Certificate in Cybersecurity

Program / Student Learning Outcomes: What Will I Learn?

Graduates of the Certificate in Cybersecurity will be able to:

1. Explain incident response handling, incident coordination, and ethical and legal issues.
2. Explain the process of building and coordinating a Security Incident Response team and a Product Security team.
3. Assess security risk and vulnerability of existing and proposed information systems.
4. Investigate cyber-crime and apply best practices for managing attack situations with a Security Incident Response team.
5. Explain how to build relationships with other Incident Response teams, organizations, and law enforcement to improve incident response effectiveness.

Assessment Methodology

Metrics, Assessments, and Levels of Achievement

The table below provides a brief overview of the measures selected to assess program outcomes for the Certificate in Cybersecurity (UG). Assessment of program/student outcomes consists of one direct measure, which is assessed in the capstone course. Benchmarks have been established to differentiate between three levels of program/student outcome achievement (exceeds expectations, meets expectations, and does not meet expectations). These three levels of achievement are color coded and used in the section below to indicate the level of achievement for each measure, for each learning outcome.

Metric Type	**Direct Measures**
Assessments	Capstone Portfolio: CYS460 Cybersecurity Investigations and Case Studies
Metrics	The percentage of students received a 2 (out of three) or higher on the learning statements and supporting evidence for the related student outcome.
Exceeds Expectations	≥ 85%

Meets Expectations	70 - 84%
Does Not Meet Expectations	< 70%

Note: Due to the small number of students who have taken the capstone course, data were aggregated from October 2014 to June 2016 to in order to have enough information to warrant a meaningful analysis.

Key: Result / N

Program/Student Outcome Achievement Results

July 2014 Term to June 2016 Term

Program / Student Learning Outcome 1

Explain incident response handling, incident coordination, and ethical and legal issues.

Direct Measure	
CYS460 (capstone) Cybersecurity Investigations and Case Studies	100%
	n = 10

Program / Student Learning Outcome 2

Explain the process of building and coordinating a Security Incident Response team and a Product Security team.

Direct Measure	
CYS460 (capstone) Cybersecurity Investigations and Case Studies	100%
	n = 10

Program / Student Learning Outcome 3

Assess security risk and vulnerability of existing and proposed information systems.

Direct Measure	
CYS460 (capstone) Cybersecurity Investigations and Case Studies	90%
	n = 10

Program / Student Learning Outcome 4

Investigate cyber crime and apply best practices for managing attack situations with a Security Incident Response team.

Direct Measure	
CYS460 (capstone) Cybersecurity Investigations and Case Studies	100%
	n = 10

Program / Student Learning Outcome 5

Explain how to build relationships with other Incident Response teams, organizations, and law enforcement to improve incident response effectiveness.

Direct Measure	
CYS460 (capstone) Cybersecurity Investigations and Case Studies	100%
	n = 10