system, spoofed thousands of objects, and overwhelmed the system's ability to process information.

The framework allows the user to capture all activity surrounding an event. Assuming this was a cyber event, there are two activities: the first was when the car stopped; the second, determined through subsequent forensic analysis, was the specific targeting of the laser ranging system. Both actions should be recorded. The user must determine how to link the two activities to the single event.

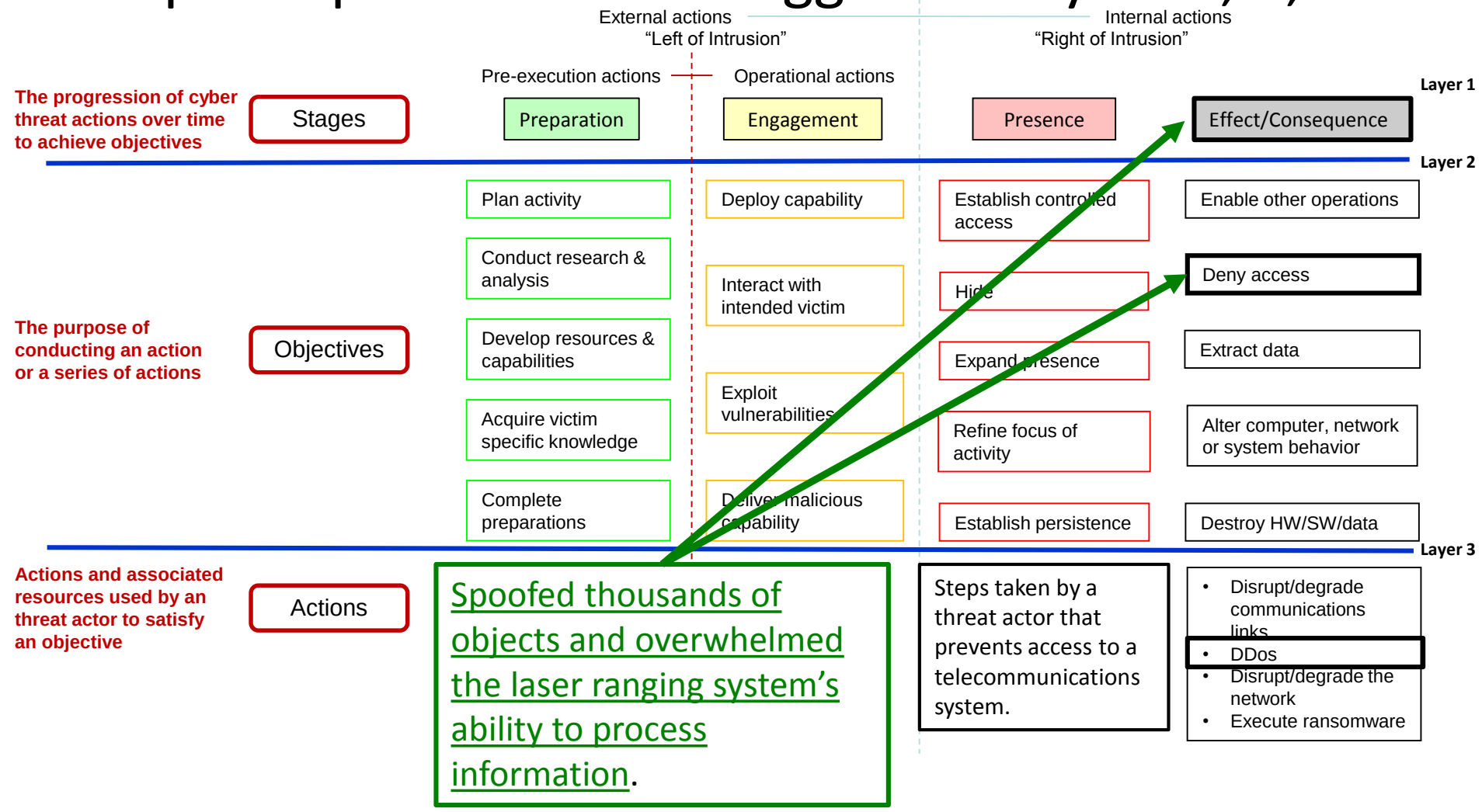
Sample Report #3 Fact 1 Tagged to Layers 1 and 2



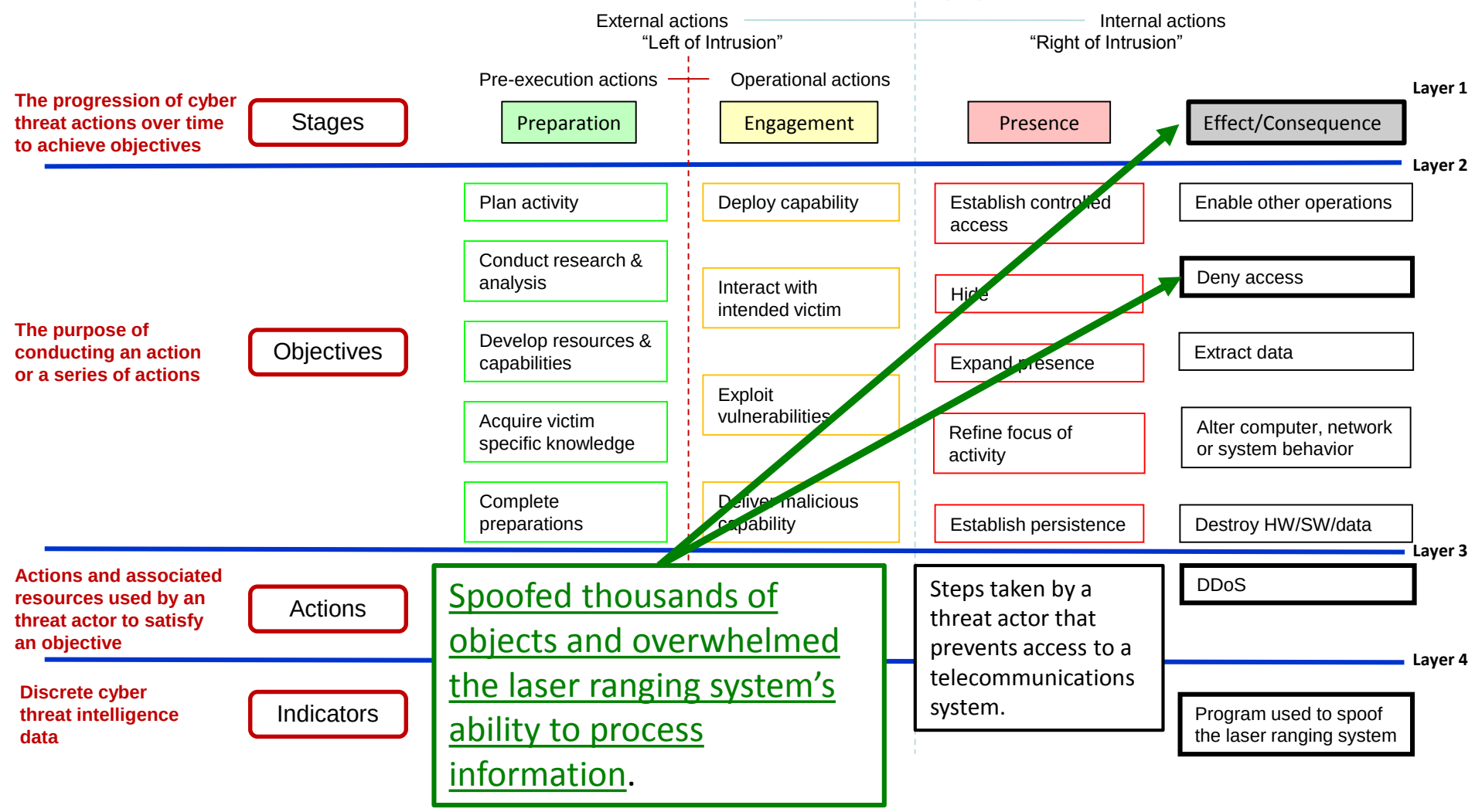
Sample Report #3 Fact 1 Tagged to Layers 1, 2 and 3



Sample Report #3 Fact 2 Tagged to Layers 1, 2, and 3



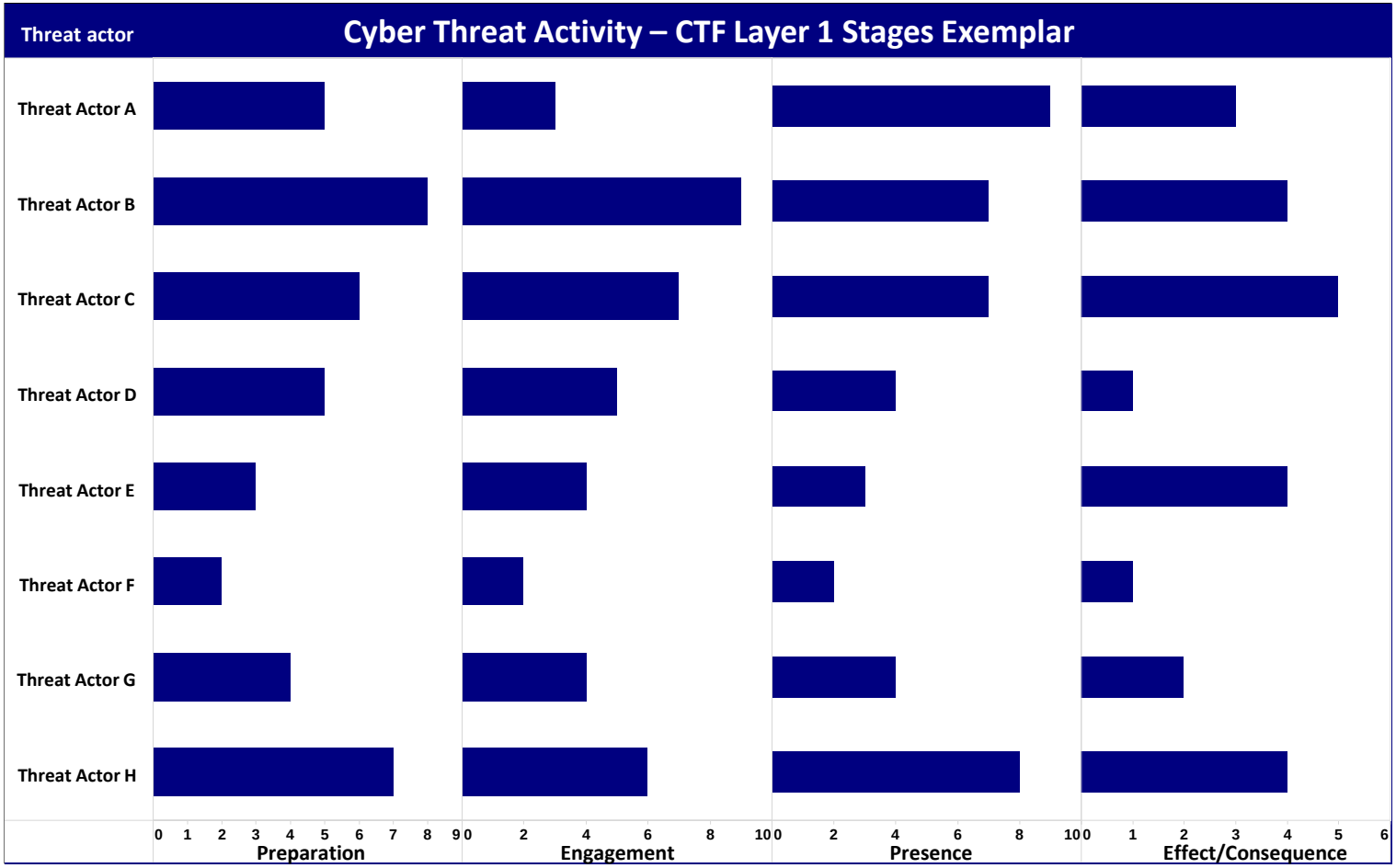
Sample Report #3 Fact 2 Tagged to Layer 4



Analysis

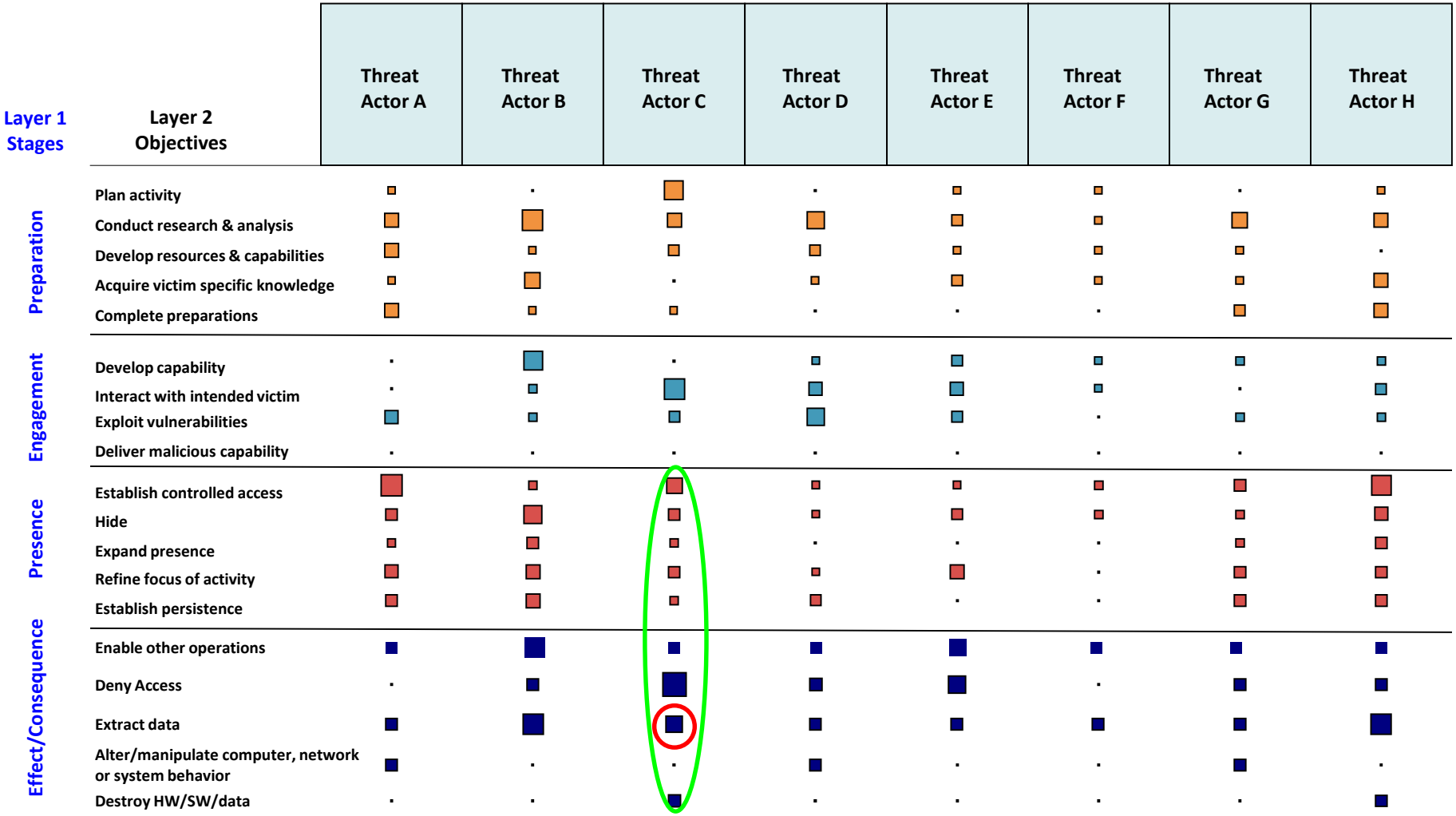
- Depending on the information selected and its presentation, one can begin to conduct a variety of analysis:
  - Trends – change over time
    - What caused the change
  - Predictive – what's next
  - Environmental
    - Was the threat different than expected
    - What vulnerabilities were missed
    - How to optimize remedial action
  - Vulnerability – risk analysis
  - Defensive posture

Threat Actor | Preparation | Engagement | Presence | Effect/Consequence



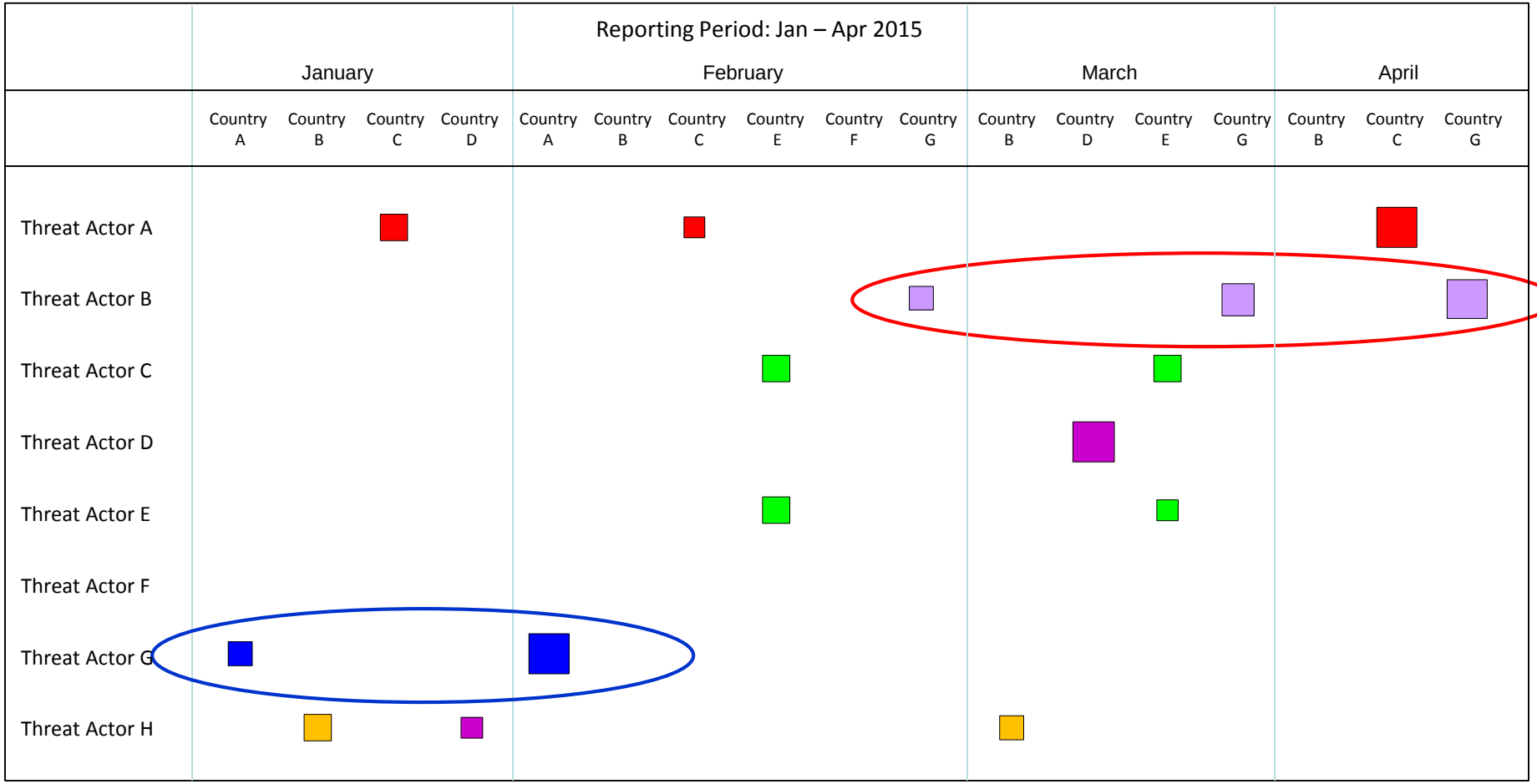
Reporting Period: January – March 2016

CTF (v4) Layer 2 Objectives Exemplar



Trend Analysis - Threat Activity Over Time

Level 2 Cyber Threat Activity by Threat Actor, Report Date, and Country of Threat Origin



Summary

- The Cyber Threat Framework can be represented in a variety of products tailored to a specific audience
- Important to understand how tagging cyber threat information to the Cyber Threat Framework works
- Cyber Threat Framework-tagged reporting can be used to produce insightful, consistent analysis from a variety of information sources

Questions?

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu