California State University San Marcos • **COURSE CHANGE(S)** • FORM C-2

ORIGINATOR'S SECTION:		
1. College: ☐ CHABSS ☐ CoBA ☐ CoEHHS ☒ CSM	Desired Term and Year of Implementation (e.g., Fall 2008): Fall 2016.	
2. Current Course abbreviation and Number: MCS 611		

TYPE OF CHANGE(S). Check √ all that apply.

Course Number Change	☐	Delete Prerequisite	☐	Other Prerequisite Change	☐
Course Title Change	☒	Add Corequisite	☐	Grading Method Change	☐
Unit Value Change	☐	Delete Corequisite	☐	Mode of Instruction Change (C/S Number)	☐
Description Change	☐	Add Consent for Enrollment	☐	Consider for G.E. If yes, also fill out appropriate GE form.	☐
Add Prerequisite	☐	Delete Consent for Enrollment	☐	Cross-list	☐

Information in this section– both current and new – is required only for items checked (√) above.

CURRENT INFORMATION:	NEW INFORMATION:
	Course abbreviation and Number:
3. Title: Intrusion Detection and Investigation	Title: *(Titles using jargon, slang, copyrighted names, trade names, or any non-essential punctuation may not be used.)* Intrusion Detection and Incident Response
4. Abbreviated Title for Banner *(no more than 25 characters):*	Abbreviated Title for PeopleSoft: *(no more than 25 characters, including spaces)*
5. Number of Units:	Number of Units:
6. Catalog Description:	Catalog Description: *(Not to exceed 80 words; language should conform to catalog copy. Please consult the catalog for models of style and format; include all necessary information regarding consent for enrollment, pre- and/or corequisites, repeated enrollment, crosslisting, as detailed below. Such information does not count toward the 80-word limit.)*

7. Mode of Instruction* *(See pages 17-23 at http://www.calstate.edu/cim/data-elem-dic/APDB-Transaction-DED-SectionV.pdf for definitions of the Course Classification Numbers)*

Type of Instruction	Number of CrediUnits	Instructional Mode (Course Classification Number)
Lecture		
Activity		
Lab		

Type of Instruction	Number of Credit Units	Instructional Mode (Course Classification Number)
Lecture		
Activity		
Lab		

8. Grading Method:*	Grading Method:*
☐ Normal (N) *(Allows Letter Grade +/-, and Credit/No Credit)*	☐ Normal (N) *(Allows Letter Grade +/-, and Credit/No Credit)*
☐ Normal Plus Report-in-Progress (NP) *(Allows Letter Grade +/-, Credit/No Credit, and Report-in-Progress)*	☐ Normal Plus Report-in-Progress (NP) *(Allows Letter Grade +/-, Credit/No Credit, and Report-in-Progress)*
☐ Credit/No Credit Only (C)	☐ Credit/No Credit Only (C)
☐ Credit/No Credit or Report-in-Progress Only (CP))	☐ Credit/No Credit or Report-in-Progress Only (CP))

9. If the NP or CP grading system was selected, please explain the need for this grade option.

*If Originator is uncertain of this entry, please consult with Program Director/Chair.

CURRENT INFORMATION:	NEW INFORMATION:
10. Course Requires Consent for Enrollment? ☐ Yes ☐ No ☐ Faculty ☐ Credential Analyst ☐ Dean ☐ Program/Department/Director/Chair	**Course Requires Consent for Enrollment?** ☐ Yes ☐ No ☐ Faculty ☐ Credential Analyst ☐ Dean ☐ Program/Department/Director/Chair
11. Course Can be Taken for Credit More than Once? ☐Yes ☐ No If yes, how many times (including first offering)	**Course Can be Taken for Credit More than Once?** ☐Yes ☐ No If yes, how many times (including first offering)
12. Is Course Cross Listed: ☐ Yes ☐ No If yes, indicate which course	**Is Course Cross-listed?** ☐ Yes ☐ No If yes, indicate which course and check "yes" in item #17 below.
13. Prerequisite(s):	**Prerequisite(s):**
14. Corequisite(s):	**Corequisite(s):**
15. Documentation attached: ☐ Syllabus ☒ Detailed Course Outline	

PROGRAM DIRECTOR/CHAIR - COLLEGE CURRICULUM COMMITTEE SECTION:
(Mandatory information – all items in this section must be completed.)

16. Does this course fulfill a requirement for any major (i.e. core course or elective for a major, majors in other departments, minors in other departments? ☒ **Yes** ☐ **No**
If yes, please specify:
Master in Cybersecurity – a required course

17. Does this course change impact other discipline(s)? ***(If there is any uncertainty as to whether a particular discipline is affected, check "yes" and obtain signature.)*** Check "yes" if the course is cross-listed. ☐ **Yes** ☒ **No**
If yes, obtain signature(s). Any objections should be stated in writing and attached to this form.

_____ Discipline _____ Signature _____ Date _____Support _____Oppose

_____ Discipline _____ Signature _____ Date _____Support _____Oppose

18. Reason(s) for changing this course:
A more general term than Investigation should be used to describe the post-intrusion activity so avoid confusion. Incidence Response is what is usually used in the industry.

SIGNATURES : (COLLEGE LEVEL) :

Rika Yoshii 3-23-16
1. Originator (Please Print) Date

2. Program Director/Chair 5-3-16 Date

3. College Curriculum Committee 5/2/2016 Date

4. College Dean (or Designee) 5/3/16 Date

(UNIVERSITY LEVEL)

5. UCC Committee Chair Date

6. Vice President for Academic Affairs (or Designee) Date

7. President (or Designee) Date

RECEIVED
MAY 0 3 2016
BY:

Course Outline: MCS 6111ntrusion Detection and **Incidence Response** (4)

Course Description:
Focuses on investigating threats against computers and network systems. Covers principles and techniques of intrusion detection such as network traffic analysis, packet analysis, application protocol layer for common protocols and log analysis. Evaluates the use of intrusion detection tools and services.

Topics include: intrusion detection such as network traffic analysis, packet analysis, application protocol layer for common protocols (HTIP, SMTP, DNS, etc) and log analysis. We will review and use typical open source intrusion detection tools such as Snort, Wireshark, tcpdump, etc. We will also review the function and implementation of proprietary Intrusion Detection applications and services. **Emphasis is placed on investigation, analysis and outcome reports.**

Prerequisite:
All four MCS 500 level courses.

3 unit lecture and 1unit Jab

Materials: *Applied Network Security Monitoring: Collection, Detection, ond Analysis, Chris Sanders and Jason Smith, Syngress; 1st edition {ISBN* 978-0124172081)

Detailed Topics:

- Network Architectures
- Review/Overview TCP/IP communications- encapsulation, routing, addressing
- 1Pv4 and 1Pv6 protocols, headers
- Network traffic collection
- Network Traffic Analysis
- Fragmentation, checksums
- layers 2 and 3 attacks (e.g. ARP spoofing, fragmentation attacks)
- Common analysis tools (e.g. wireshark, tcpdump}
- Analysis of flow data
- Application Protocols
- Common network application protocols (e.g. DNS, SMTP, HTIP}
- Common attacks, e.g. DDoS, TCP reset, MiM
- DNS and DNSSEC
- Intrusion Detection Tools and Products
- Open source tools (e.g. Snort, Bro)
- Commercial tools (e.g. Palo Alto, Cisco, Juniper)
- Attack Cases Studies
- Analysis of recent network attacks
- logging & log Analysis
- Fundamentals of log analysis
- Types, formats of typical log files
- Analysis tools and utilities, syslog servers, regular expressions
- Incident Handling and Reporting
- Fundamentals of incident response
- Evidence, analysis and incident report writing

In the laboratory sessions, students will learn to use the tools open source and/or vendor-provided tools.

Student learning outcomes:

Upon successful completion of the course, students will be able to:

1. Understand and identify threats against computers and network systems.
2. Analyze and evaluate network traffic, system logs.
3. Describe principles of incident response and incident management.
4. Develop incident reports and analysis presentations.

Typical Evaluation Components

Quizzes	25%
Hands-on Assignments	25%
In-class labs/participation	25%
Final Exam/Project	25%