Incident Containment and Eradication

Question 1:

**What is NOT part of the security incident validation effort?**

* Scanning
* Sanitization
* Patching
* Permissions

Question 2:

**What containment technique is the strongest possible response to an incident?**

* Segmentation
* Isolating affected systems
* Isolating the attacker
* Removal

Question 3:

**What sanitization technique uses only logical techniques to remove data?**

* Clear
* Degauss
* Destroy
* Purge