Incident Response Process

Georgia Tech

Incident Response Process

- Developing an incident response capability is a **critical step in the maturity of an organization's security program**.
- Having a **well-defined and practiced incident response program** allows the security team and organization's leadership to **effectively and efficiently handle** an incident.
- Several **regulations require** that an organization **maintain an incident response program.**

Georgia Tech

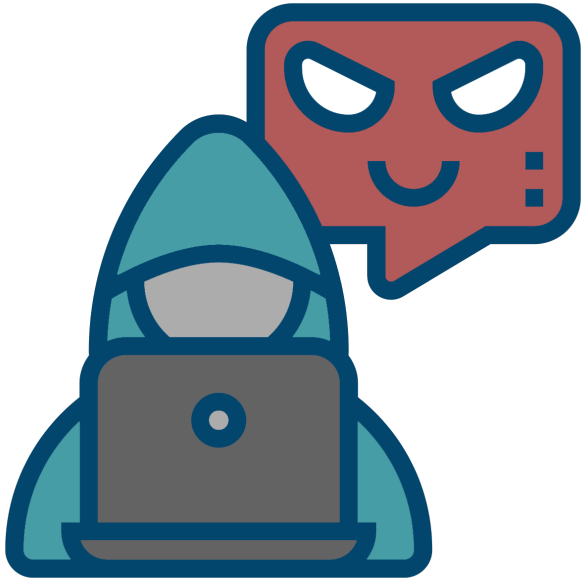
Incident Definition and Standards

Georgia Tech

- An **event** is **any observable occurrence in a system or network**. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- **Adverse events** are **events with a negative consequence**, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
- A **computer security incident** is **a violation or imminent threat of violation of computer security policies**, acceptable use policies, or standard security practices.

Events vs. Incidents

Georgia Tech



- An attacker **commands a botnet** to send high volumes of connection requests to a web server, **causing it to crash**.
- Users **are tricked into opening** a “quarterly report” sent via email that is actually **malware**; running the tool has infected their computers and established connections with an external host.
- An attacker **obtains sensitive data** and **threatens that the details will be released publicly** if the organization does not pay a designated sum of money.
- A user **provides or exposes sensitive information** to others through **peer-to-peer file sharing** services.

Examples of Incidents

Georgia Tech

- **NIST 800-61** (we will reference this standard for our discussions)

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- **SANS**

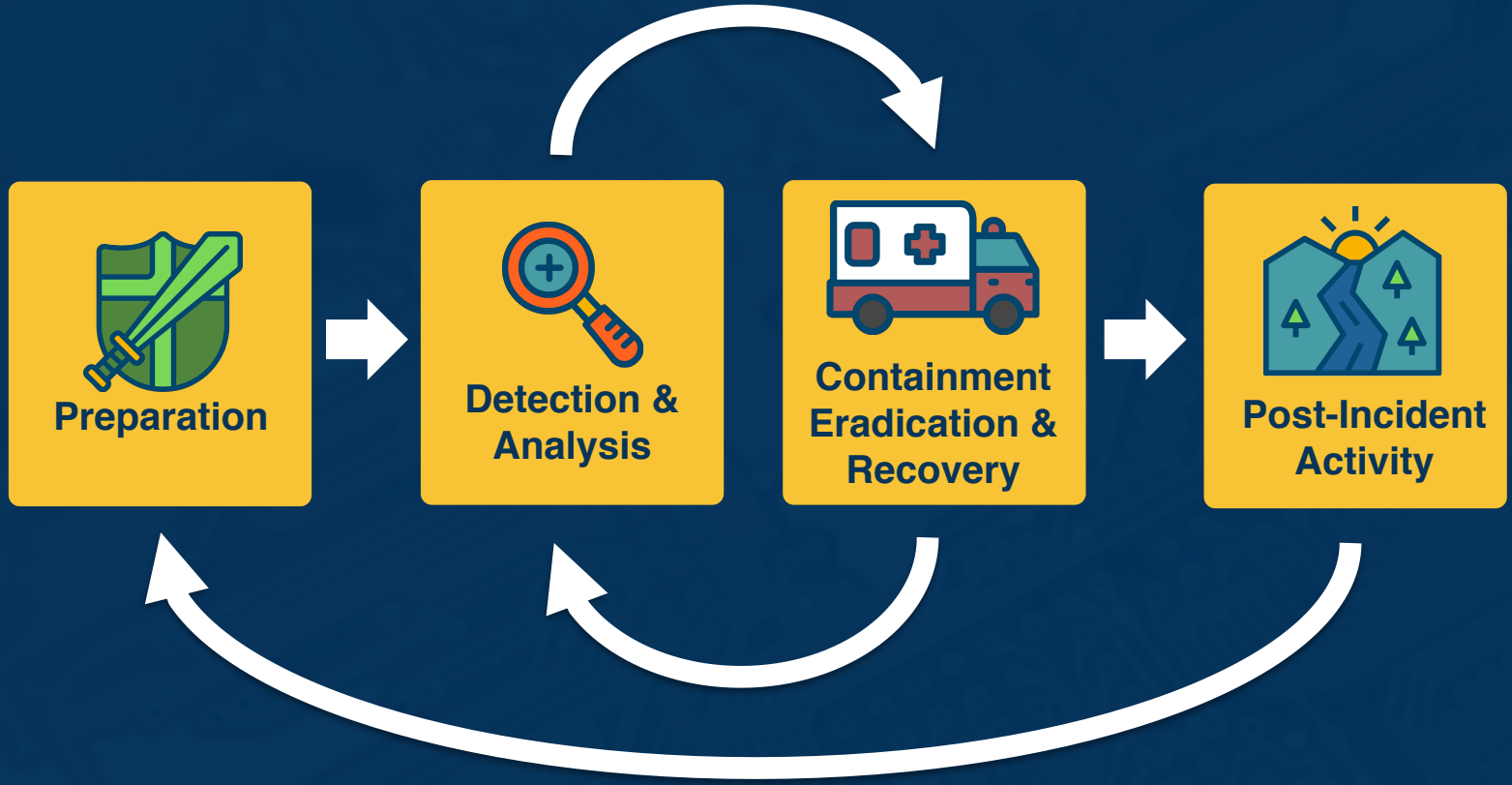
  https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

- **ISO/IEC 27035:2016**

  https://www.iso.org/standard/62071.html

Incident Response Lifecycle

Georgia Tech



Incident Response Life Cycle

Georgia Tech

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

Post Incident Activity

- **Lessons learned analysis**
  - Should include **analysis of what's needed** to mitigate **future risk** to systems and users
  - Should also include **analysis of what improvements** are needed for the incident response process
- **Evidence retention**

Georgia Tech