OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Application of the Common Cyber Threat Framework

Use Cases

James Richberg
National Intelligence Manager for Cyber
National Security Partnerships
July 18, 2018

Goals for a Common Approach to Threat Frameworks

Following a common approach helps to:

- *Establish a shared ontology* and *enhance information-sharing* since it is easier to maintain mapping of multiple models to a common reference than directly to each other
- *Characterize and categorize threat activity* in a straightforward way that can support missions ranging from strategic decision-making to analysis and cybersecurity measures and users from generalists to technical experts
- *Support common situational awareness* across organizations

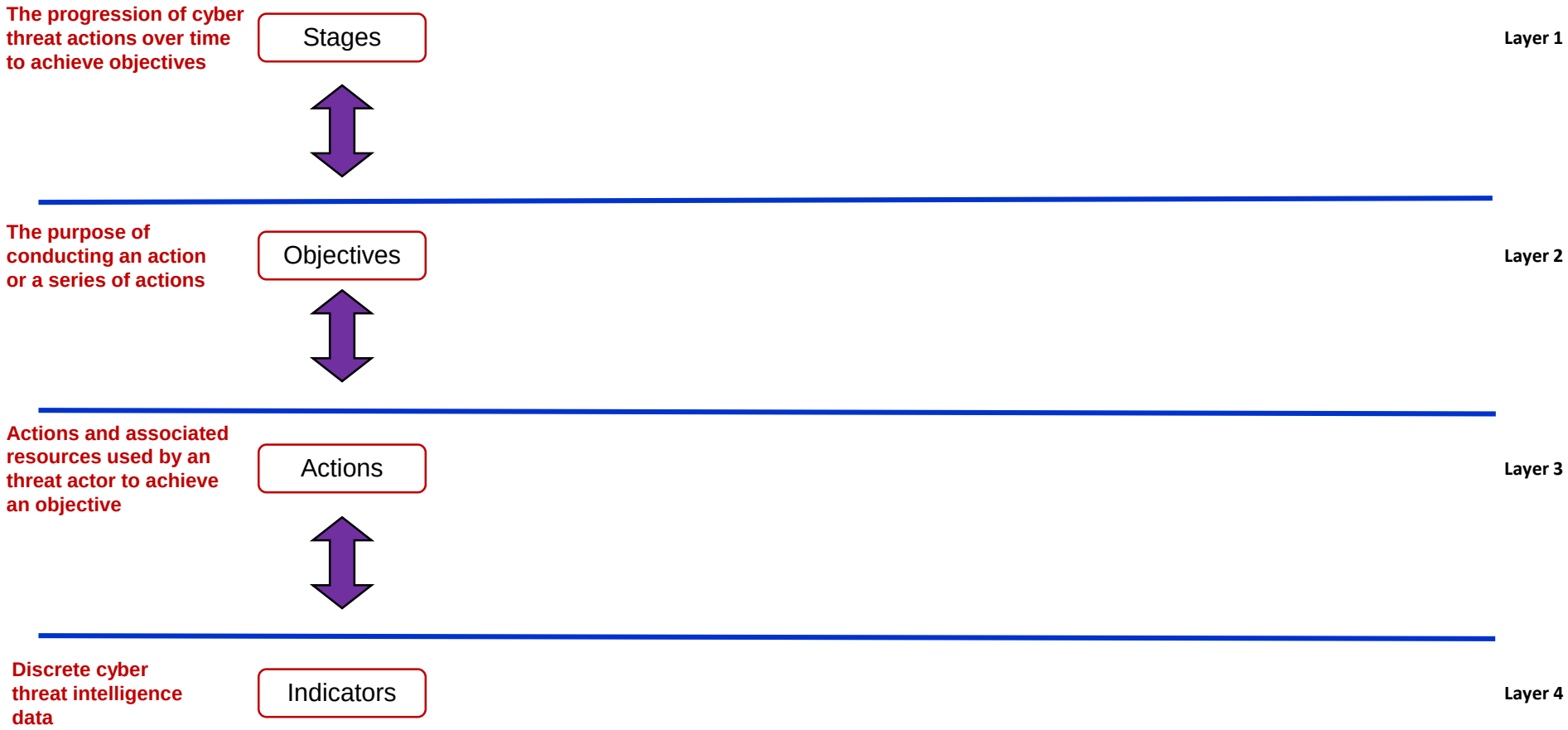
Key Attributes and Goals in Building a Cyber Threat Framework

- Incorporate a *hierarchical/layered perspective* that allows a focus on a level detail appropriate to the audience while maintaining linkage and traceability of data
- Employ *Structured and documented categories* with explicitly *defined terms* and labels (lexicon)
- Focus on *empirical/sensor-derived 'objective' data*
- Accommodate a wide variety of data sources, threat actors and activity
- Provide as a foundation for analysis and decision-making

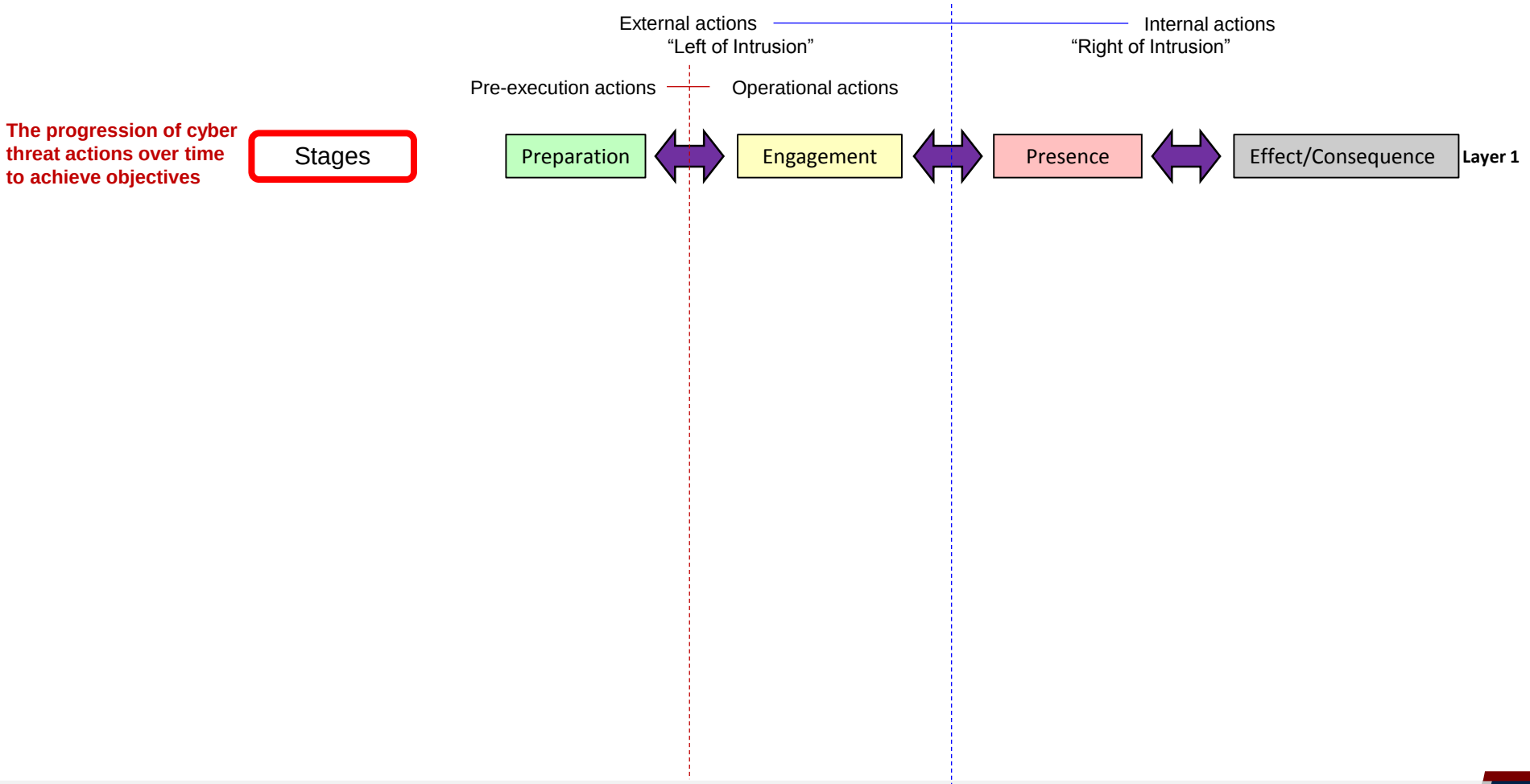
The Common Cyber Threat Framework

- Since 2012, the Office of the DNI has worked with interagency partners to build and refine The Common Cyber Threat Framework reflecting these key attributes and goals
- The Common Cyber Threat Framework is not intended to displace or replace an organization's existing model which is tailored to its specific mission and requirements; rather, it is intended to:
  - *Serve as a viable Universal Translator* (a cyber Esperanto or Rosetta Stone) facilitating efficient and possibly automated exchange of data and insight across models once each has been mapped to it and the mappings shared
  - *Provide a Starting Point* featuring a simple threat model and value-neutral concepts. It can be customized for any organization as needed—and any deviations from the common approach are readily apparent, facilitating mapping and data exchange.

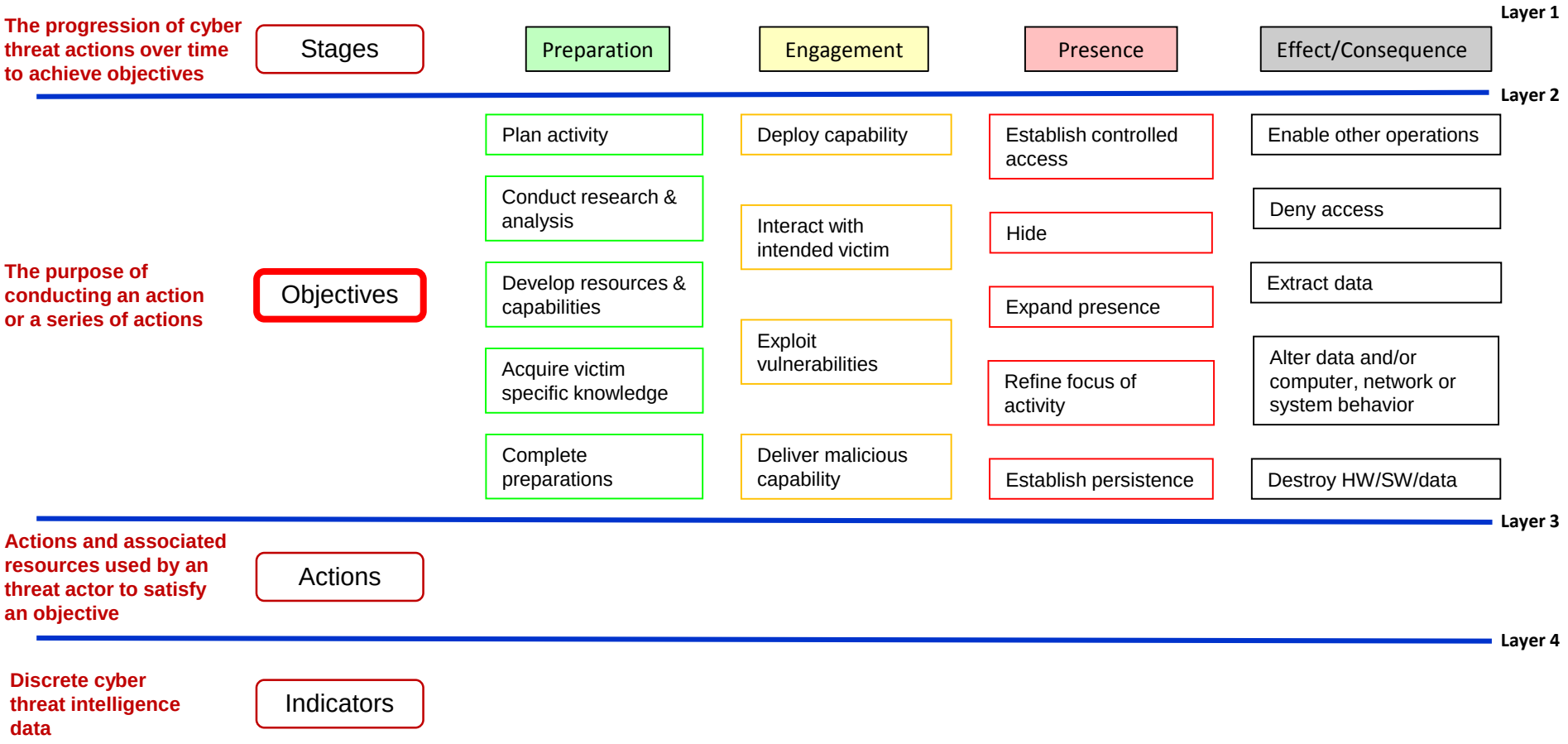
The Common Cyber Threat Framework
A Hierarchical, Layered Approach



The Common Cyber Threat Framework
Structured around a Simplified "Threat Lifecycle"

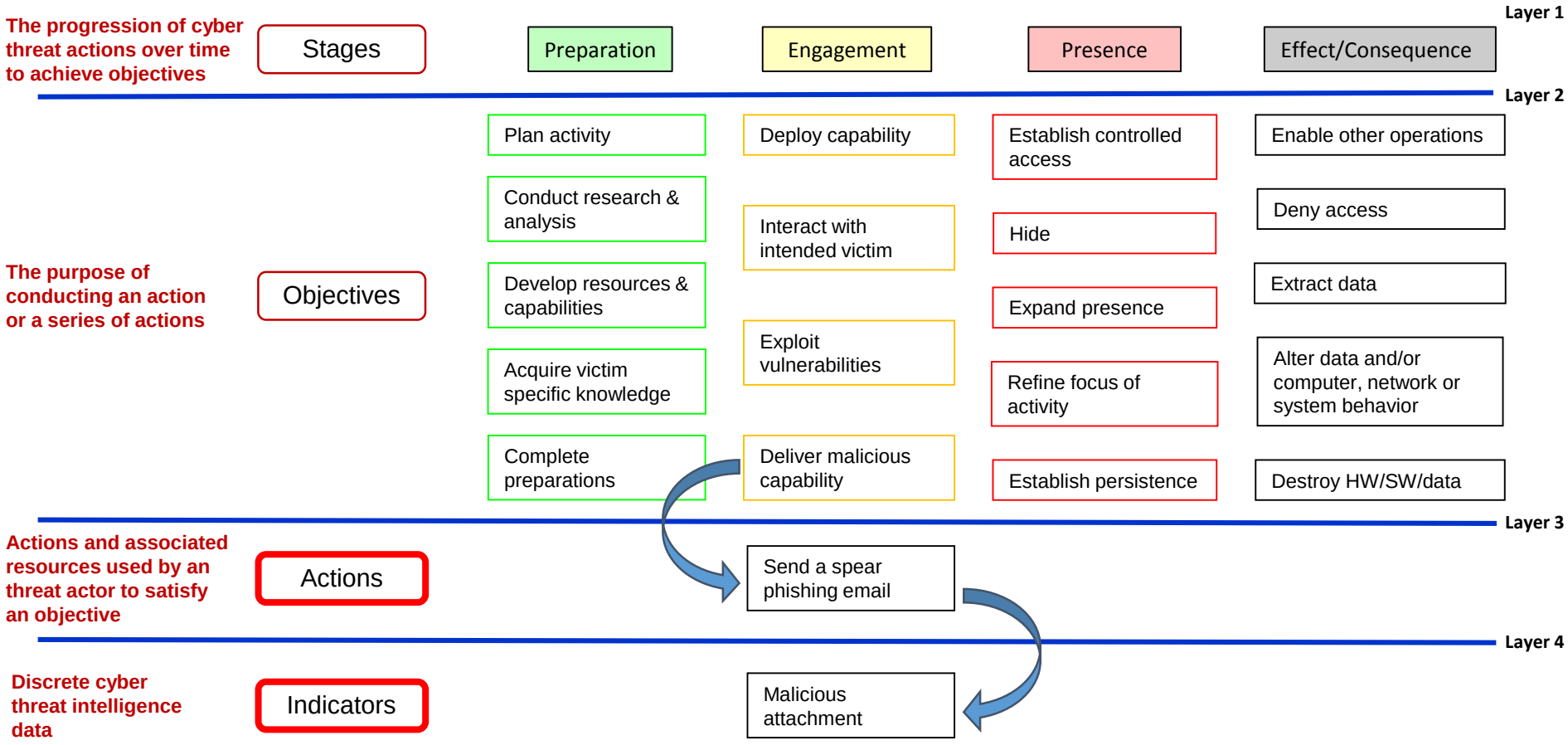


The Common Cyber Threat Framework
Threat Actor Objectives within the "Threat Lifecycle"



The Common Cyber Threat Framework

Actions and Indicators are the Details of Threat Activity



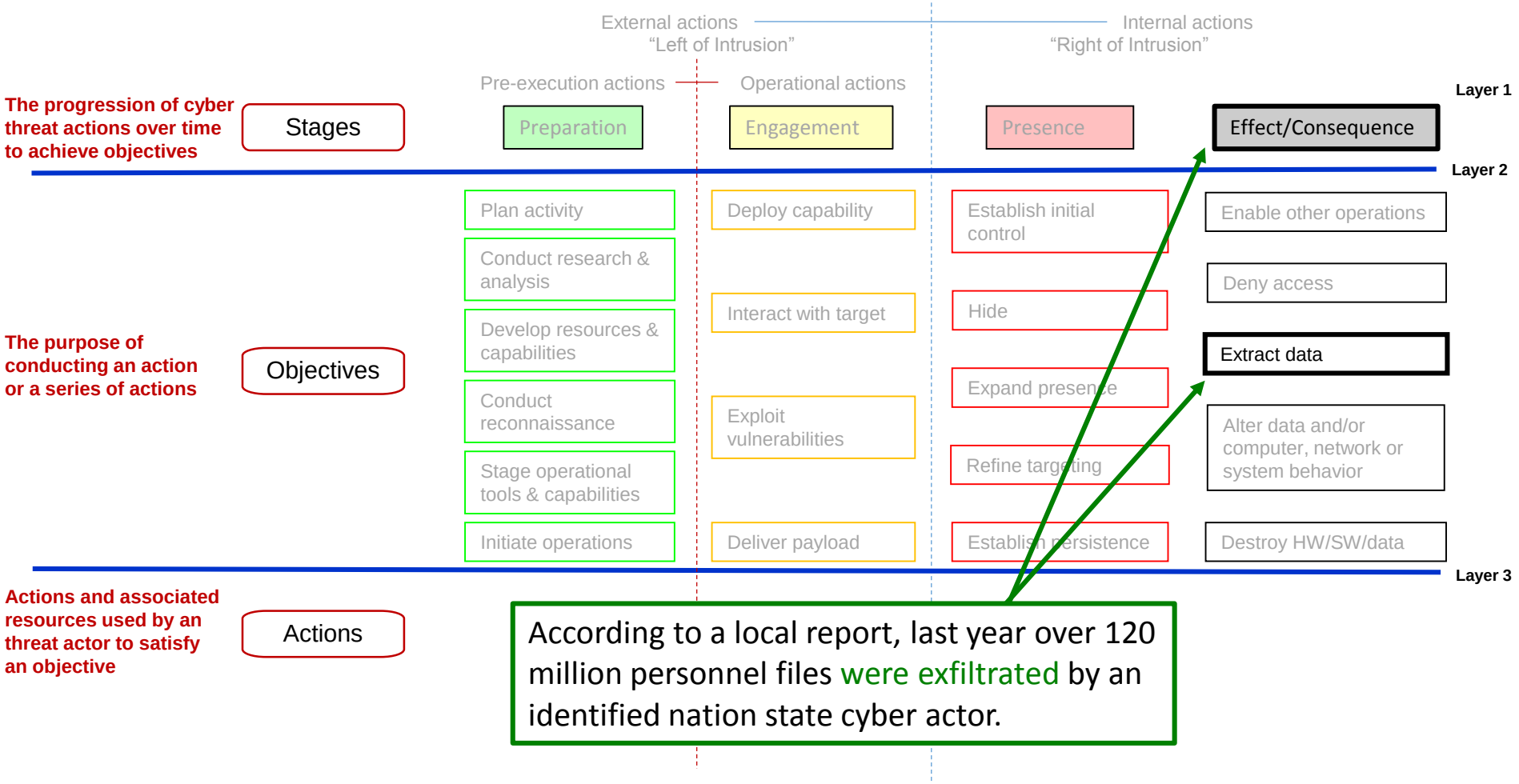
Sample Report #1

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

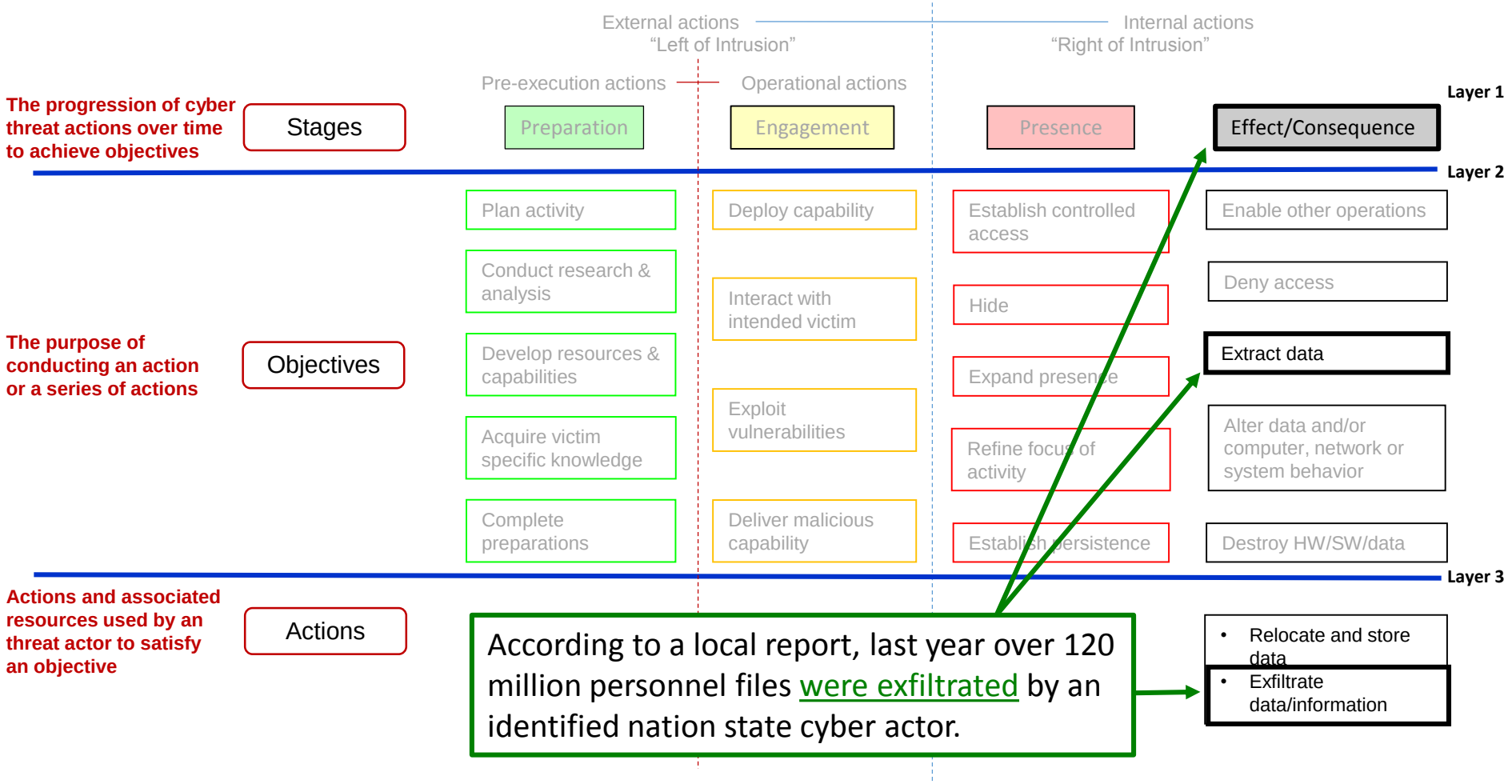
Sample Report #1 Highlighted

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

Sample Report #1 Mapped to Layer 1 and 2



Sample Report Mapped to Layers 1, 2, and 3



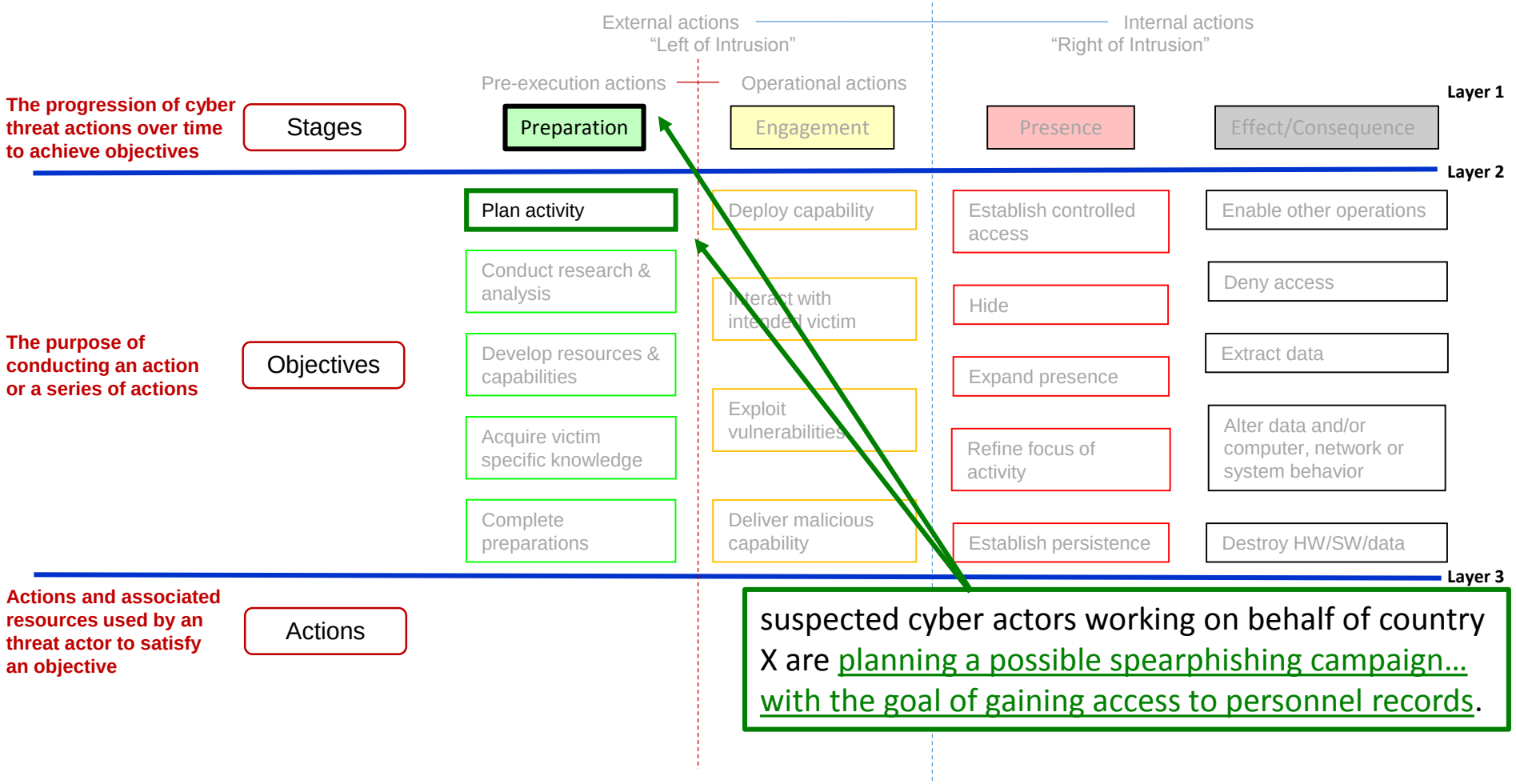
Sample Report #2

- 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.

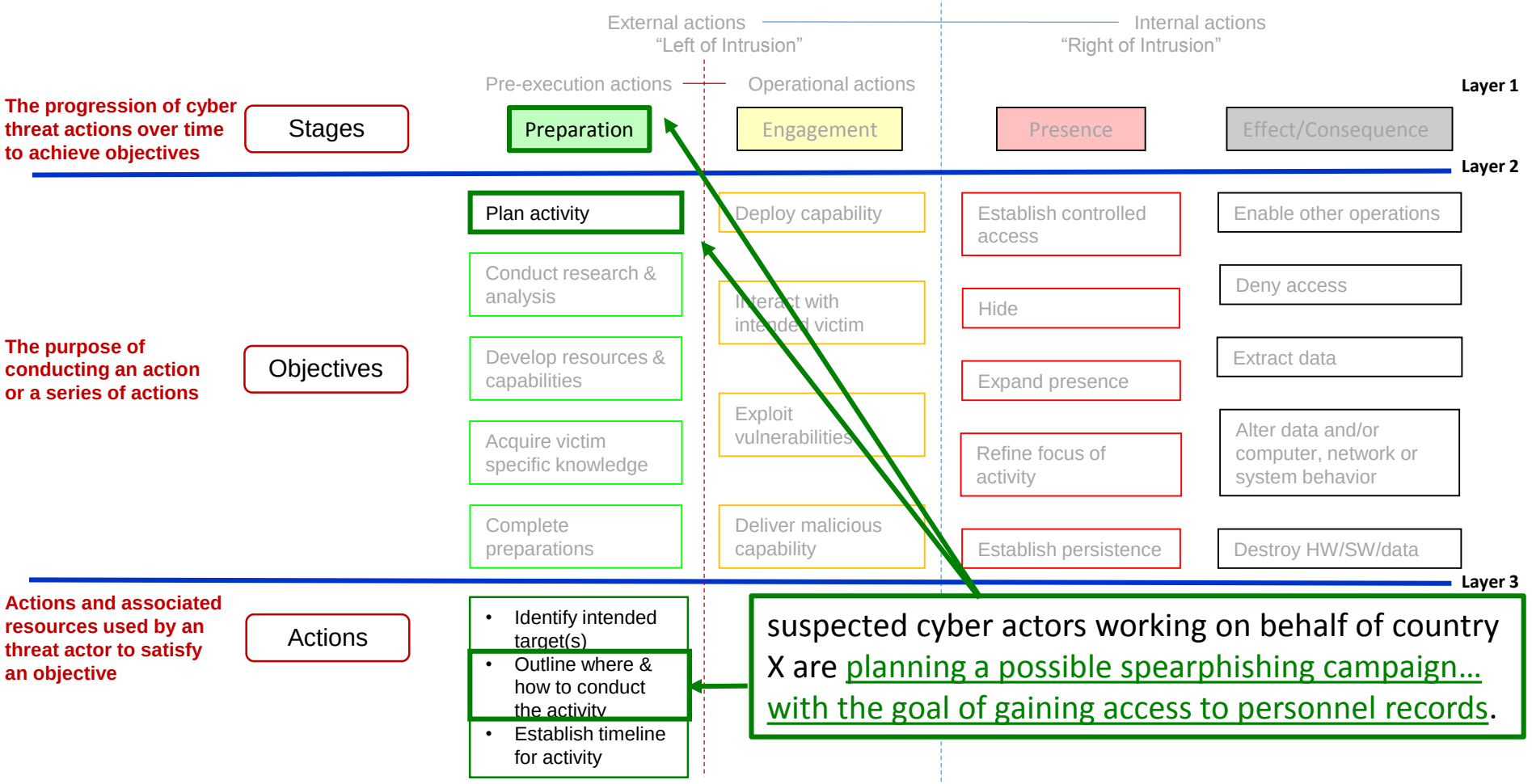
Sample Report #2 Highlighted

- 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.

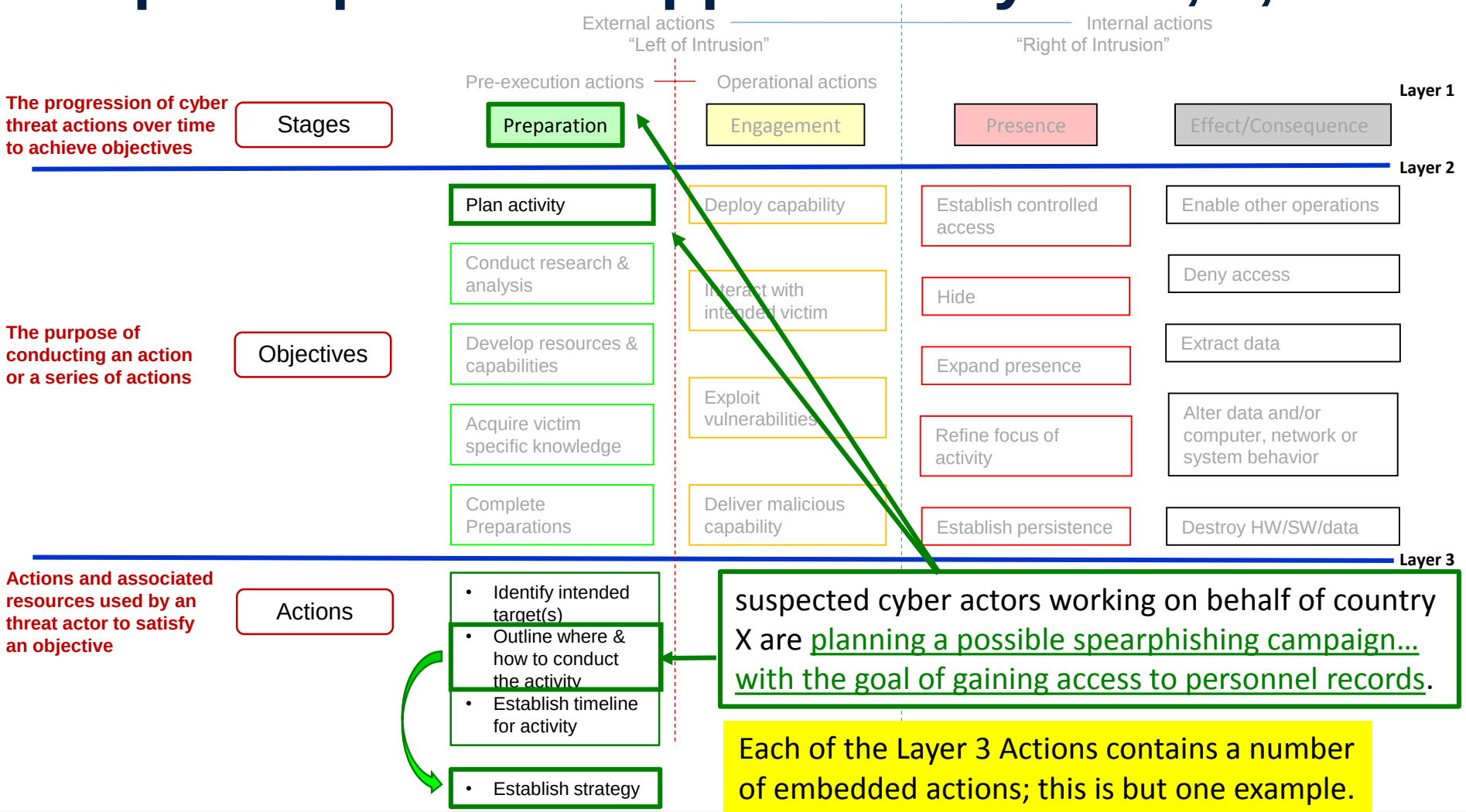
Sample Report #2 Mapped to Layers 1 and 2



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



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



Sample Report #3

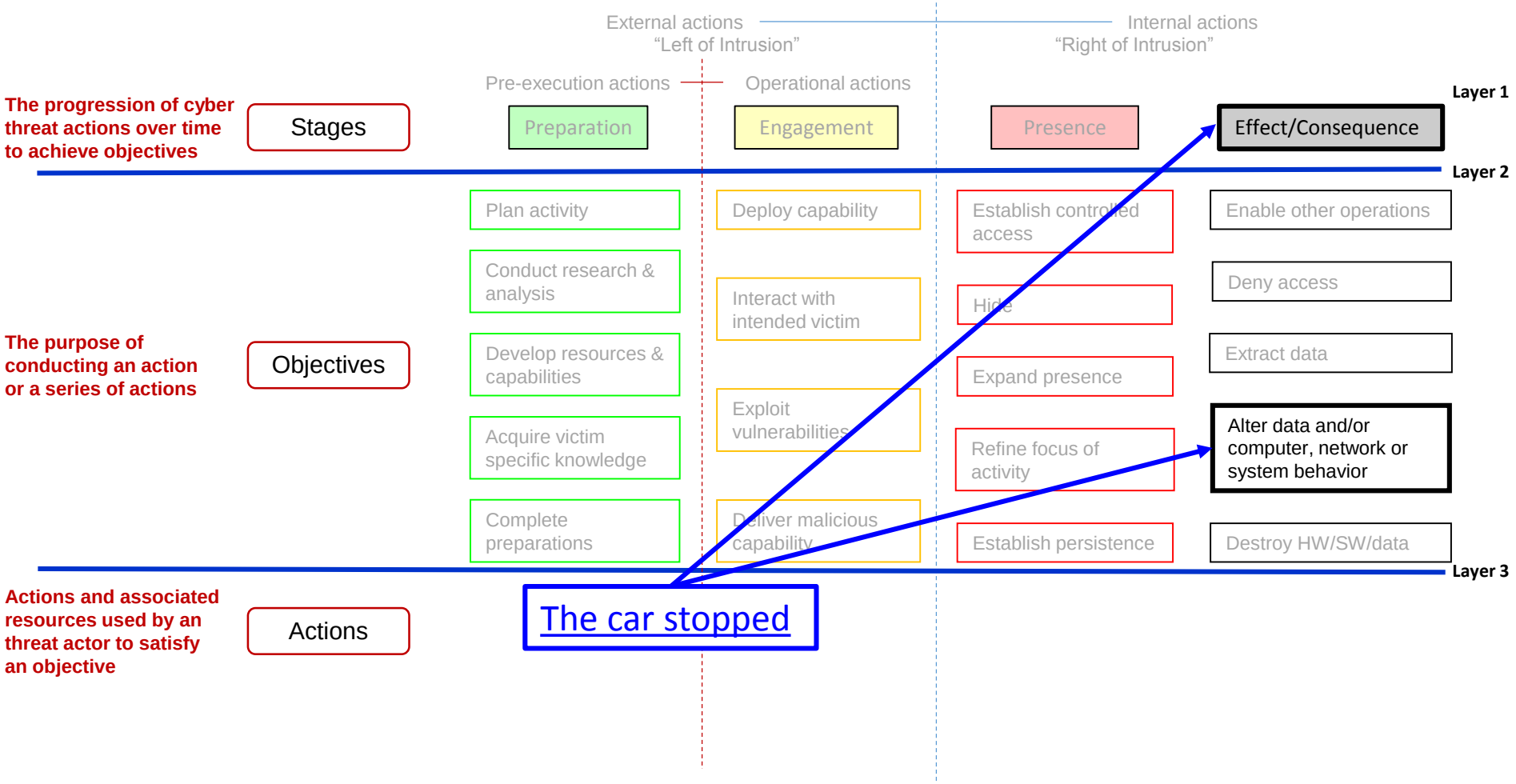
Hackers attacked a self-driving car, bringing the car to a complete stop. Investigation showed that the hackers targeted the laser ranging system, spoofed thousands of objects, and overwhelmed the system's ability to process information.

Sample Report #3 Highlighted

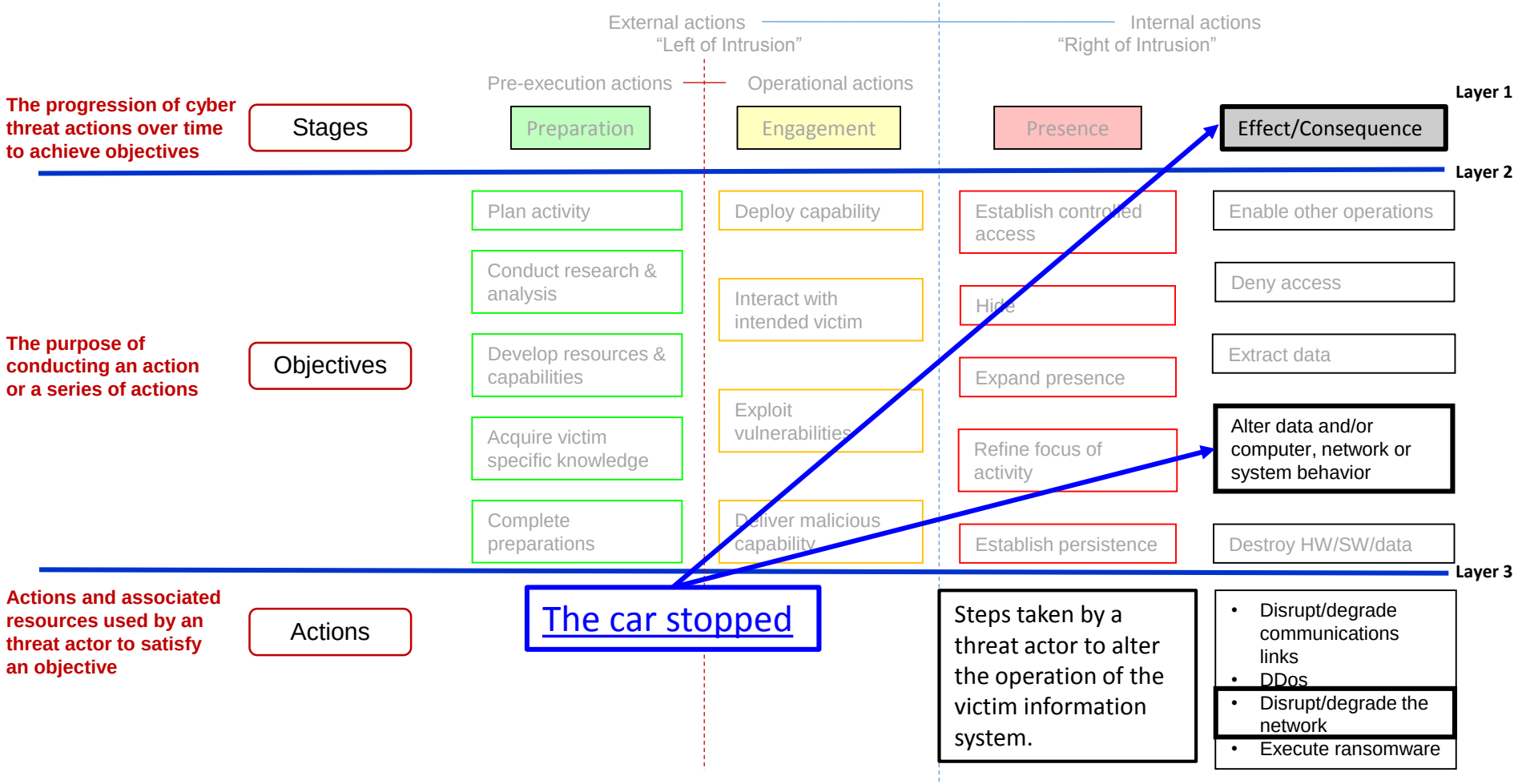
Hackers attacked a self-driving car, bringing the car to a complete stop. Investigation showed that the hackers targeted the laser ranging system, spoofed thousands of objects, and overwhelmed the system's ability to process information.

NOTE: 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.

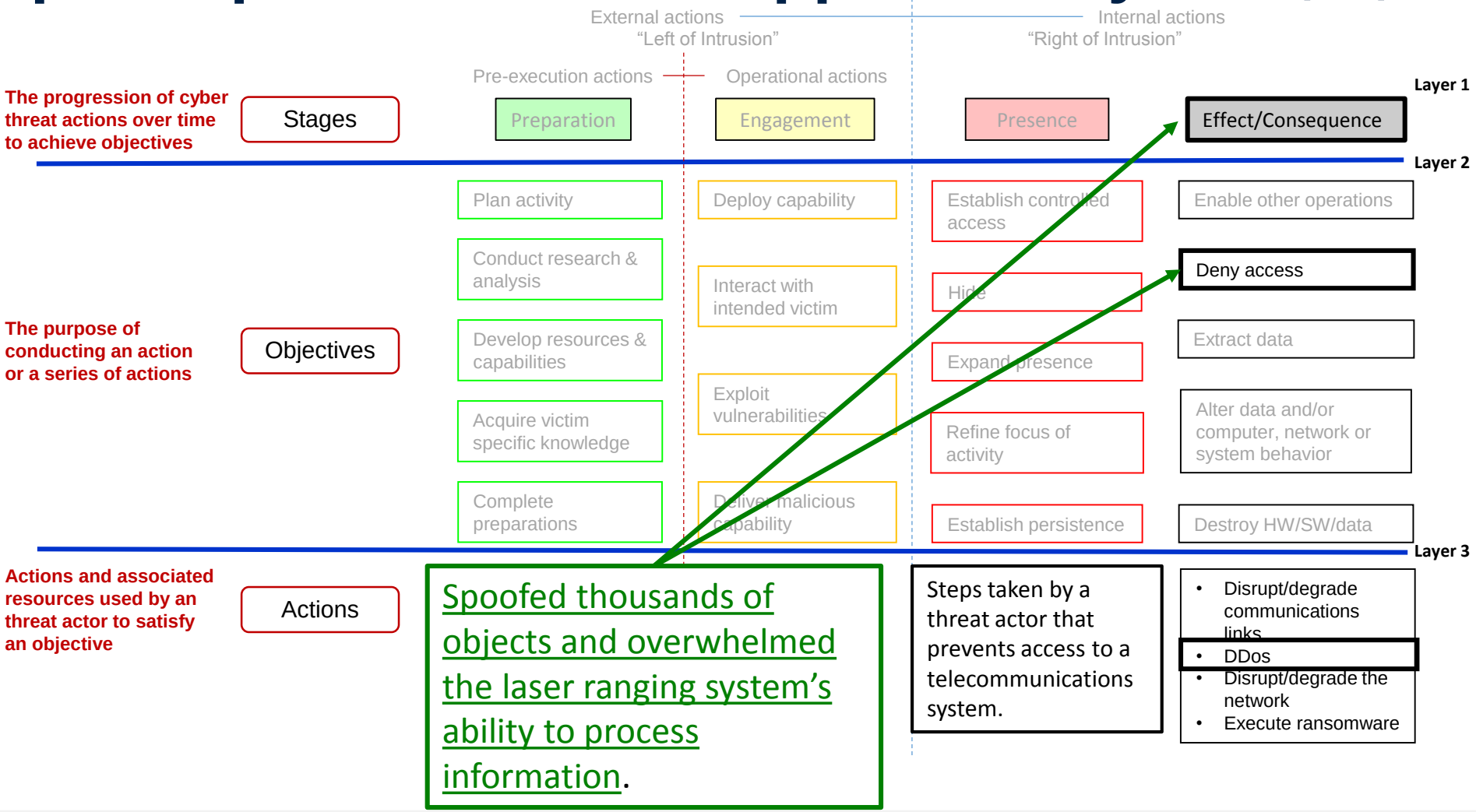
Sample Report #3 Fact 1 Mapped to Layers 1 and 2



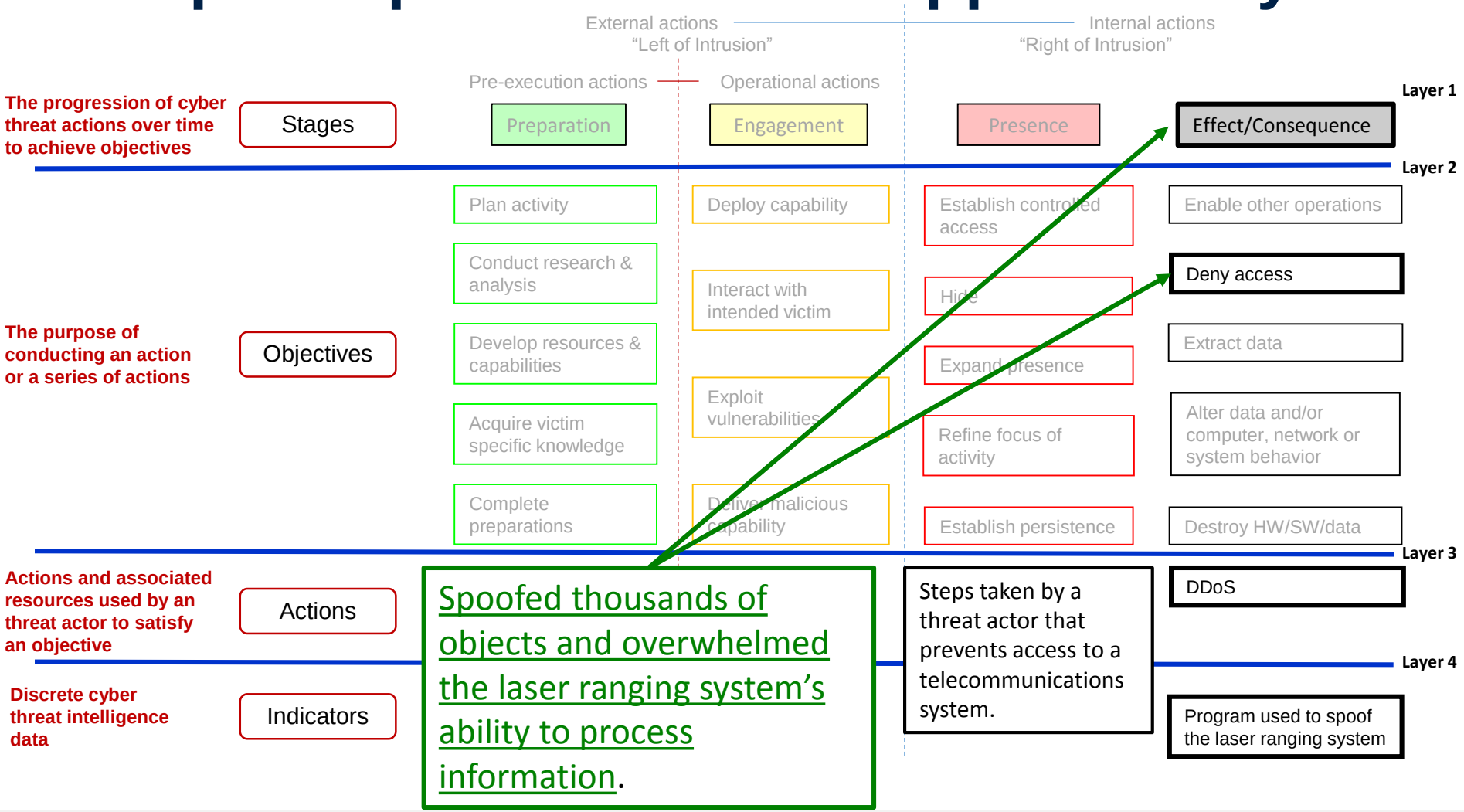
Sample Report #3 Fact 1 Mapped to Layers 1, 2, and 3



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



Sample Report #3 Fact 2 Mapped to Layer 4



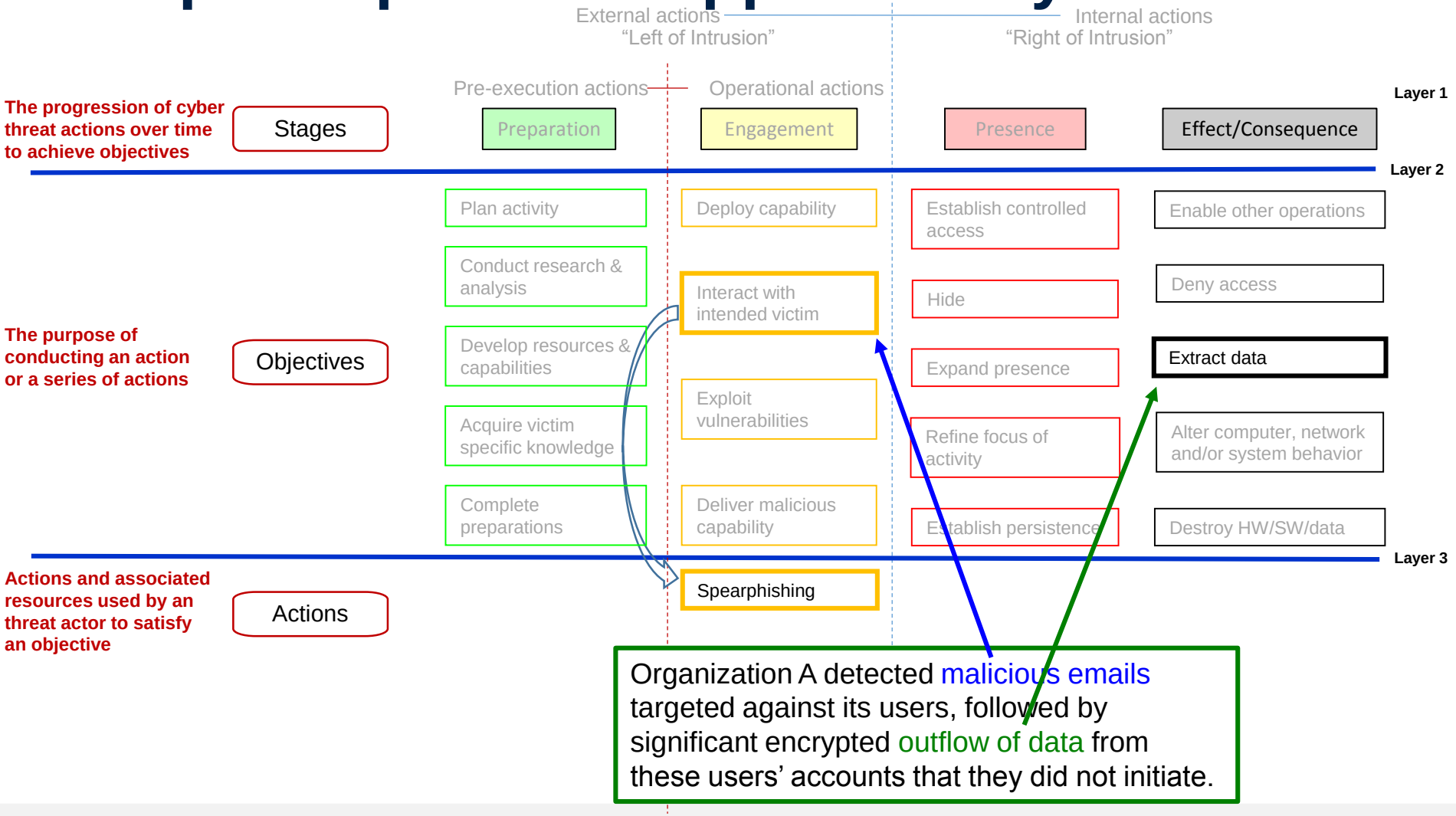
Sample Report #4

An accounting firm detected malicious emails targeted against its users, followed by significant encrypted outflow of data from these users' accounts that they did not initiate.

Sample Report #4 Highlighted

An accounting firm detected malicious emails targeted against its users, followed by significant encrypted outflow of data from these users' accounts that they did not initiate.

Sample Report #4 Mapped to Layers 2 and 3



Exercise

The Rose Hotel, a local affiliiate of the multi-national Palm Garden Hotel Corporation, suffered a cyber attack the last week in April during which their on-line reservation system was unavailable for almost a full day.

Subsequent forensic analysis revealed the presence of rosepetal malware on the system that was extracting guest information (addresses), and that the threat actor was attempting to access the Palm Garden corporate systems through the Rose Hotel system.

The Rose Hotel Manager is asking you what actions you have taken to ensure the availability of the reservation system and to disable the rosepetal malware and prevent a recurrence of the exfiltration.

The Palm Garden Corporate Board has also heard the Rose Hotel system has crashed, the Hotel is loosing revenue as a result, and the potential for legal action regarding the loss of customer information.

TASK: Demonstrate how the Cyber Threat Framework can be used to clarify the ongoing cyber threat activity, provide context, and effectively communicate threat activity and ongoing remediation efforts to both the hotel manager and the corporate board?

.

Exercise
What do we know from the Scenerio

What do we know from the Scenerio? The threat activity: The communications challenge:

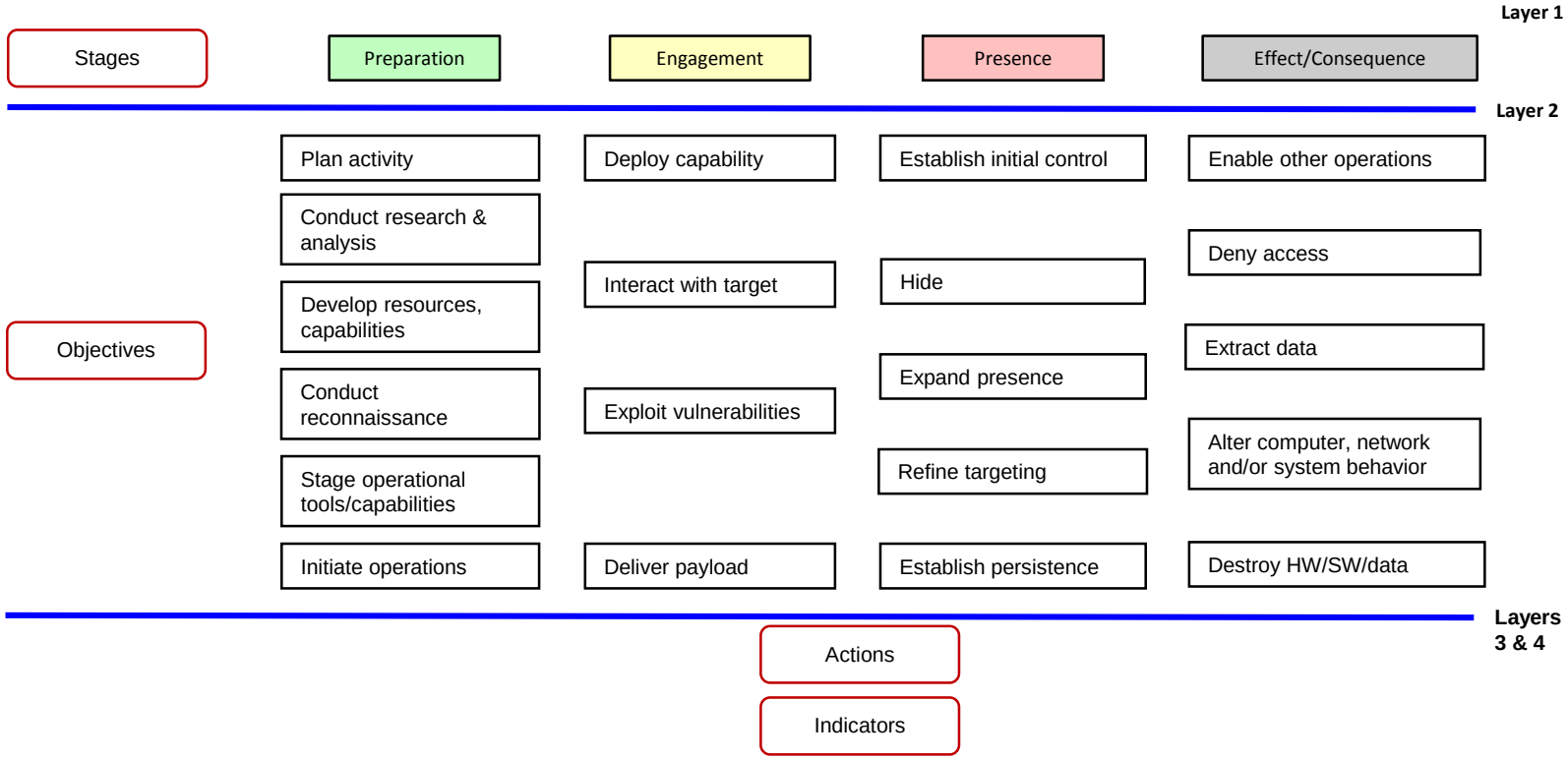
The Rose Hotel, a local affiliiate of the multi-national Palm Garden Hotel Corporation, suffered a cyber attack the last week in April during which their on-line reservation system was unavailable for almost a full day.

Subsequent forensic analysis revealed the presence of rosepetal malware on the system that was extracting guest information (addresses), and that the threat actor was attempting to access the Palm Garden corporate systems through the Rose Hotel system.

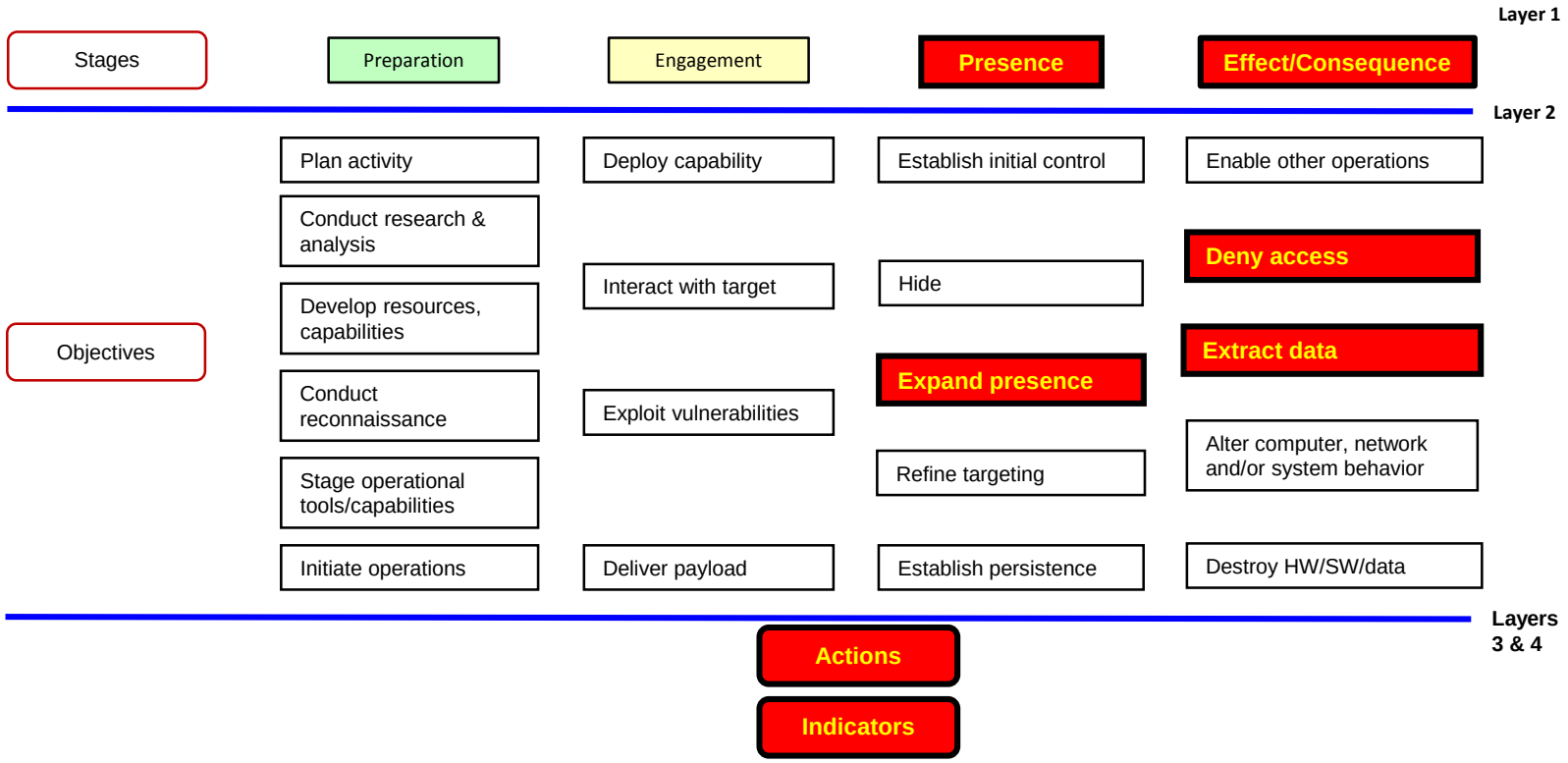
The Rose Hotel Manager is asking you what actions you have taken to ensure the availability of the reservation system and to disable the rosepetal malware and prevent a recurrence of the exfiltration.

The Palm Garden Corporate Board has also heard the Rose Hotel system has crashed, the Hotel is loosing revenue as a result, and the potential for legal action regarding the loss of customer information.

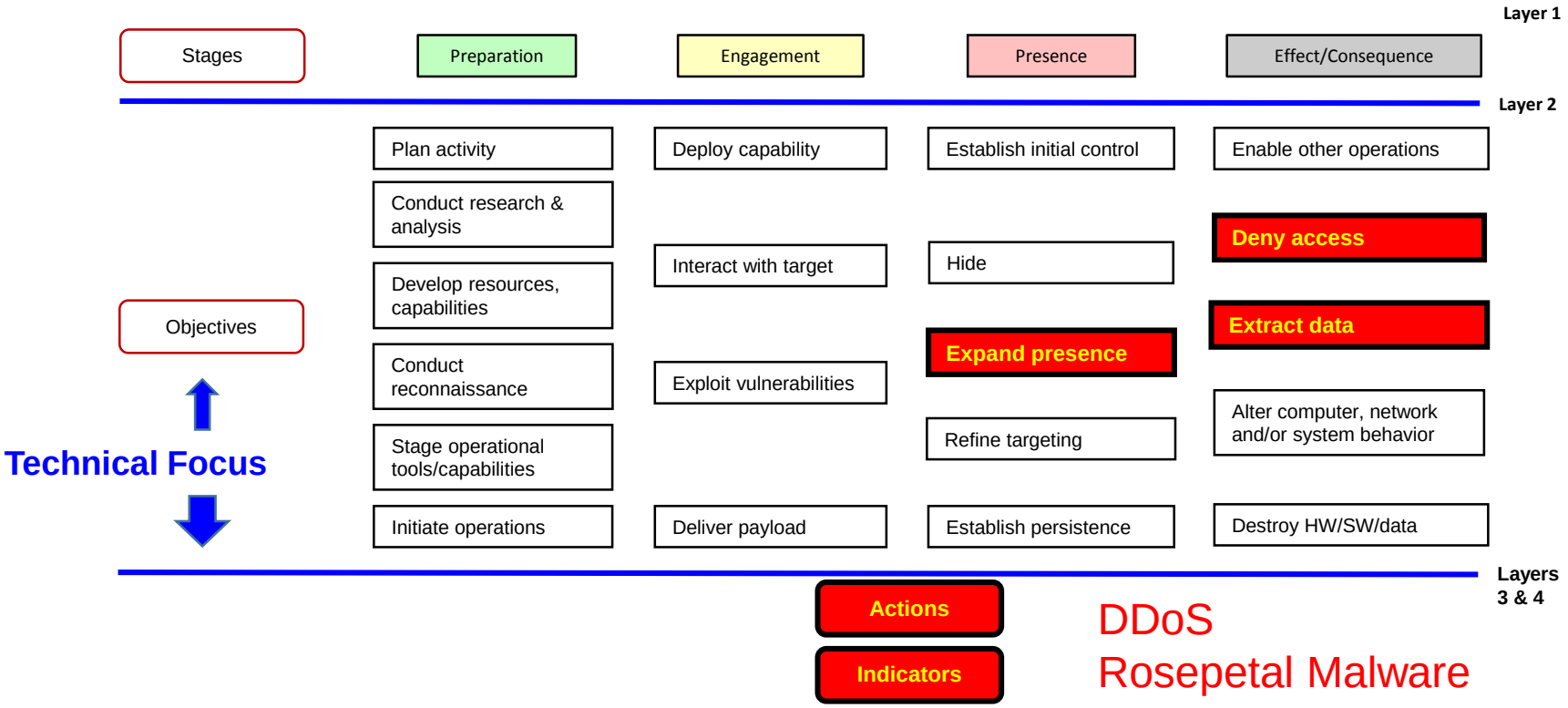
Exercise
Applying the Cyber Threat Framework



Applying the Cyber Threat Framework
What is known about the incident?

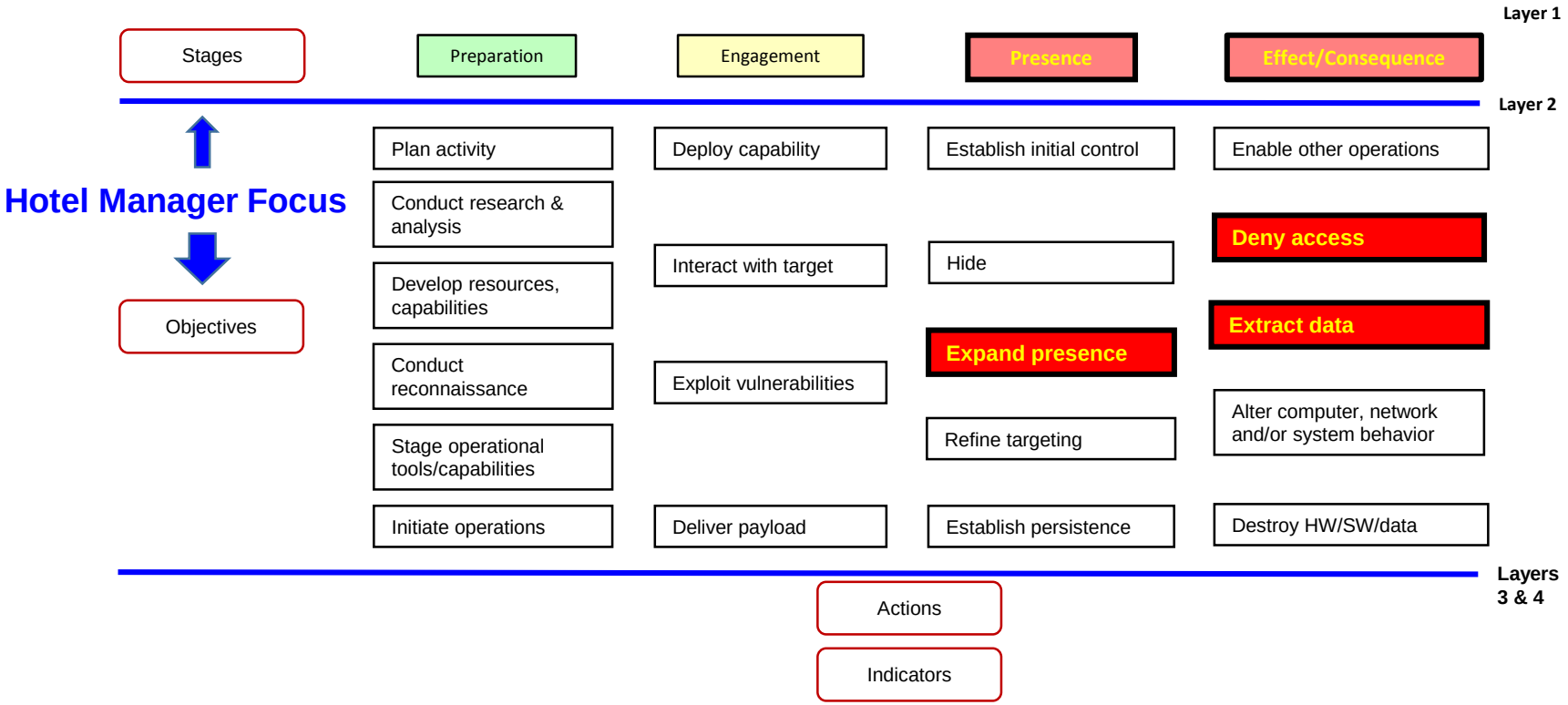


Applying the Cyber Threat Framework
What is needed to resolve the incident?



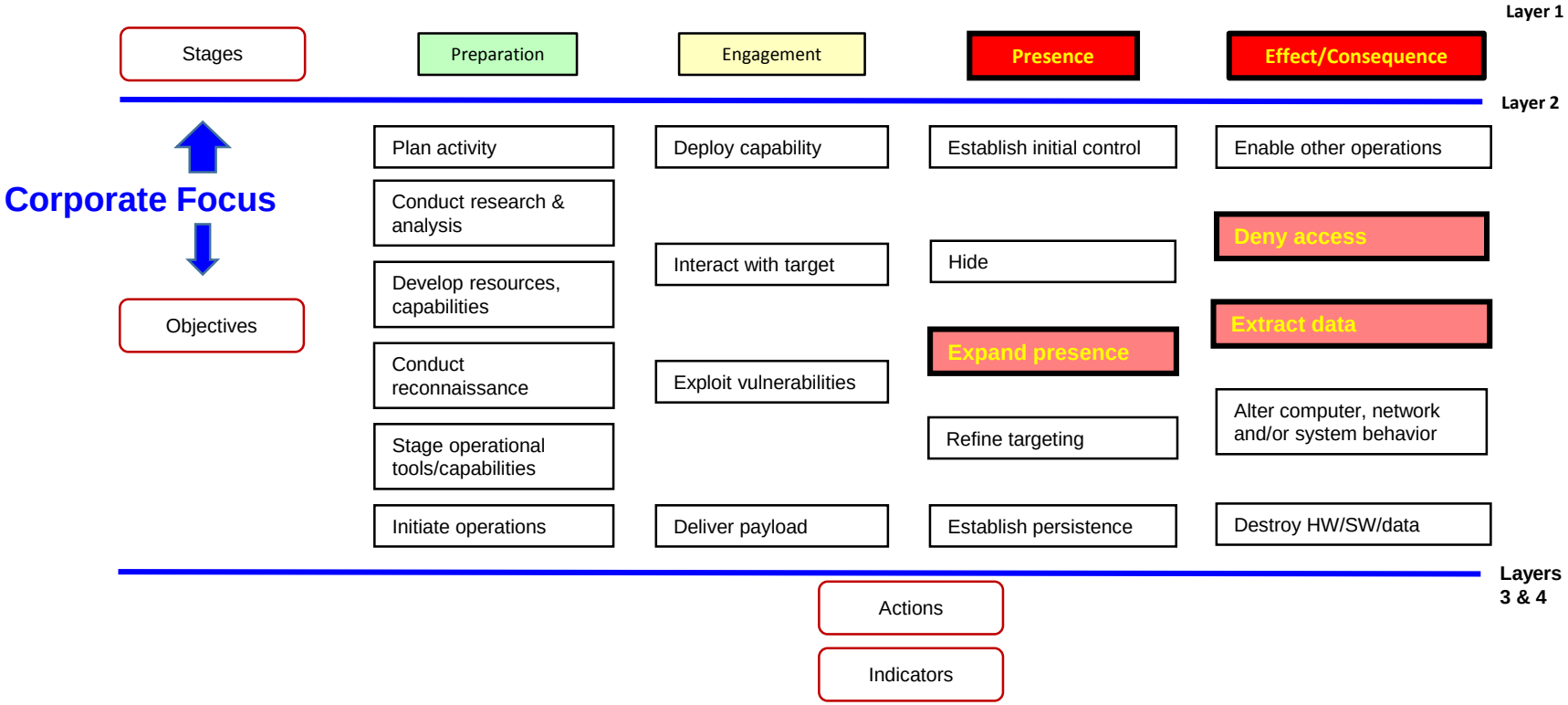
The **working level** technical details and what that impacted.

Applying the Cyber Threat Framework
What does the Hotel Manager need to know?



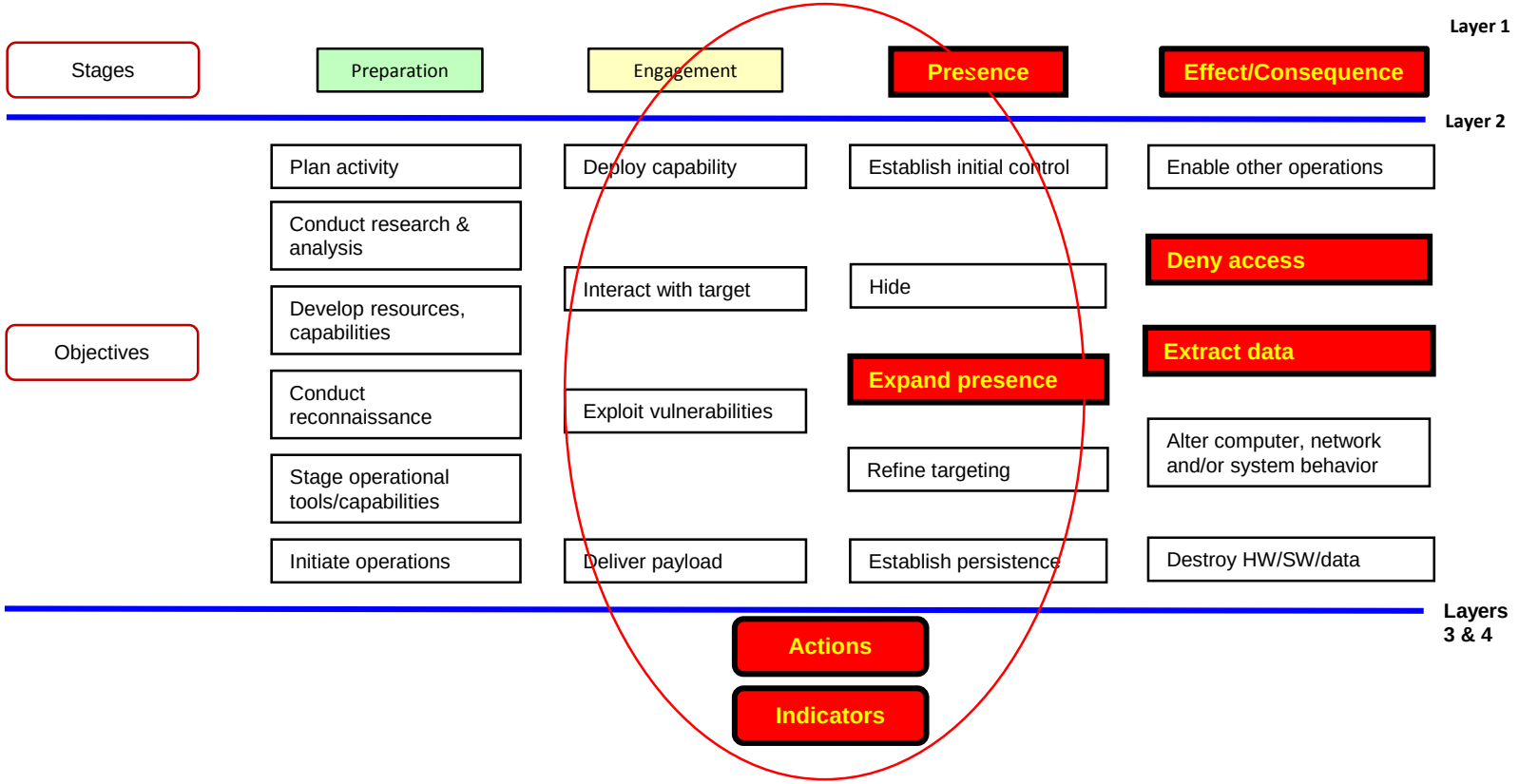
The **hotel manager** needs a summary report (layer 1 – what stage of activity) and the details of what happened (level 2 – objectives)

Applying the Cyber Threat Framework
What does Corporate need to know?



Corporate needs a summary report (layer 1 – what stage of activity) and enough of the details of what happened (level 2 – objectives) to substantiate the summary and to correct misinformation.

Applying the Cyber Threat Framework
Take-Aways



Is the hotel/corporation postured to deal with Cyber Threats (capabilities, patching, cyber hygiene)?

Why didn't the hotel see the threat coming (capability, focus, patching, threat itself)?

How does the corporation share cyber threat information (form, format, frequency)?