**Tentative Schedule:**

**Day #1 Friday 5:00 pm until 10:00 pm**

 -Intro-Welcome!!

- Resources

 -Attendance

 -Break into teams/groups (We will create groups when we meet on Friday)

 -Discuss project

***- Assessment – 5 points***

**Day #2 Saturday 8:00 am until 10:00 pm (lunch at 12 – 1 and dinner at 5:00 – 6:30 breaks)**

- Attendance/Assessment (assessments may be any time during the day)

- Break into teams/groups

- Work on project

-Teams will prepare to complete projects on Saturday and present projects on Sunday

***- Assessment – 5 points***

**Day #3 Sunday 8:00 am until 1:30 pm**

- Attendance/Discussion Board

- Team presentations

- ***Practical Connection Assignment after Presentations – 50 points (5% of your final grade). If you leave before this is assigned, you will NOT be able to take it later.***

- Student Sign-out

**Project Details:** You are part of an incident response team.   Each group has been assigned an incident from Appendix A in the NIST SP 800-61, Rev. 2 document. You need to respond to this incident by completing 4 deliverables:

1. **Incident Response Team Charter – 50 points.** Textbook has guidelines beginning on page 330. Minimum page length 3 double-spaced pages.

**2)** **Action Plan – 50 points.** Teams will respond to a specific incident. Groups have been assigned the following Incidents. Each Group will develop an Incident Response Plan with a **minimum** page length of 3 double-spaced pages addressing the following security incident. Be certain to include the questions in the scenario, as well as the General Questions in the Appendix:

* Group 1 – Scenario 2: Worm and Distributed Denial of Service (DDoS) Agent Infestation
* Group 2 – Scenario 3: Stolen Documents
* Group 3 – Scenario 4: Compromised Database Server
* Group 4 – Scenario 5: Unknown Exfiltration
* Group 5 – Scenario 6: Unauthorized Access to Payroll Records
* Group 6 – Scenario 8: Telecommuting Compromise
* Group 7 – Scenario 10: Peer-to-Peer File Sharing
* Group 8 – Scenario 11: Unknown Wireless Access Point
* Group 9 – Scenario 1: Domain Name System (DNS) Server Denial of Service (DoS)

**3) Incident Response Plan - 50 points.** A minimum of 5 pages Incident Response Plan will be developed that addresses IRT members and their tasks, and generic procedures for Incident Response (beginning page 342 - 347 and in the SP 800-61).

**4) Presentation – 50 points.** Each group will present a summary of their deliverables (all members must present). The presentation will consist of, at least, a title page with list of group members, and one or two slides for each section. Presentations should not be longer than 30 minutes per group, otherwise they will be marked down. **All team members MUST be present for ALL of the presentations, and not talking during the presentations - or their presentation will be marked down 20%.** There will be time after the presentations are completed for you to polish and submit your group papers.

The four parts are worth a total of 200 points and will based on the following:

* Meets Standard Criteria
* Completeness/content
* Logic of Processes and Actions (Thoroughness)
* Alignment of the Incident Response Plan and Action Plan in addressing guidelines in the text and NIST SP 800-61
* Completeness of the Topic
* Presentation Delivery

***The total number of points from the Residency (260) will be weighted as 60% of your final grade.***