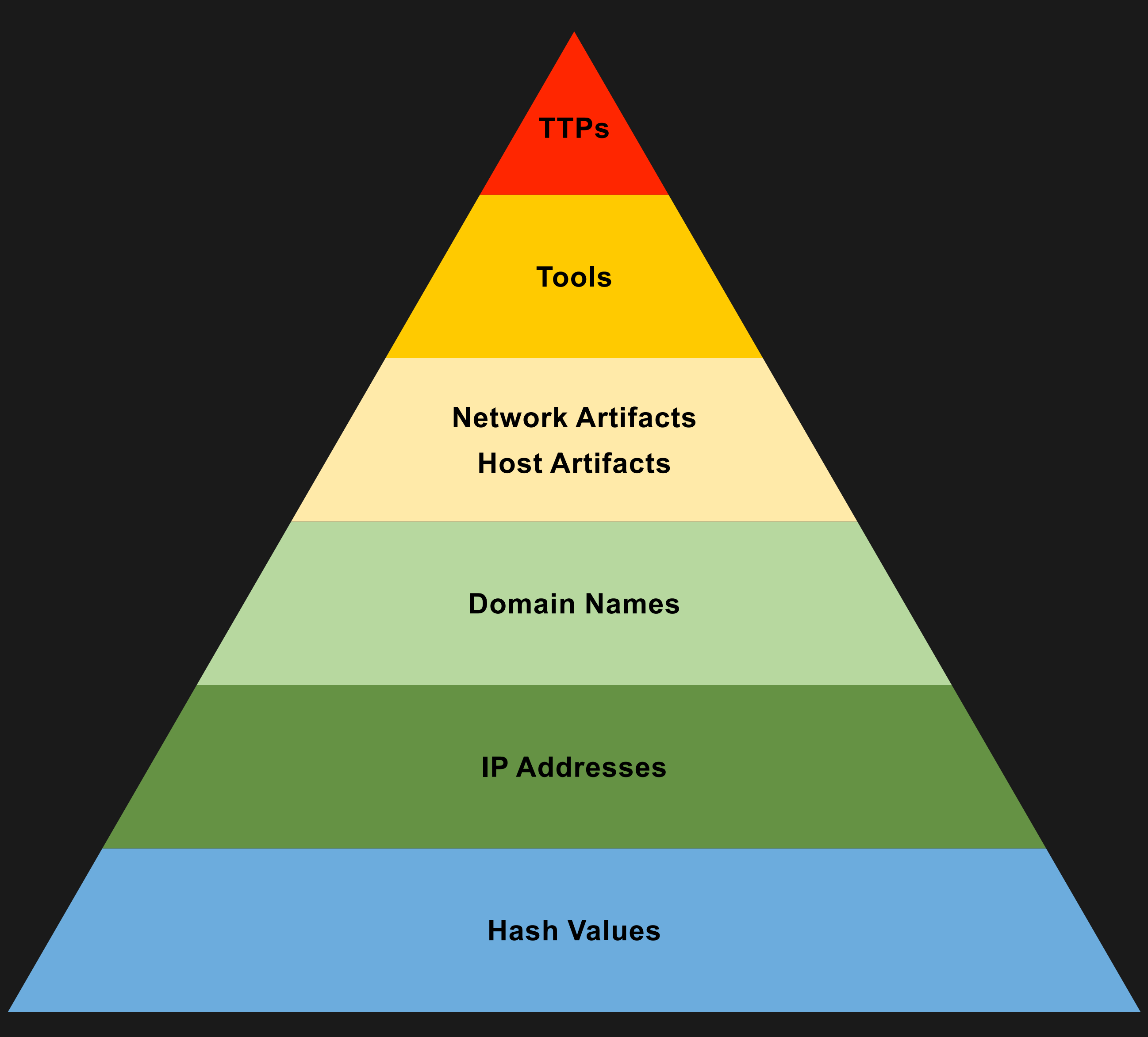
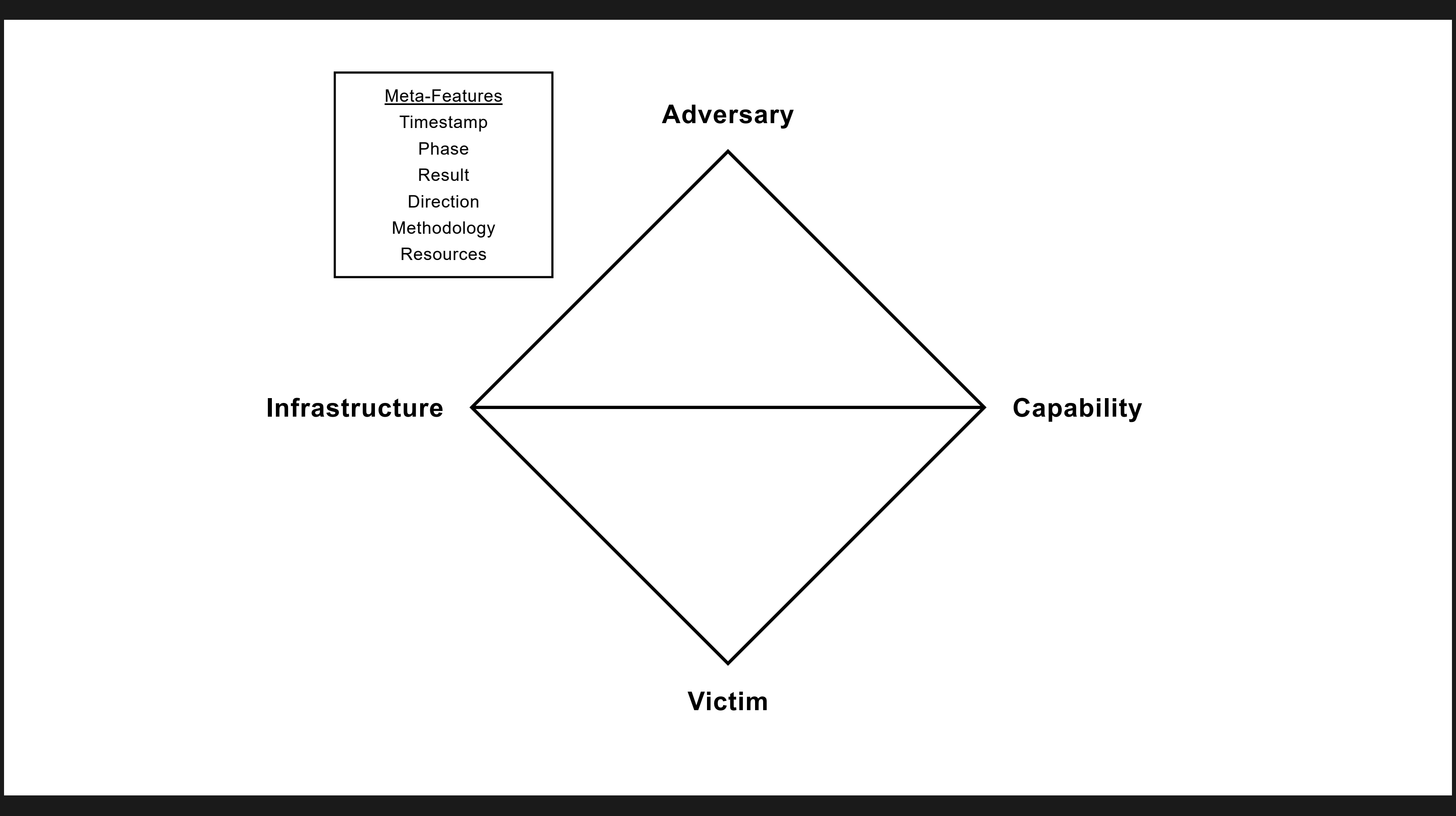
PYRAMID OF PAIN



DIAMOND MODEL OF INTRUSION ANALYSIS



Adversary	Attacker, Enemy, Cyber Threat Actor, Cyber Threat Organization, Hacker
Adversary Operator	The entity that conducts the attack
Adversary Consumer	The entity that stands to benefit from the attack
Victim	Organization, Person, Email Address, IP Address, Social Account, Domain etc.
Victim Personae	The entities that are being targeted and whose assets are being attacked (Organizations, People)
Victim Assets	Systems, Networks, Email Addresses, IP Addresses, Social Accounts, Domains etc.
Capability	Skills, Tools, Tactics Techniques Procedures (TTPs)
Capability Capacity	All of the vulnerabilities and exposures that an individual capability can use regardless of the victim
Adversary Arsenal	An adversary's complete set of capabilities (Capabilities + Capacities)
Infrastructure	Hardware (physical) or Software (logical) communication structures the adversary uses to deliver a capability or maintain control of a capability (C2), and effect results from a victim (exfiltrate data)
Type 1 Infrastructure	Infrastructure controlled or owned by the adversary
Type 2 Infrastructure	Infrastructure controlled or owned by an intermediary that might or might not be aware of it (Malware Staging Servers, Compromised Systems, Compromised Email Accounts etc.)
Service Providers	Organizations that provide critical services to the adversary (Internet Service Providers, Domain Registrars, WebMail Providers etc.)
Timestamp	The date and time of the event
Phase	The phase of intrusion (Cyber Kill Chain)
Result	Results of the adversary's actions (Success, Failure, Unknown) (Confidentiality, Integrity, Availability)
Direction	Adversary-to-Infrastructure, Infrastructure-to-Adversary, Infrastructure-to-Infrastructure Victim-to-Infrastructure, Infrastructure-to-Victim, Bidirectional, Unknown
Methodology	General classification of an intrusion (Phishing, DDoS, Breach, Port Scan etc.)
Resources	Quote: "Every intrusion event requires one or more external resources to be satisfied prior to success" (1. Software, 2. Knowledge, 3. Information, 4. Hardware, 5. Funds, 6. Facilities, 7. Access)

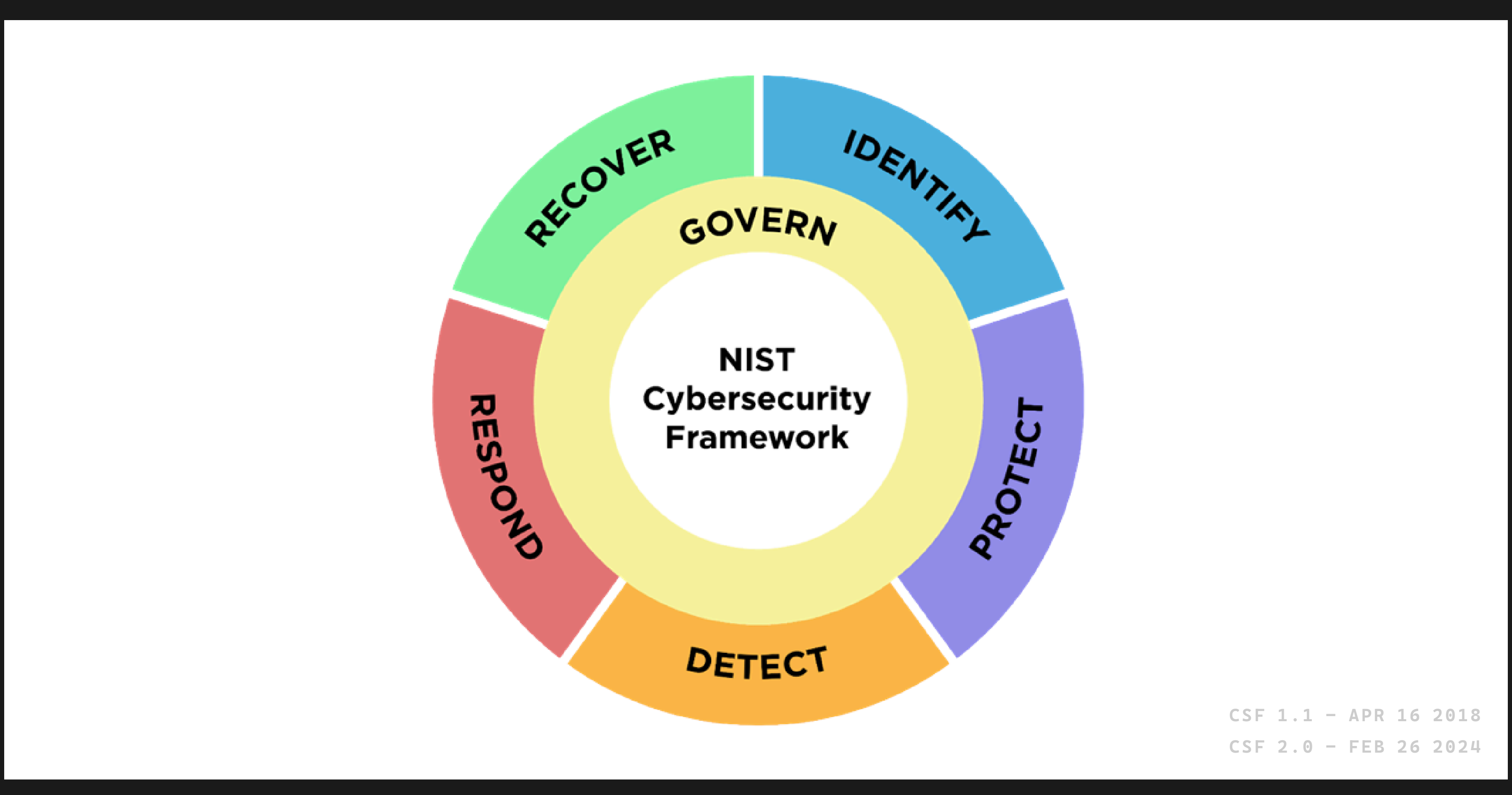
CYBER KILL CHAIN

01. Reconnaissance
02. Weaponization
03. Delivery
04. Exploitation
05. Installation
06. Command & Control
07. Actions on Objectives

UNIFIED KILL CHAIN

#	Attack Phase	Description
1	Reconnaissance	Researching, identifying and selecting targets using active or passive reconnaissance
2	Resource Development	Preparatory activities aimed at setting up the infrastructure required for the attack
3	Delivery	Techniques resulting in the transmission of a weaponized object to the targeted environment
4	Social Engineering	Techniques aimed at the manipulation of people to perform unsafe actions
5	Exploitation	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution
6	Persistence	Any access, action or change to a system that gives an attacker persistent presence on the system
7	Defense Evasion	Techniques an attacker may specifically use for evading detection or avoiding other defenses
8	Command & Control	Techniques that allow attackers to communicate with controlled systems within a target network
9	Pivoting	Tunneling traffic through a controlled system to other systems that are not directly accessible
10	Discovery	Techniques that allow an attacker to gain knowledge about a system and its network environment
11	Privilege Escalation	The result of techniques that provide an attacker with higher permissions on a system or network
12	Execution	Techniques that result in execution of attacker-controlled code on a local or remote system
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials
14	Lateral Movement	Techniques that enable an adversary to horizontally access and control other remote systems
15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal

NIST CYBERSECURITY FRAMEWORK (CSF 2.0)



NIST INCIDENT RESPONSE LIFE CYCLE