|  |  |
| --- | --- |
| **Project 2** | *Incident Response* |
| **Brief description/purpose** | Teams of students will review an organization’s incident response policies, procedures, framework, and roles/responsibilities. They will then analyze the data to develop an incident response questionnaire and complete an investigation form as part of the incident response process. |
| **Courses to integrate** | NDG Security+ Lab 4, Incident Response Procedures |
| **Key terms/major topics** | * *Key terms:* Incident response, CIRT, Policies, Incident Response Policies, Incident Response Procedure, data breach * *Technical skills:* Analyze the incident response policy, procedure, and workflow process to develop an incident response questionnaire to cope with a serious data breach. * *Employability skills:*   1. **Teamwork.** Develop interview questions that determine if the incident should trigger a CIR level investigation.   2. **Problem solving.** Analyze the incident response policy, procedures, and workflow processes to identify questions that can be used to differentiate a CIR-level investigation versus a non-critical investigation.   3. **Written communications.** Write questions designed to gather relevant qualitative data associated with the incident. |
| **Equipment/materials** | * **Internet access** to:   1. Incident Handler’s Handbook: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>   2. REN-ISAC.net: <http://www.ren-isac.net/about/index.html>   3. PCI ComplianceGuide.org <https://www.pcicomplianceguide.org/pci-faqs-2/> * **Handouts:**   1. Student\_IncidentResponse   2. Data Breach Response Policy (document)   3. IT Security Information Breach Notification Procedure (document)   4. Memo from XYZ College (document)   5. Security Incident Response Questionnaire (document) * **Estimated time required:** 1–2 hours |