CYBR-104 – Security Operations and Incident Response

Technology

Effective Term & Year: Fall 2027
Course Outline Review Date: 2032-03-01

Program Area: Information Technology

Description:

This course develops practical skills in security operations, threat detection, and incident response within modern organizational environments. Students use Security Information and Event Management (SIEM) systems, intrusion detection and prevention systems (IDPS), endpoint detection and response (EDR) tools, and network traffic analysis technologies to identify, investigate, and respond to cybersecurity incidents.

Through hands-on laboratory activities and real-world scenarios, students develop the technical and analytical skills required to support security operations centres and organizational incident response processes.

Program Information:

This course is required for the first year of the Cybersecurity Operations program.

Delivery Methods: Hybrid – On-campus (Face-to-Face) and Online

Credit Type: College of the Rockies Credits

Credits: 3

Instructional Activity and Hours:

Activity	Hours
Classroom, Directed Studies or Online Instruction	30
Seminar/Tutorials	

Laboratory/Studio	30
Practicum/Field Experience	
Co-op/Work Experience	
Other	
Total	60

Course Requisites:

Prior Learning and Recognition: Yes

Students are able to request formal recognition of their prior learning or experience outside the classroom. Challenge examination, portfolio-assisted assessment, work-based assessment or a combination of assessments that is appropriate to identify, assess, and recognize prior skills, competencies, and knowledge to achieve course credit. Tuition fees apply, refer to Policy 2.5.5 Prior Learning Assessment and Recognition (PLAR) or contact an education advisor for more information.

Course Transfer Credit:

For information about receiving transfer credit for courses taken at either British Columbia or Alberta institutions, please see https://www.bctransferguide.ca/ or https://transferalberta.alberta.ca . For more transfer credit information, please visit https://www.cotr.bc.ca/Transfer

All requests for course transfer credit from institutions in British Columbia or elsewhere should go to the College of the Rockies Enrollment Service office.

Textbook Resources:

Textbook selection varies by instructor and may change from year to year. At the Course Outline Effective Date the following textbooks were in use:

Please see the instructor's syllabus or check COTR's online text calculator https://textbook.cotr.bc.ca/ for a complete list of the currently required textbooks.

Learning Outcomes:

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

- use SIEM systems to support organizational security operations and compliance reporting;
- use Intrusion Detection and Prevention Systems (IDPS) to support incident response and apply threat hunting techniques;
- apply endpoint detection and response (EDR) techniques to monitor, analyze, and respond to security threats in real time;
- analyze and interpret network traffic using appropriate tools and integrate findings into incident response workflows;
- conduct proactive threat hunting activities by applying structured methodologies to identify indicators of compromise and emerging threats within organizational environments; and
- document and communicate security incidents by producing structured incident reports that support organizational response, compliance requirements, and post-incident review.

Course Topics:

- SOC Operations and Analyst Roles
- Cyber Threats, Attack Methods, and IoCs
- Log Management and Centralized Logging
- SIEM Architecture and Use Case Development
- SIEM-Based Incident Detection and Alert Triage
- Intrusion Detection and Prevention Systems (IDPS)
- Endpoint Detection and Response (EDR)
- Network Traffic Analysis (NTA)
- Proactive Threat Hunting
- Incident Response and Post-Incident Reporting

See instructor's syllabus for the detailed outline of weekly readings, activities and assignments.

Evaluation and Assessments

Assessment Type: On-Campus (face-to-face) and Online, or Hybrid

Assessment Type	% of Total Grade
Assignments (x2)	40%
Midterm	20%
Progress Milestone	10%
Final Exam	30%
Total	100%

Grade Scheme

A+	A	A-	B+	B	B-	C+	C	C-	D	F

>=90	89-85	84-80	79-76	75-72	71-68	67-64	63-60	59-55	54-50	<50

Evaluation Notes: A grade of “D” grants credit, but may not be sufficient as a prerequisite for sequential courses.

Evaluation Notes Comments:

Please see the instructor’s syllabus for specific classroom policies related to this course, such as details of evaluation, penalties for late assignments and use of electronic aids.

Exam Attendance:

Students must attend all scheduled exams at the appointed time and place. Instructors may approve an alternate exam to accommodate an illness or personal crisis. Department heads will consider other written requests. Any student who misses a scheduled exam without prior approval will receive a “0” on the exam.

Academic Policies:

College of the Rockies policies related to courses can be found at https://cotr.bc.ca/about-us/college-policies/ and include the following:

- Policy 2.1.4 Course Audit
- Policy 2.4.1 Credential Framework
- Policy 2.4.3 Students with Documented Disabilities
- Policy 2.4.4 Student Rights, Responsibilities and Conduct
- Policy 2.4.8 Academic Performance
- Policy 2.4.9 Student Feedback and Concerns
- Policy 2.4.11 Storage of Academic Works
- Policy 2.5.3 Student Appeal
- Policy 2.5.5 Prior Learning Assessment and Recognition (PLAR)

Course Changes:

The College of the Rockies updates course outlines regularly to meet changing educational, employment and marketing needs. The instructor will notify students in writing of any updates to this outline during the semester. The instructor reserves the right to revise, add or delete material while meeting the learning outcomes of this course outline.