Cyber Incident Response Program

Question 1:

**What is the proper threat classification for a security breach that employs brute-force methods to compromise, degrade, or destroy systems?**

* Impersonation
* Attrition
* Improper Usage
* Loss of theft of Equipment

Question 2:

**What is *not* a major category of security event indicator?**

* Alerts
* Logs
* People
* Databases

Question 3:

**When does an organization assemble an incident response toolkit during the incident response process?**

* Preparation
* Detection and Analysis
* Containment, Eradication and recovery
* Post incident activity