Preparation

Establishing an **incident response capability** should include the following actions:

- Creating an incident response **policy and plan**
- Developing **procedures** for performing incident handling and reporting
- Implementing **detective and preventative** security controls
- Selecting a **team structure** and **staffing model**
- **Establishing relationships and lines of communication** between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)

Georgia Tech

Detection & Analysis

- Events should be **analyzed** to determine if they are **true positives**
- Once determined to be a true positive, you must **determine if the event was malicious**
- If a true positive and malicious, then you **declare an incident**
- **Capture incident documentation** by archiving relevant digital evidence and noting all actions taken
- **Perform initial analysis** to make cursory determination of scope
- **Determine potential impact** of incident and prioritize response efforts
- If appropriate, begin executing **communications plan**

Georgia Tech

Containment, Eradication, and Recovery

Containment

- **Limiting the ability** of the attackers to do **further damage**
- **Containment strategies** should be determined for **various types of potential threats** (e.g. compromised accounts, ransomware, exploited webserver)
- What if you want to **allow the attacker to persist**?
- What **evidence needs to be collected** prior to containment?

Georgia Tech

Containment, Eradication, and Recovery

Eradication and Recovery

- **Removing the attackers** from your environment
- **Eradication activities** can include resetting user accounts, removing malicious files, and mitigating vulnerabilities
- **Recovery activities** including restoring systems to their production state
- **Restored systems should be patched** and/or otherwise secured to insure re-compromise doesn't occur

Georgia Tech