CIS*6570
Security Monitoring and Cyber Threat Hunting
Fall Semester

1 INSTRUCTOR

Instructor: Hassan Khan and Ali Dehghantanha
Office: REY 3319
Phone extension: 53138
E-mail: hkhan15@uoguelph.ca; adehghan@uoguelph.ca

2 AIMs & OBJECTIVES

2.1 Calendar Description
This course provides a comprehensive review of tools, techniques, and procedures for monitoring network events and assets to build a secure network architecture. It trains students in methods for hunting attackers that could bypass designed network defense mechanisms in an enterprise.

2.2 Course Description
This course provides a comprehensive review of tools, techniques, and procedures for monitoring network events and assets to build a secure network architecture. It trains students in methods for hunting attackers that could bypass designed network defense mechanisms in an enterprise.

2.3 Learning Outcomes
Upon successful completion of this course, students will have demonstrated the ability to:

1. Identify, interpret, and evaluate continuous monitoring and cyber threat hunting requirements of organizations of different sizes;

2. Examine deficiencies in existing network architectures to build a defensible architecture that supports continuous monitoring;
3. Leverage different machine learning and data mining techniques to build intelligent data-driven systems for active defense;
4. Integrate legal and ethical requirements and best practices in monitoring network activities; and
5. Work collaboratively in teams to conduct research and communicate rational and reasoned arguments using appropriate methods.

2.4 Instructor’s Role and Responsibility to Students

The role of the instructor is to deliver lectures, conduct labs, facilitate discussion, and provide feedback to students.

3 Teaching and Learning Activities

3.1 Timetable

Lectures: 3 hours per week

3.2 Course Topics and Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>Introduction, privacy and ethical issues in network monitoring and threat hunting</td>
</tr>
<tr>
<td>Weeks 2, 3</td>
<td>Setting up network monitoring and threat hunting infrastructure</td>
</tr>
<tr>
<td>Weeks 4, 5</td>
<td>Applied machine learning for cyber threat detection and analysis</td>
</tr>
<tr>
<td>Weeks 6, 7</td>
<td>Network attacks, attack tools and network monitoring</td>
</tr>
<tr>
<td>Weeks 8, 9</td>
<td>Proactive network threat hunting and monitoring</td>
</tr>
<tr>
<td>Weeks 10, 11</td>
<td>Network events and attack analysis</td>
</tr>
<tr>
<td>Week 12</td>
<td>Network vulnerability management and automated threat hunting</td>
</tr>
</tbody>
</table>

4 Learning Resources

4.1 Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*6570 CourseLink site. Students are responsible for checking the site regularly.
4.2 Required Resources

- Scott Roberts, Rebekah Brown (2017), Intelligence-Driven Incident Response Outwitting the Adversary

5 ASSESSMENT

5.1 Dates and Distribution

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Due Date</th>
<th>Weighting</th>
<th>Learning Outcome(s) Assessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment</td>
<td>TBD</td>
<td>50%</td>
<td>LO1, LO2, LO4, LO5</td>
</tr>
<tr>
<td></td>
<td>(before the 40th class day)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Practical Exam</td>
<td>TBD</td>
<td>50%</td>
<td>LO1, LO2, LO3, LO4</td>
</tr>
</tbody>
</table>

5.2 Assessment Descriptions

Assignment
Students will: analyse different monitoring solutions; define network monitoring and secure networking architectures for emerging cyber platforms; build an automated AI-based platform to hunt for attackers in those networks; and submit a professionally written, high-quality academic report. This is a group-based assignment (max 3-person in each group) that should be submitted electronically as advised by the instructor prior to the submission deadline. Submission deadline is at 23:59 on the due date. Detailed instruction on the content of the assignment will be distributed during the term.

Practical Exam
The practical exam will be conducted in the cybersecurity lab. The exam evaluates students’ capabilities in defining a proper architecture for monitoring of given assets, identification of security loopholes, and planning for hunting residual active adversaries in the network using artificial intelligence techniques. Students will document their results and compile a professionally written, high-quality penetration testing report.

5.3 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the
semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

**Passing grade:** In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

### 6 UNIVERSITY STATEMENTS

#### 6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

#### 6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

#### 6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-regchg.shtml

#### 6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

#### 6.5 Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.
More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6 Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University’s policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7 Recording of Materials

Presentations that are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

6.8 Resources

The Academic Calendars are the source of information about the University of Guelph’s procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs: https://www.uoguelph.ca/academics/calendars