MCM 217: DATA-DRIVEN CYBERSECURITY

In Workflow

1. CBA College Committee Chair (panggabean@csus.edu,joseph.taylor@csus.edu)
2. CBA Dean (ptong@csus.edu)
3. Academic Services (catalog@csus.edu)
4. Senate Curriculum Subcommittee Chair (curriculum@csus.edu)
5. Dean of Undergraduate and Graduate (Dean of Undergraduate and Graduate@csus.edu)
6. Catalog Editor (catalog@csus.edu)
7. Registrar's Office (k.mcfarland@csus.edu)
8. PeopleSoft (PeopleSoft@csus.edu)

Approval Path

1. 2026-06-02T19:09:25Z
   Tota Panggabean (panggabean): Approved for CBA College Committee Chair
2. 2026-06-23T20:26:47Z
   Pingsheng Tong (ptong): Approved for CBA Dean

New Course Proposal

Date Submitted: 2026-05-18T19:08:22Z

Viewing: MCM 217 : Data-Driven Cybersecurity

Last edit: 2026-05-18T19:08:21Z

Changes proposed by: Zahra Aivazpour (223025621)

Contact(s):

Name (First Last)	Email	Phone 999-999-9999
Ramakrishna Dantu	Ramakrishna.dantu@csus.edu	916-278-7058

Catalog Title:
Data-Driven Cybersecurity

Class Schedule Title:
Data-Driven Cybersecurity

Academic Group: (College)
CBA

Academic Organization: (Department)
Information Systems and Business Analytics

Will this course be offered through the College of Continuing Education (CCE)?
Yes

Please specify:
CCE Only

Catalog Year Effective:
Fall 2027 (2027/2028 Catalog)

Subject Area: (prefix)
MCM - Master of Cybersecurity Management

Catalog Number: (course number)
217

Course ID: (For administrative use only.)
TBD

Units:
3

Is the ONLY purpose of this change to update the term typically offered or the enforcement of existing requisites at registration?
No

In what term(s) will this course typically be offered?
Fall, Spring, Summer

Does this course require a room for its final exam?
Yes, final exam requires a room

Does this course replace an existing experimental course?
No

This course complies with the credit hour policy:
Yes

Justification for course proposal:
The proposed course, Data-Driven Cybersecurity, is an essential offering within the MS in Cybersecurity Management program under the College of Business. In today's enterprise environments, cybersecurity analysts are not limited by a lack of data but by the challenges of managing, processing, and extracting insights from vast and varied data sources. Traditional approaches to threat detection often fall short in handling the complexity and volume of modern network data. This course addresses that gap by equipping students with the skills to apply data analytics and visualization techniques to detect threats and inform cybersecurity decision-making.

Students will learn to transform raw cybersecurity data—from log files to proprietary binary formats—into meaningful intelligence using scripting tools, data science platforms, and modern machine learning libraries. The course emphasizes a practical, hands-on approach while also developing a deep understanding of how data-driven methods can support proactive and responsive cybersecurity strategies. By bridging cybersecurity and data science, this course empowers students to lead data-informed security initiatives and reinforces the program's mission of developing cybersecurity professionals capable of managing advanced analytical and operational challenges in the digital landscape.

Course Description: (Not to exceed 90 words and language should conform to catalog copy.)
This course equips students to address cybersecurity challenges using data analytics. With the overwhelming volume and variety of network data, analysts must transform diverse sources—like log files and binaries—into actionable insights. Students gain hands-on experience with scripting, visualization tools, and machine learning libraries to analyze and interpret cybersecurity data. Emphasizing data-driven decision-making over traditional methods, the course enables students to detect threats, assess risks, and strengthen security strategies using modern data science techniques.

Are one or more field trips required with this course?
No

Fee Course?
No

Is this course designated as Service Learning?
No

Is this course designated as Curricular Community Engaged Learning?
No

Does this course require safety training?
No

Does this course require personal protective equipment (PPE)?
No

Does this course have prerequisites?
Yes

Prerequisite:
Admission to the MS in Cybersecurity Management program

Prerequisites Enforced at Registration?
Yes

Does this course have corequisites?
No

Graded:
Letter

Approval required for enrollment?
No Approval Required

Course Component(s) and Classification(s):
Seminar

Seminar Classification
CS#05 - Seminar (K-factor=1 WTU per unit)
Seminar Units
3

Is this a paired course?
No

Is this course crosslisted?
No

Can this course be repeated for credit?
No

Can the course be taken for credit more than once during the same term?
No

Description of the Expected Learning Outcomes and Assessment Strategies:

List the Expected Learning Outcomes and their accompanying Assessment Strategies (e.g., portfolios, examinations, performances, pre-and post-tests, conferences with students, student papers). Click the plus sign to add a new row.

	Expected Learning Outcome	Assessment Strategies
1	LO1: Describe the structure, types, and significance of various cybersecurity data sources (e.g., logs, network flows, and packet captures) used in enterprise environments.	Quizzes, Exams, Homework Assignments, Lab Assignments
2	LO2: Identify and explain fundamental cybersecurity concepts, data analytics principles, and their intersection in modern security operations.	Quizzes, Exams, Homework Assignments, Lab Assignments
3	LO3: Apply data analytics techniques to analyze security datasets and detect potential threats and anomalies in various cybersecurity contexts.	Quizzes, Exams, Homework Assignments, Lab Assignments
4	LO4: Evaluate the effectiveness of data-driven cybersecurity strategies and tools (e.g., SIEMs, ML models) in detecting and responding to threats and make informed decisions about security strategies based on analytical evidence.	Quizzes, Exams, Homework Assignments, Lab Assignments
5	LO5: Analyze patterns, anomalies, and threats in large-scale network and log data.	Quizzes, Exams, Homework Assignments, Lab Assignments

Attach a list of the required/recommended course readings and activities:
MCM 217_Syllabus.docx

For whom is this course being developed?
Majors in the Dept

Is this course required in a degree program (major, minor, graduate degree, certificate?)
No

Does the proposed change or addition cause a significant increase in the use of College or University resources (lab room, computer)?

No

Will there be any departments affected by this proposed course?

Yes

Indicate which department(s) will be affected by the proposed course:

Department(s)
Computer Science

Attach evidence of consultation with the affected department

EMAIL-CSConsult.pdf

I/we as the author(s) of this course proposal agree to provide a new or updated accessibility checklist to the Dean's office prior to the semester when this course is taught utilizing the changes proposed here.

I/we agree

University Learning Goals

Graduate (Masters) Learning Goals:

Disciplinary knowledge
Communication
Critical thinking/analysis
Information literacy
Professionalism

Is this course required as part of a teaching credential program, a single subject, or multiple subject waiver program (e.g., Liberal Studies, Biology) or other school personnel preparation program (e.g., School of Nursing)?

No

Is this a Graduate Writing Intensive (GWI) course?

No

Key: 15339