# Final Project - Handle an Incident

Submit Assignment

**Due** Nov 27 by 11:59pm **Points** 40 **Submitting** a file upload
**Available** after Oct 31 at 12am

**Company Name**: North American Lumber Coalition
**Description**: North American Lumber Coalition is a global company that specializes in the harvesting and processing of lumber. They are a sustainability first company that is very concerned with responsible forest management.

**Scenario**: You are part of a two person incident response team for the North American Lumber Coalition. The Cyber Security operations team has been alerted that the North American Lumber Coalition main website stopped working. The company has received a ransom from the bad guys for .3 bitcoin in order to have their website restored.

Your job is to use the available system logs and security events generated by your security systems in order to investigate this incident. If you find in your investigation that you need additional resources please send a message to the systems administration team (use Inbox in canvas to email the Teachers) with what you have discovered and what information you think you need.

Additionally, there is another team in security operations responsible for containment, eradication, and recovery. They are patiently awaiting your report so that they can make informed decisions about recovery, and ensure that NALC systems don't become immediately re-infected when brought back into production service. As you find actions the containment team should take, please send an message (also via canvas to the Teachers), on how they should contain the attack.

Updates to this assignment will occur throughout the time of the investigation as other details are found.

**Teams**: Work in teams of 2, identify teams and report to us by Thursday Nov. 2nd

**Resources**: Resources including details on the company systems, system logs, and security alerts are available in files located in Canvas.

**Deliverables**:
- Investigation log (refer to sample investigation log within Canvas)
- Incident report (will have a class lecture on what should be included in an incident report)
- Lessons learned report (will also cover in class lecture)