
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

Incident Response/ Management

Dr. Sandra Scott-Hayward

CSC3064 Lecture 16

School of Electronics, Electrical Engineering and Computer Science

Session Overview

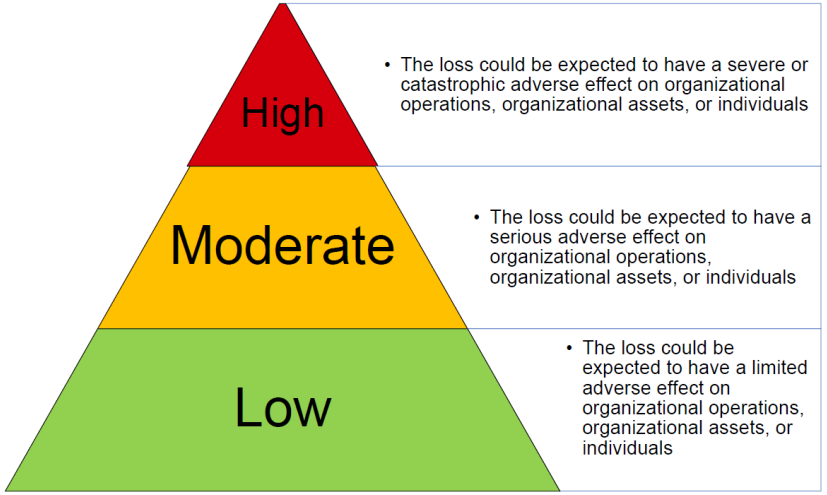
- Incident Response
- Network Forensics

References:
Davidoff, Sherri, and Jonathan Ham. *Network forensics: tracking hackers through cyberspace*. Vol. 2014. Upper Saddle River: Prentice hall, 2012.

QUEEN'S UNIVERSITY BELFAST

What do we already know?

Breach of Security – Levels of Impact



Security standards

ISO-27002 (http://www.27000.org/iso-27002.htm)

"Code of Practice for Information Security Management"

NIST Special Publications 800-14 (https://csrc.nist.gov/publications/detail/sp/800-14/final)

Control Objects for Information and Related Technology (COBIT)

"Framework for IT management"

Other Examples:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Sarbanes-Oxley (SOX) - Internal controls for financial reporting
- Health Insurance Portability and Accountability Act (HIPAA)

QUEEN'S UNIVERSITY BELFAST

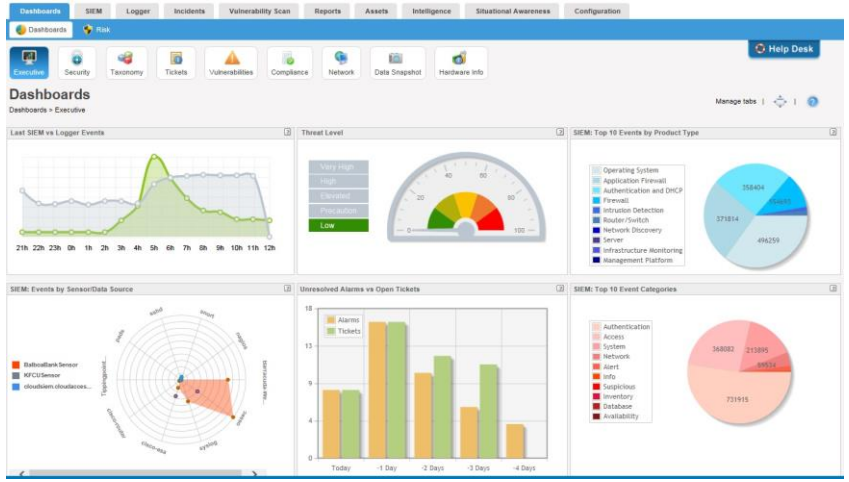
What do we already know?

Access control types

Control Type	*Directive*	*Deterrent*	*Preventative*	*Detective*	*Corrective*	*Recovery*	*Compensating*
Administrative	Policy	Policy	User registration procedure	Review violation reports	Termination	DR Plan	Supervision, Job Rotation, Logging
Logical	Config. Standards	Warning Banner	Password based login, IPS	Logs, IDS	Unplug, isolate, & terminate connection	Backups	CCTV, Keystroke Monitoring
Physical	Authorized personnel only signs, Traffic Lights	Beware of dog sign	Fence	Sentry, CCTV	Fire Extinguisher	Rebuild	Layered Defense

QUEEN'S UNIVERSITY BELFAST

Security Operations Centre



QUEEN'S UNIVERSITY BELFAST

Incident Response

Incident Response Lifecycle is described in the NIST Computer Security Incident Handling Guide (NIST 800-61rev2 08/2012).

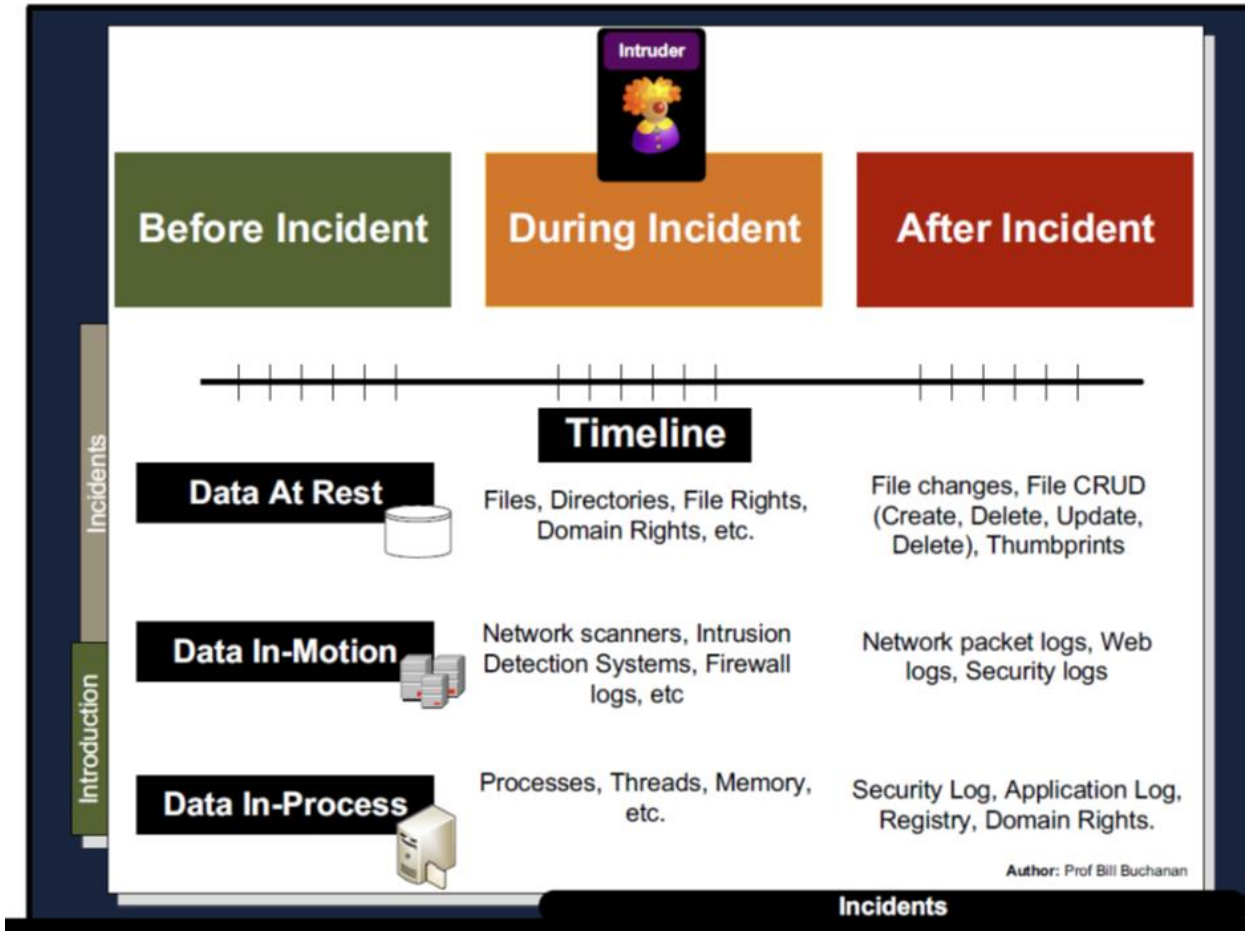
Other international standard frameworks for incident response include ISO/IEC 27035 and the ENISA (EU Agency for Network and Information Security) strategies for incident response and cyber crisis cooperation.

QUEEN'S UNIVERSITY BELFAST

NIST 800-14

Computer Security Incident Handling

- Provide ability to respond quickly and effectively
- Contain and repair damage from incidents
- Prevent future damage



QUEEN'S UNIVERSITY BELFAST

Incident Response

Preparation:

- Prepare the facilities (such as a central coordination room and storage facilities for collected evidence) and the communication mechanisms (cell phones, contact and on-call information, and others).
- Define the incident analysis hardware and software tools, such as protocol analyzers and forensics software.
- Define prevention procedures, such as patch management and user awareness and training methods.

Incident Response

Detection and Analysis:

- Analyze and implement tools for log and event correlation, identifying the business- and risk-relevant incidents

Containment, eradication, and recovery:

- Definition of tools to identify the attacker and context and time to perform this function (need for evidence preservation, time and resources to implement the strategy, sustainable service availability, and others).
- Steps to eradicate the threat and vulnerabilities, or at least mitigate them, and steps to recover operating systems, hardware components, and productive time.

QUEEN'S UNIVERSITY BELFAST

Incident Response

Post-incident activity:

- Documentation of sequence of events
- Root-cause analysis
- Handover to law enforcement? Prosecution?

QUEEN'S UNIVERSITY BELFAST

Computer Security Incident Response Team (CSIRT)

A service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.

- Internal e.g. bank, university etc.
- National e.g. U.K. NCSC
- Vendor Teams
- Incident Response Providers
- etc.

CSIRT (Computer Security Incident Response Team) - we will receive all incident reports and will provide advice and support on the cyber aspects to operators and Digital Service providers in the event of an incident. We will be responsible for the dissemination of appropriate risk and incident information to Competent Authorities and other relevant stakeholders.[1]

[1] https://www.ncsc.gov.uk/information/ncsc-support-nis-directive-implementation

QUEEN'S UNIVERSITY BELFAST

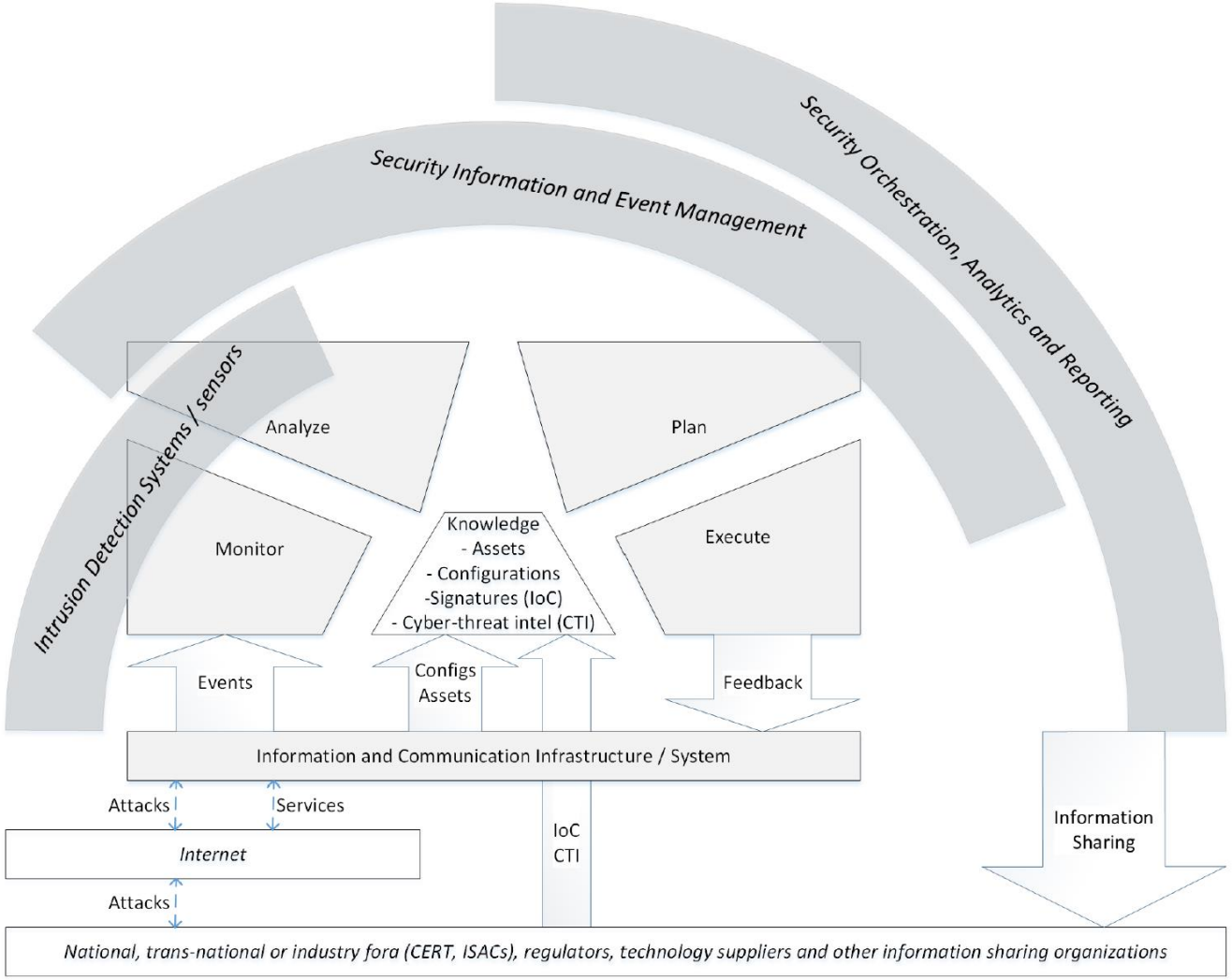
IRP Video

https://tinyurl.com/y59bxn6r

QOL->Resources->Quizzes->Quiz_incidentmanagement

QUEEN'S UNIVERSITY BELFAST

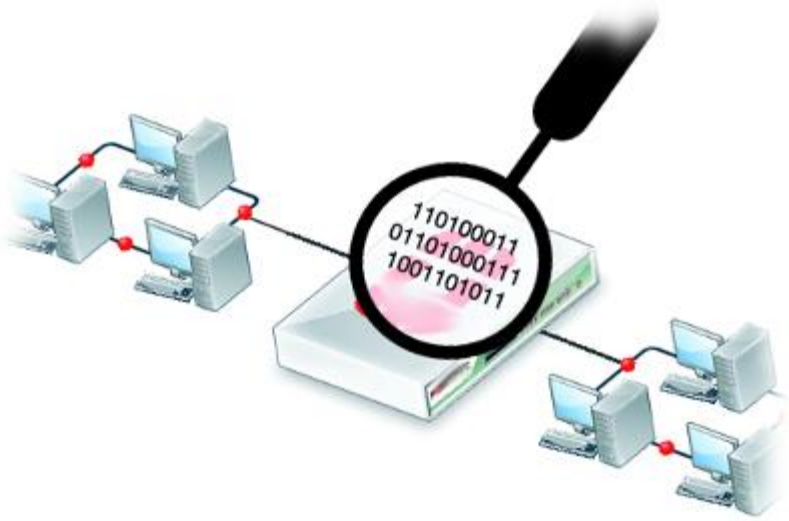
Security Operations and Incident Management workflow



QUEEN'S UNIVERSITY BELFAST

Network Forensics Investigative Methodology (OSCAR)

- Obtain information
- Strategize
- Collect evidence
- Analyze
- Report



QUEEN'S UNIVERSITY BELFAST

Obtain Information

The Incident
Description of what happened (as is currently known)
Date, time, and method of incident discovery
Persons involved
Systems and data involved
Actions taken since discovery
Summary of internal discussions
Incident manager and process
Legal issues
Time frame for investigation/recovery/resolution
Goals

The Environment
Business Model
Legal Issues
Network topology
Available sources of network evidence
Organizational structure
Incident response management process/procedures
Communications systems
Resources available (staff, equipment, funding, time)

QUEEN'S UNIVERSITY BELFAST

Strategize

- Accurately assess resources and plan investigation

Investigative Strategy
Understand the goals and time frame of the investigation
List your resources, including personnel, time, and equipment
Identify likely sources of evidence
For each source of evidence, estimate the value and cost of obtaining it
Prioritize your evidence acquisition
Plan the initial acquisition/analysis
Decide upon method and times of regular communication/updates
Keep in mind that after conducting your initial analysis, you may decide to go back and acquire more evidence. Forensics is an iterative process.

QUEEN'S UNIVERSITY BELFAST

Strategize

- Example of evidence prioritization (note: values will be unique to each investigation)

Source of Evidence	Likely Value	Effort	Volatility	Priority
Firewall logs	High	Medium	Low	2
Web proxy cache	High	Low	Medium	1
ARP tables	Low	Low	High	3

QUEEN'S UNIVERSITY BELFAST

Collect Evidence

- Document: Keep a careful log of all systems accessed and all actions taken during evidence collection. Store notes securely.
- Capture: Capture the evidence itself e.g. capturing packets and writing them to a hard drive, copying logs to hard drive, or imaging hard drives of web proxies or logging servers.
- Store/Transport: Ensure the evidence is stored securely and maintain the chain of custody.

QUEEN'S UNIVERSITY BELFAST

What is evidence?

What is evidence? The *Compact Oxford English Dictionary* defines “evidence” as:

evidence (noun)

1. information or signs indicating whether a belief or proposition is true or valid.
2. information used to establish facts in a legal investigation or admissible as testimony in a law court.

In the broadest sense, any observable and recordable event, or artefact of an event, that can be used to establish a true understanding of the cause and nature of an observed occurrence.

QUEEN'S UNIVERSITY BELFAST

Categories of Evidence

Type	Description	Example
“Real”	any physical, tangible object that played a relevant role in an event that is being adjudicated	E.g. Physical Hard Drive/USB device
Best	best evidence that can be produced in court. If the original evidence is not available, then alternate evidence of its contents may be admitted under the “best evidence rule.”	E.g. a file recovered from the computer hard drive, a bit-for-bit snapshot of a network transaction
Direct	testimony offered by a direct witness of the act or acts in question.	E.g. “I watched him crack passwords using John the Ripper and a password file he shouldn’t have.”
Circumstantial	evidence that does not directly support a specific conclusion. Rather, circumstantial evidence may be linked together with other evidence and used to deduce a conclusion.	E.g. A file containing password hashes on the defendant’s computer
Hearsay	the label given to testimony offered second-hand by someone who was not a direct witness of the act or acts in question	E.g. a text file containing a personal letter
Business Records	any documentation that an enterprise routinely generates and retains as a result of normal business processes, and that is deemed accurate enough to be used as a basis for managerial decisions	E.g. /var/log/messages

Network-based Digital Evidence

Digital evidence that is produced as a result of communications over a network.

Examples of “network-based digital evidence” can include:

- Emails and IM sessions
- Browser activity, including web-based email
- Routinely kept packet logs
- /var/log/messages

Challenges relating to Network Evidence

- Acquisition: can be difficult to locate specific evidence in a network environment (multiple sources or difficult to gain access)
- Content: only selected metadata available rather than complete records
- Storage: no persistent storage so data may not survive device reset
- Privacy: possible legal issues involving personal privacy
- Seizure: seizing a network device is disruptive
- Admissibility: limited precedent for admission of network-based digital evidence (as compared to filesystem-based evidence)

QUEEN'S UNIVERSITY BELFAST

Analyze

- Correlation
  - What data can be compiled, from which sources, and how can it be correlated.
- Timeline:
  - Build a timeline of activities – who did what, when and how
- Events of Interest:
  - Isolate events that are of greatest interest
- Corroboration:
  - Verify events by corroborating them through multiple sources
- Recovery of additional evidence:
  - Be prepared to repeat the process until the events of interest are well understood.
- Interpretation:
  - Develop a working theory of the case (assess meaning of evidence)

QUEEN'S UNIVERSITY BELFAST

Report

- Produce a report that is:
  - Understandable by nontechnical laypeople, such as:
    - Legal teams, managers, human resources personnel, judges, juries
  - Defensible in detail
  - Factual

QUEEN'S UNIVERSITY BELFAST

Summary

- Incident Response/Management
- Network Forensics
    - OSCAR Methodology
        - Obtain information
        - Strategize
        - Collect evidence
        - Analyze
        - Report

QUEEN'S UNIVERSITY BELFAST

Schedule Update

Original lecture schedule:

Week 1 (14): Introduction to Network Security	Week 2 (15): Network Security Architecture	Week 3 (16): Security of Internet Protocols	Week 4 (17): Tunneling and VPNs
Week 5 (18): AAA and Firewalls	Week 6 (19): Denial of Service	Week 7 (20): Intrusion Detection/ Protection Systems	Week 8 (21): Network Security Administration
Week 9 (22): Incident Mgmt./ Network Forensics	Week 10 (23): Cloud/Virtualization Security	Week 11 (24): Wireless/Mobile Network Security	Week 12 (25): Review/Q&A

QUEEN'S UNIVERSITY BELFAST

Schedule Update

Revised lecture schedule:

Week 1 (14): Introduction to Network Security	Week 2 (15): Network Security Architecture	Week 3 (16): Security of Internet Protocols	Week 4 (17): Security of Internet Protocols
Week 5 (18): Tunneling and VPNs	Week 6 (19): AAA and Firewalls	Week 7 (20): Intrusion Detection/ Protection Systems	Week 8 (21): Network Security Administration
Week 9 (22): Incident Mgmt./ Network Forensics	Week 10 (23) Denial of Service	Week 11 (24): Cloud/Virtualization Wireless/Mobile	Week 12 (25): Review/Q&A

QUEEN'S UNIVERSITY BELFAST

Schedule Update

Revised lecture schedule:

Week 10:	Denial of Service (2 lectures)
Week 11:	Cloud/Virtualization (2 lectures)
	Wireless/Mobile (1 lecture)
Week 12:	Revision (1 session)

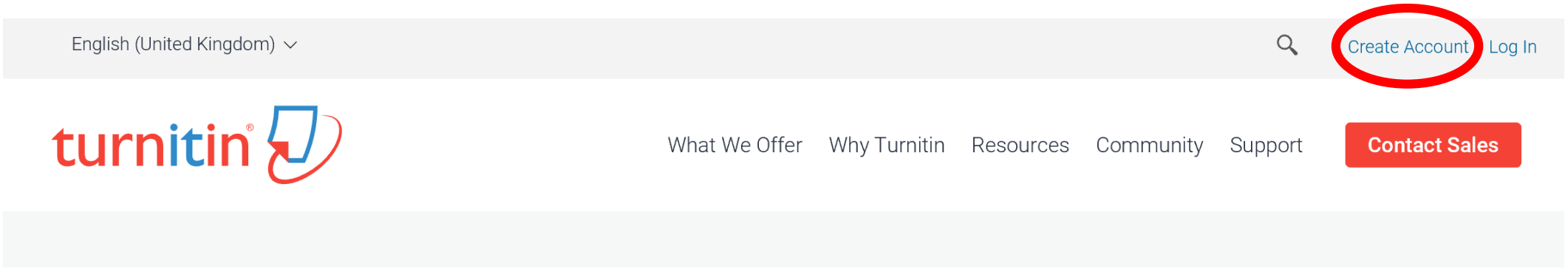
Class Test 2 Date: Monday, 13 May – 9.30am

QUEEN'S UNIVERSITY BELFAST

Coursework – TurnItIn Details (1)

One member of each group should submit a pdf version of your final report to Turnitin:

www.turnitinuk.com

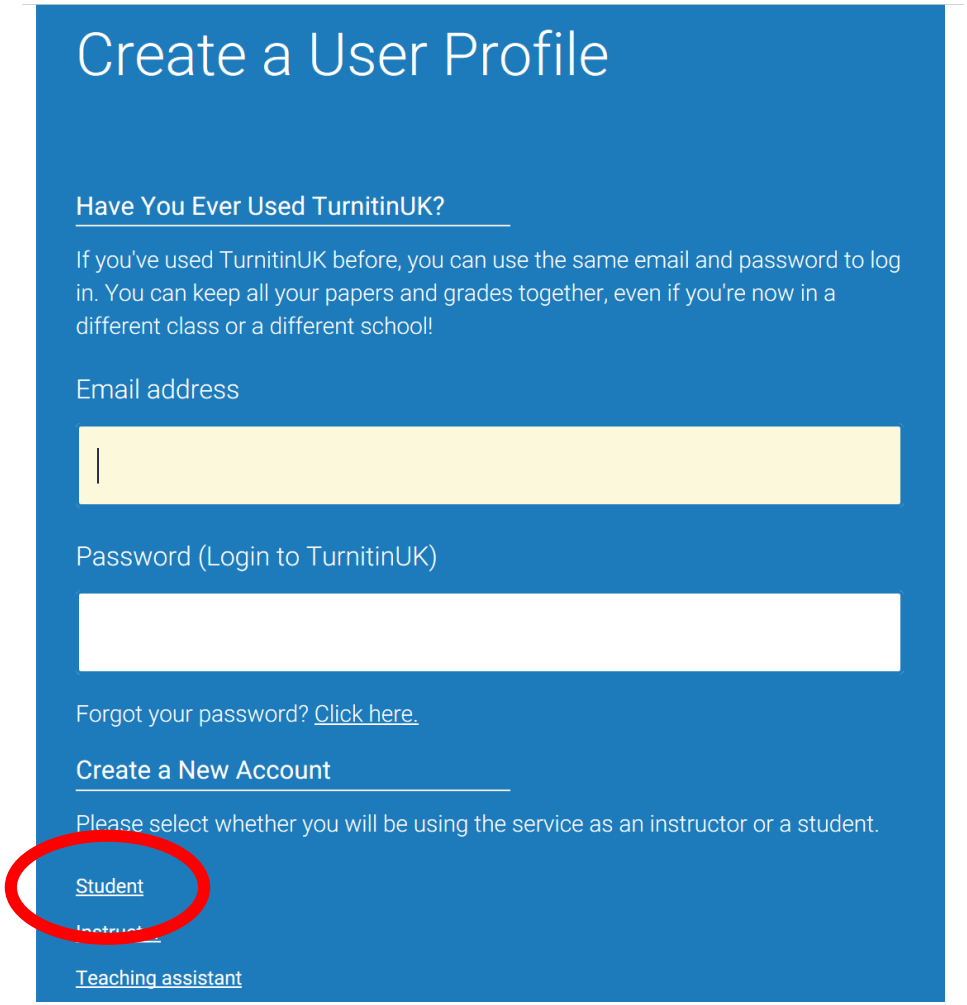


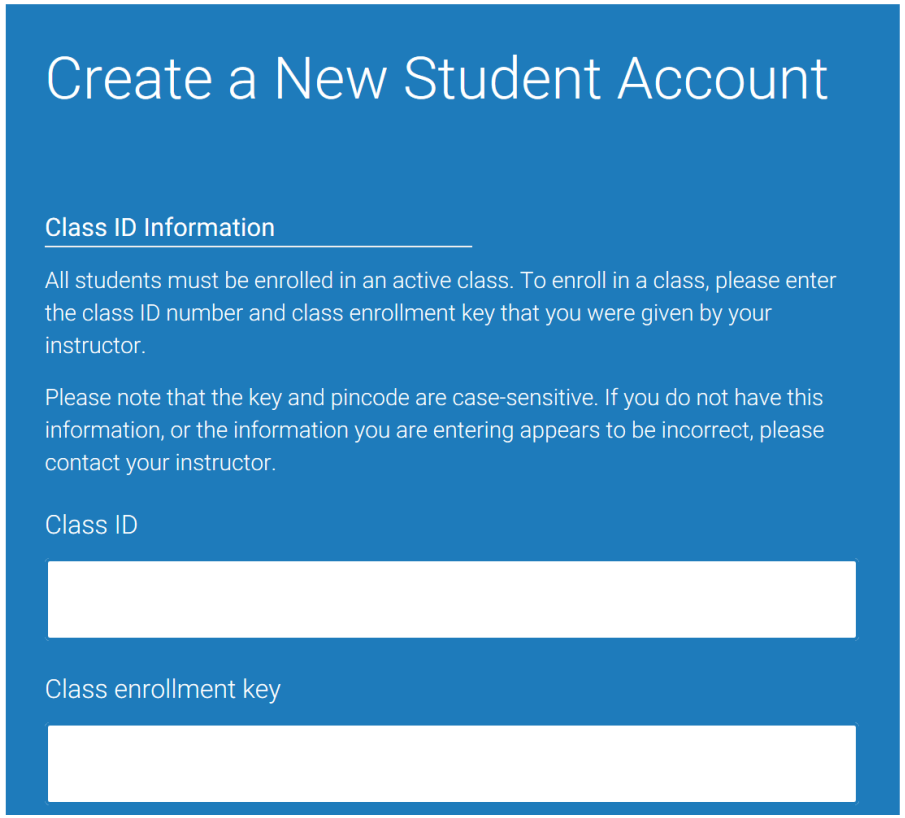
Class ID: 4114676

Enrolment Key: CSC3064_2019

QUEEN'S UNIVERSITY BELFAST

Coursework – TurnItIn Details (2)





Questions?

Next Session: Denial of Service

Thursday, 21 March 2019

QUEEN'S UNIVERSITY BELFAST