Syllabus

Course Number: MSIA 692
Course Title: Information Assurance Practicum 1

Course Description:

Students gain additional information assurance experience through detailed analysis of network datasets with known malware through the framework of a threat intelligence environment. This practicum, while not limited to our Cybersecurity specialty, focuses on the knowledge and skills acquired in the specialty.

Prerequisite Courses:

MSCC630, MSIA672, MSIA678, MSIA680, MSIA682, and minimum of ten degree program courses.

Course Overview

Key concepts to be covered in this course include:

- Overview of Cyber Intelligence
- Implementation of threat intelligence
- Threat actors and attack attribution
- Building a threat intelligence program
- Attacking the CyberKill Chain

Course Outcomes:

Upon completion of this course, learners should be able to:

- Understand and explain the concept of Cyber Intelligence
- Implement a threat intelligence program in an organization
- Identify threat actors and perform at least one method of threat attribution
- Analyze malware in network traffic to create attribution report

Course Materials:

N/A
Required Texts:


Required Resources:

N/A

Technology Tools:

N/A

Optional Materials:

(Syllabus Author: please use APA format and include ISBN numbers)

Pre-Assignment:

Online Format: N/A

Classroom-based Format: Sign on to D2L (Home Page) and become familiar with the course navigation of the Web Curriculum. This class is a hybrid class which will require students to participate live (either in class or via Zoom) during the schedule timeframe.

Pre-Assignment Due Dates:

Classroom-based Format: N/A
Online Format: N/A

Course Assignments and Activities:

(Syllabus Author: fill in Week, Topics, Readings, Activities, Assignments Due, and Points or % of Grade)

<table>
<thead>
<tr>
<th>Topics</th>
<th>Readings</th>
<th>Activities Assignments and Associated Points</th>
</tr>
</thead>
</table>
| 1 | Overview of Cyber Intelligence | Dietle – Chapter 1  
20 Questions for an Intrusion Analyst  
Threat Intelligence: Collecting, Analyzing and Evaluating  
13 Principles of Threat Intelligence Communication |
|   | Implementation Threat Intelligence | Dietle – Chapter 2  
The Pyramid of Pain  
15 Knowledge Areas of Skills for Cyber Analysts  
Cyber Intelligence Tradecraft | Case Study Assigned |
|---|----------------------------------|-------------------------------------------------|------------------|
| 3 | Threat Actors/Attribution        | The Diamond Model of Intrusion Analysis  
The Attribution Problem in Cyber Attacks.pdf |                  |
| 4 | Building Threat Intelligence Program | Dietle – Chapter 3  
Building Threat Hunting Strategies with the Diamond Model | Case Study Due |
| 5 | Attacking the Cyber Kill Chain   | Security Intelligence: Attacking the Cyber Kill Chain  
Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains  
Stallions – On TTPs | Overview of Data Analysis Due |
| 6 | Analyzing Data                  |                                                 |                  |
| 7 | Analyzing Data                  |                                                 |                  |
| 8 | Presentations                   | Presentation of final project and final paper due. | Maximum Points Possible: |

**Course Policies and Procedures:**

This class is a hybrid class – requiring participation during the scheduled classroom period (usually one night a week for 4 hours). This participation can be either in class or via the web. Students who are not able to participate during the class period must let the instructor know prior to the first night of the class.

**Student Evaluation Grid:**

*(Should not be part of template, but included in many syllabi)*

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Weighted Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Study</td>
<td>10 %</td>
</tr>
<tr>
<td>Participation</td>
<td>10 %</td>
</tr>
</tbody>
</table>
Overview | 5 %
---|---
Final Paper | 75 %
TOTAL | 100 %

**CC&IS Grading Scale**

<table>
<thead>
<tr>
<th>Letter Grade</th>
<th>Percentage</th>
<th>Grade Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>93 to 100</td>
<td>4.00</td>
</tr>
<tr>
<td>A–</td>
<td>90 to less than 93</td>
<td>3.67</td>
</tr>
<tr>
<td>B+</td>
<td>87 to less than 90</td>
<td>3.33</td>
</tr>
<tr>
<td>B</td>
<td>83 to less than 87</td>
<td>3.00</td>
</tr>
<tr>
<td>B–</td>
<td>80 to less than 83</td>
<td>2.67</td>
</tr>
<tr>
<td>C+</td>
<td>77 to less than 80</td>
<td>2.33</td>
</tr>
<tr>
<td>C</td>
<td>73 to less than 77</td>
<td>2.00</td>
</tr>
<tr>
<td>C–</td>
<td>70 to less than 73</td>
<td>1.67</td>
</tr>
<tr>
<td>D+</td>
<td>67 to less than 70</td>
<td>1.33</td>
</tr>
<tr>
<td>D</td>
<td>63 to less than 67</td>
<td>1.00</td>
</tr>
<tr>
<td>D–</td>
<td>60 to less than 63</td>
<td>.67</td>
</tr>
<tr>
<td>F</td>
<td>Less than 60</td>
<td>0</td>
</tr>
</tbody>
</table>

Additional information about grading can be found in the latest edition of the University Catalog, available at [http://www.regis.edu/Academics/Course%20Catalog.aspx](http://www.regis.edu/Academics/Course%20Catalog.aspx).

**CC&IS Policies and Procedures**

Each of the following CC&IS Policies & Procedures is incorporated here by reference. Students are expected to review this information each term, and agree to the policies and procedures as identified here and specified in the latest edition of the University Catalog, available at [http://www.regis.edu/Academics/Course%20Catalog.aspx](http://www.regis.edu/Academics/Course%20Catalog.aspx) or at the link provided.

- The CC&IS Academic Integrity Policy.
- The Student Honor Code and Student Standards of Conduct.
- Incomplete Grade Policy, Pass / No Pass Grades, Grade Reports.
- The Information Privacy policy and FERPA. For more information regarding FERPA, visit the [U.S. Department of Education](http://www.ed.gov).
- The HIPPA policies for protected health information. The complete Regis University HIPAA Privacy & Security policy can be found here: [http://www.regis.edu/About-Regis-University/University-Offices-and-Services/Auxiliary-Business/HIPAA.aspx](http://www.regis.edu/About-Regis-University/University-Offices-and-Services/Auxiliary-Business/HIPAA.aspx).

The CC&IS Policies & Procedures Syllabus Addendum summarizes additional important policies including, Diversity, Equal Access, Disability Services, and Attendance & Participation that apply to every course offered by the College of Computer & Information Sciences at Regis University. A copy of the CC&IS Policies & Procedures Syllabus Addendum can be found here: https://in2.regis.edu/sites/ccis/policies/Repository/CCIS%20Syllabus%20Addendum.docx.