Here's a concise breakdown of **incident lifecycle frameworks**, with a focus on **NIST CSF** and the **NIST Incident Response Lifecycle**, based on the video:

**Incident Lifecycle Frameworks**

Frameworks provide structured support for incident response:

* Help standardize processes
* Improve consistency and effectiveness
* Can be adapted to fit an organization’s specific needs

**NIST Cybersecurity Framework (CSF)**

**Five core functions**:

1. **Identify** – Understand assets, risks, and vulnerabilities
2. **Protect** – Implement safeguards
3. **Detect** – Identify the occurrence of cybersecurity events
4. **Respond** – Take action on detected incidents
5. **Recover** – Restore capabilities and services

➡️ *This course focuses on the last three:* ***Detect****,* ***Respond****, and* ***Recover***.

**NIST Incident Response Lifecycle**

An expanded framework specific to incident response. **Not linear** — steps may **overlap**.

**Phases**:

1. **Preparation** – Set up policies, tools, and team readiness
2. **Detection and Analysis** – Identify and assess incidents
3. **Containment, Eradication, and Recovery** – Stop the threat, remove it, restore systems
4. **Post-Incident Activity** – Document and analyze the incident, improve processes

**Incident vs. Event**

* **Event**: Observable occurrence (e.g., failed login, password reset)
* **Incident**: An event that **violates security policy** or **jeopardizes CIA** (Confidentiality, Integrity, Availability)

✅ All incidents are events,  
❌ Not all events are incidents

**Incident Investigation**

Investigations focus on the **5 W's**:

* **Who** triggered it
* **What** happened
* **When** it happened
* **Where** it occurred
* **Why** it occurred

**Incident Handler’s Journal**

* A tool to document findings during incident response
* Helps analysts track evidence and progress
* Essential for final reporting and analysis