OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

A Common Cyber Threat Framework
How to Use

LEADING INTELLIGENCE INTEGRATION

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

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

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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Cyber Threat Framework (v4) Layers 1 and 2

External actions "Left of Intrusion" — Internal actions "Right of Intrusion"

Pre-execution actions — Operational actions

Layer 1

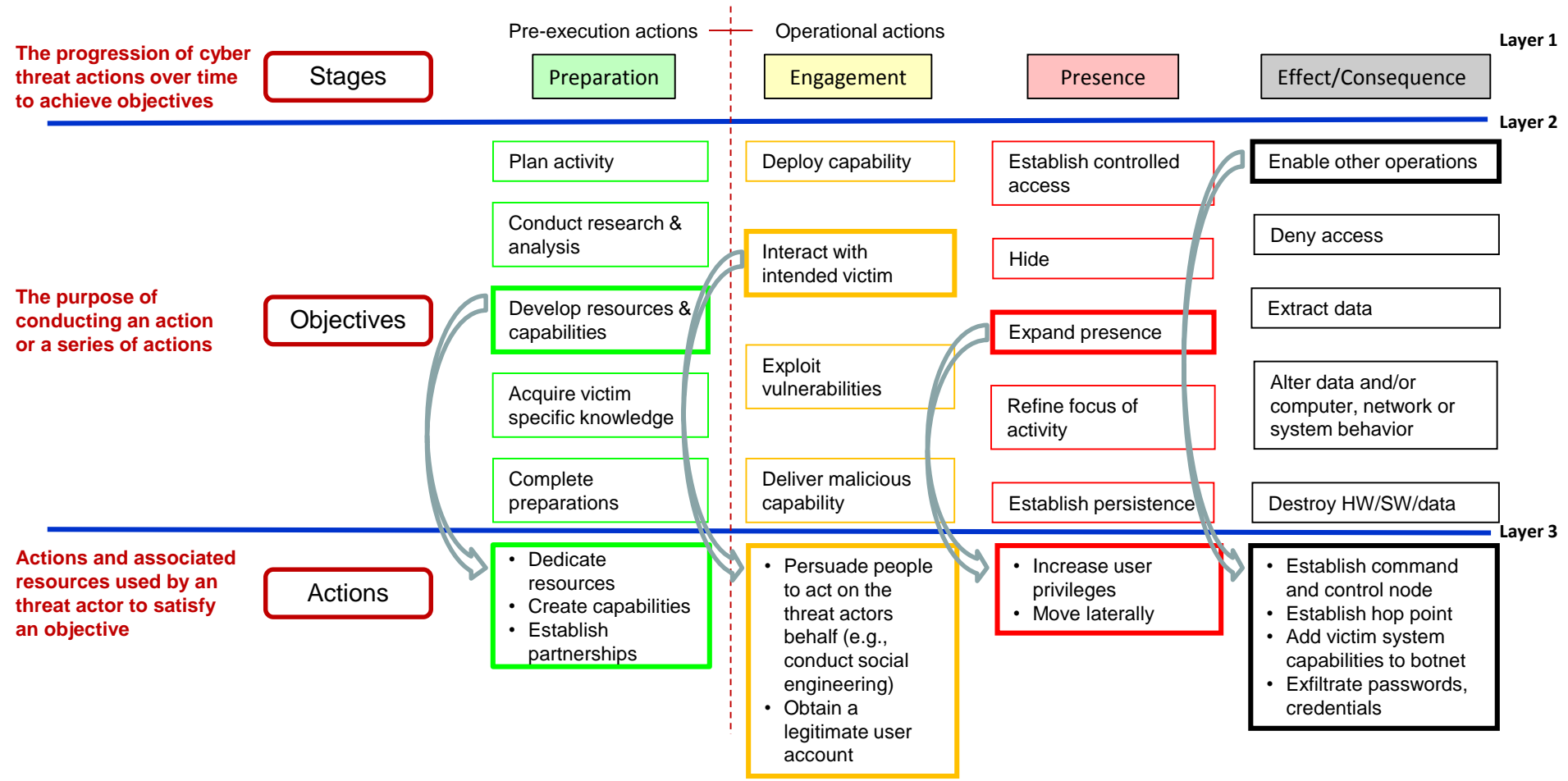|	Stages	Preparation	Engagement	Presence	Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

Layer 2

The purpose of conducting an action or a series of actions — Objectives

Preparation	Engagement	Presence	Effect/Consequence
Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities	Exploit vulnerabilities	Expand presence	Extract data
Acquire victim specific knowledge		Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Cyber Threat Framework (v4) Layer 3 Exemplars

Layer 1

Pre-execution actions | Operational actions

The progression of cyber threat actions over time to achieve objectives

Stages	Preparation	Engagement	Presence	Effect/Consequence

Layer 2

The purpose of conducting an action or a series of actions

	Preparation	Engagement	Presence	Effect/Consequence
	Plan activity	Deploy capability	Establish controlled access	Enable other operations
Objectives	Conduct research & analysis	Interact with intended victim	Hide	Deny access
	Develop resources & capabilities		Expand presence	Extract data
	Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
	Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

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

Actions	Preparation	Engagement	Presence	Effect/Consequence
	• Dedicate resources • Create capabilities • Establish partnerships	• Persuade people to act on the threat actors behalf (e.g., conduct social engineering) • Obtain a legitimate user account	• Increase user privileges • Move laterally	• Establish command and control node • Establish hop point • Add victim system capabilities to botnet • Exfiltrate passwords, credentials

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Cyber Threat Framework (v4) Layer 4 Exemplar

External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions | Operational actions

	Stages	Preparation	Engagement	Presence	Effect/Consequence

The progression of cyber threat actions over time to achieve objectives — Layer 1

Layer 2

	Objectives	Preparation	Engagement	Presence	Effect/Consequence
		Plan activity	Deploy capability	Establish controlled access	Enable other operations
		Conduct research & analysis	Interact with intended victim	Hide	Deny access
		Develop resources & capabilities		Expand presence	Extract data
		Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
		Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

The purpose of conducting an action or a series of actions

Layer 3

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

Actions

- Dedicate resources
- Create capabilities
- Establish partnerships

> These are representative Actions that can contribute to achieving the Layer 2 Objectives.

Layer 4

Discrete cyber threat intelligence data

Indicators

Company XXX reported to have created Malware QQ

> This is a simple example of the multitude of potential Indicators of threat actor Actions.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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

	Layer	
Executive	**Layer 1**	Stages
Executive	**Layer 2**	Objectives
Tactical	**Layer 3**	Actions
Tactical	**Layer 4**	Indicators

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Cyber Threat Framework (v4)

External actions — "Left of Intrusion" Internal actions — "Right of Intrusion"

Pre-execution actions — Operational actions

	Preparation	Engagement	Presence	Effect/Consequence
Stages — The progression of cyber threat actions over time to achieve objectives				**Layer 1**
	Plan activity	Deploy capability	Establish controlled access	Enable other operations
	Conduct research & analysis	Interact with intended victim	Hide	Deny access
Objectives — The purpose of conducting an action or a series of actions	Develop resources & capabilities		Expand presence	Extract data
	Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
	Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 2

Layer 3

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

Layer 4

Indicators — Discrete cyber threat intelligence data

This one page outline can help identify layer 1 or layer 2 category of reported information

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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 data and/or computer, network, and/or system behavior	
	Alter data stored on the victim's system(s)
	Change process run-state on victim system(s)
	Change decisions
	Change machine-to-machine (MtM) communications
Destroy hardware/software/data	

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

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

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 intitial 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.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Sample Report #1 Highlighted

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

Sample Report #1 Tagged to Layer 1 and 2

External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions — Operational actions

Layer 1

	Preparation	Engagement	Presence	Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

Stages

Layer 2

The purpose of conducting an action or a series of actions

Objectives

Preparation	Engagement	Presence	Effect/Consequence
Plan activity	Deploy capability	Establish initial control	Enable other operations
Conduct research & analysis		Hide	Deny access
Develop resources & capabilities	Interact with target		Extract data
Conduct reconnaissance	Exploit vulnerabilities	Expand presence	Alter data and/or computer, network or system behavior
Stage operational tools & capabilities		Refine targeting	
Initiate operations	Deliver payload	Establish persistence	Destroy HW/SW/data

Layer 3

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

Actions

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

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

External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions — Operational actions

Layer 1

The progression of cyber threat actions over time to achieve objectives

Stages	Preparation	Engagement	Presence	Effect/Consequence

Layer 2

The purpose of conducting an action or a series of actions

Objectives	Plan activity	Deploy capability	Establish controlled access	Enable other operations
	Conduct research & analysis	Interact with intended victim	Hide	Deny access
	Develop resources & capabilities	Exploit vulnerabilities	Expand presence	Extract data
	Acquire victim specific knowledge		Refine focus of activity	Alter data and/or computer, network or system behavior
	Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

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

Actions

According to a local report, last year over 120 million personnel files <u>were exfiltrated</u> by an identified nation state cyber actor.

- Relocate and store data
- Exfiltrate data/information

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

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

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.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Sample Report #2 Tagged to Layers 1 and 2

External actions "Left of Intrusion" — Internal actions "Right of Intrusion"

Pre-execution actions — Operational actions

Layer 1

	Stages	Preparation	Engagement	Presence	Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

Layer 2

The purpose of conducting an action or a series of actions — Objectives

Preparation	Engagement	Presence	Effect/Consequence
Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

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

suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign... with the goal of gaining access to personnel records.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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

External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions — Operational actions

Layer 1

	Stages	Preparation	Engagement	Presence	Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

Layer 2

The purpose of conducting an action or a series of actions

Objectives

Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

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

Actions

- Identify intended target(s)
- Outline where & how to conduct the activity
- Establish timeline for activity

suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign... with the goal of gaining access to personnel records.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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

External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions —— Operational actions

Layer 1

The progression of cyber threat actions over time to achieve objectives

Stages	Preparation	Engagement	Presence	Effect/Consequence

Layer 2

The purpose of conducting an action or a series of actions

Objectives

Preparation	Engagement	Presence	Effect/Consequence
Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete Preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

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

Actions

- Identify intended target(s)
- Outline where & how to conduct the activity
- Establish timeline for activity
- Establish strategy

suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign... with the goal of gaining access to personnel records.

Each of the Layer 3 Actions contains a number of embedded actions; this is but one example.

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.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
LEADING INTELLIGENCE INTEGRATION

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

The progression of cyber threat actions over time to achieve objectives — Stages

External actions "Left of Intrusion" / Internal actions "Right of Intrusion"

Pre-execution actions / Operational actions

Layer 1

Preparation	Engagement	Presence	Effect/Consequence

Layer 2

Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

The purpose of conducting an action or a series of actions — Objectives

Layer 3

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

The car stopped

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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

External actions — Internal actions
"Left of Intrusion" — "Right of Intrusion"

Pre-execution actions — Operational actions

Layer 1

	Stages	Preparation	Engagement	Presence	Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

Layer 2

The purpose of conducting an action or a series of actions — Objectives

Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

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

The car stopped

Steps taken by a threat actor to alter the operation of the victim information system.

- Disrupt/degrade communications links
- DDos
- Disrupt/degrade the network
- Execute ransomware

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
LEADING INTELLIGENCE INTEGRATION

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

External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions   Operational actions

Layer 1

	Stages	Preparation	Engagement	Presence	Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

Layer 2

The purpose of conducting an action or a series of actions — Objectives

Preparation	Engagement	Presence	Effect/Consequence
Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

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

Spoofed thousands of objects and overwhelmed the laser ranging system's ability to process information.

Steps taken by a threat actor that prevents access to a telecommunications system.

- Disrupt/degrade communications links
- DDos
- Disrupt/degrade the network
- Execute ransomware

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Sample Report #3 Fact 2 Tagged to Layer 4

External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions | Operational actions

The progression of cyber threat actions over time to achieve objectives

Stages — Layer 1

| Preparation | Engagement | Presence | Effect/Consequence |

Layer 2

Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

The purpose of conducting an action or a series of actions

Objectives

Layer 3

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

Actions

Spoofed thousands of objects and overwhelmed the laser ranging system's ability to process information.

Steps taken by a threat actor that prevents access to a telecommunications system.

DDoS

Layer 4

Discrete cyber threat intelligence data

Indicators

Program used to spoof the laser ranging system

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Threat Actor	Preparation	Engagement	Presence	Effect/Consequence

Cyber Threat Activity – CTF Layer 1 Stages Exemplar
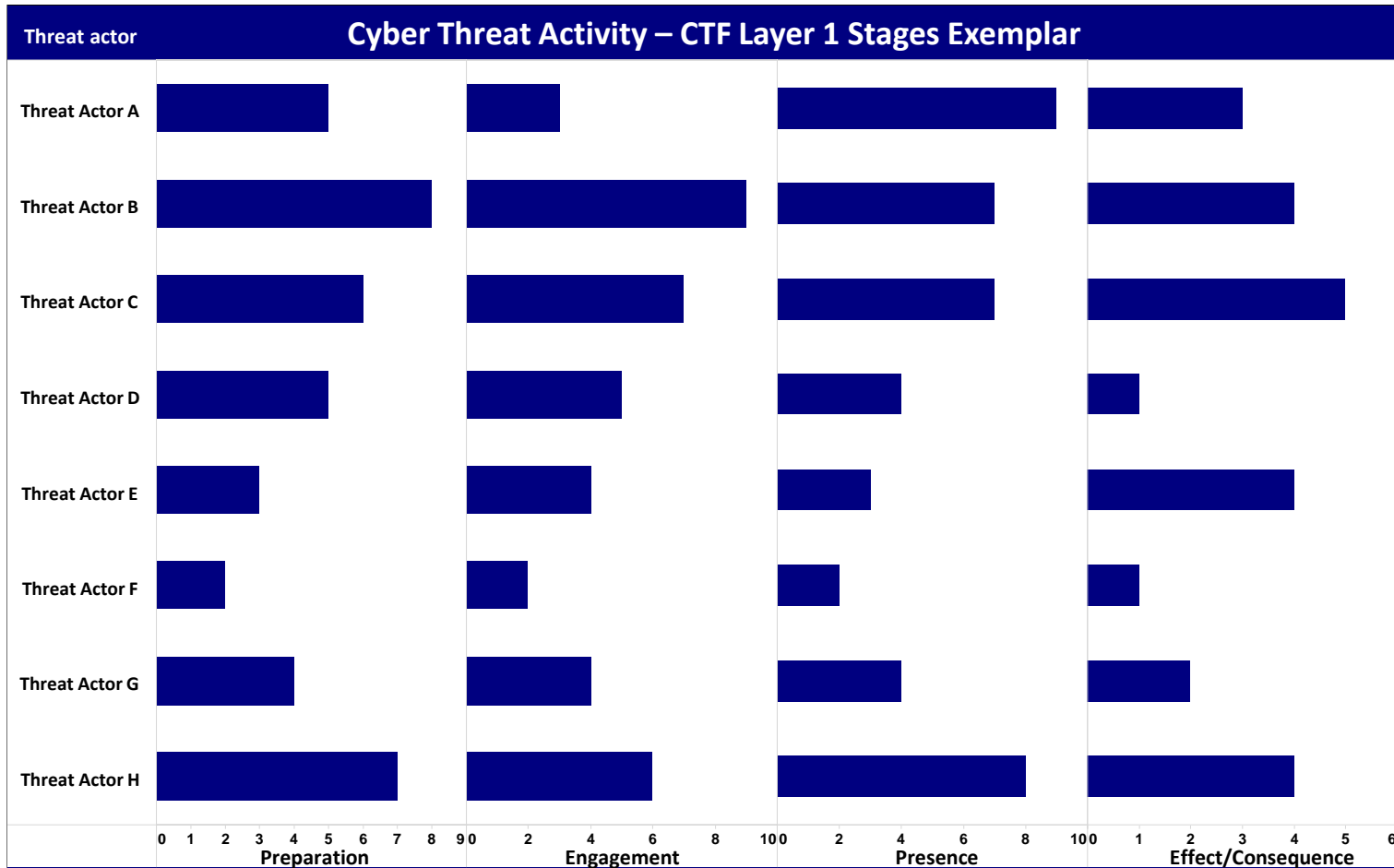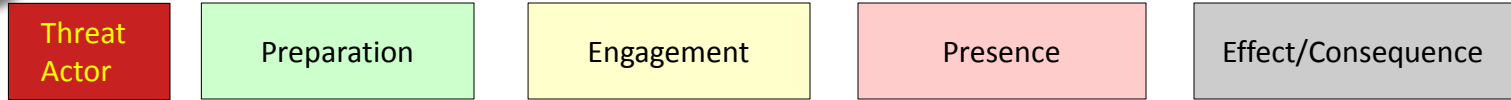
Reporting Period: January – March 2016

CTF (v4) Layer 2 Objectives Exemplar


Layer 1 Stages	Layer 2 Objectives	Threat Actor A	Threat Actor B	Threat Actor C	Threat Actor D	Threat Actor E	Threat Actor F	Threat Actor G	Threat Actor H
Preparation	Plan activity	·	·	■	·	·	·	·	·
	Conduct research & analysis	■	■	■	■	■	■	■	■
	Develop resources & capabilities	■	·	■	■	·	■	·	·
	Acquire victim specific knowledge	·	■	·	■	■	■	■	■
	Complete preparations	■	·	·	·	·	·	■	■
Engagement	Develop capability	·	■	·	■	■	■	■	■
	Interact with intended victim	·	■	■	■	■	■	·	■
	Exploit vulnerabilities	■	■	■	■	■			
	Deliver malicious capability	·	·	·	·	·	·	·	·
Presence	Establish controlled access	■	■	■		■	■	■	■
	Hide	■	■	■		■	■	■	■
	Expand presence	■	■	·	·	·	·	■	■
	Refine focus of activity	■	■	■	■	·	■	·	·
	Establish persistence	■	■	·	■	·	·	·	·
Effect/Consequence	Enable other operations	■	■	■	■	■	■	■	■
	Deny Access	·	■	■	■	■	·	■	■
	Extract data	■	■	■	■	■	■	■	■
	Alter data and/or computer, network or system behavior	■	·	·	■	·	·	■	·
	Destroy HW/SW/data	·	·	■	·	·	·	·	■

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION
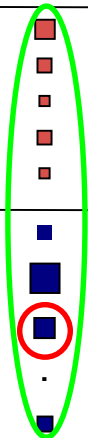
Trend Analysis - Threat Activity Over Time

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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION
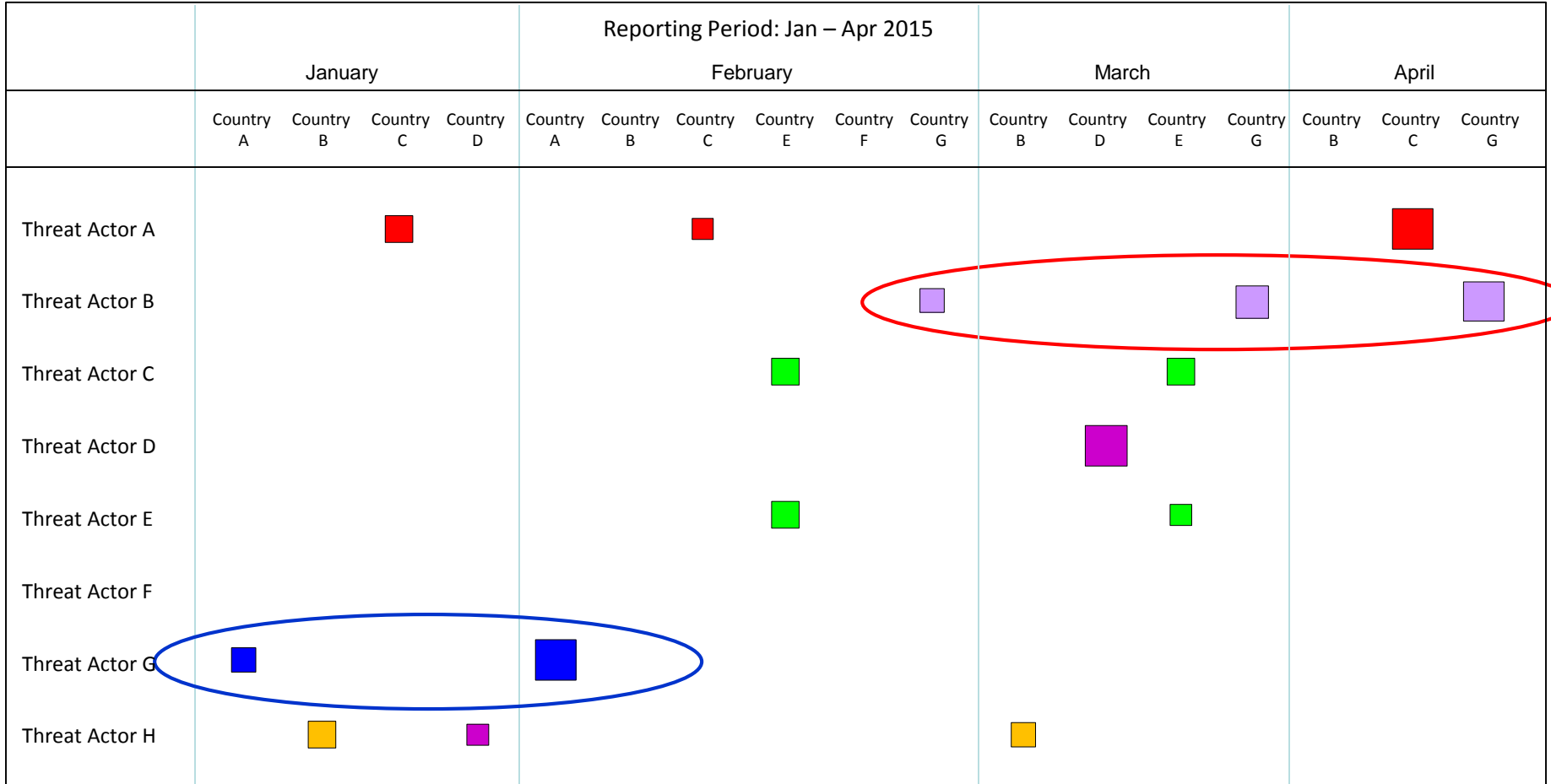
Summary

- 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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Questions?