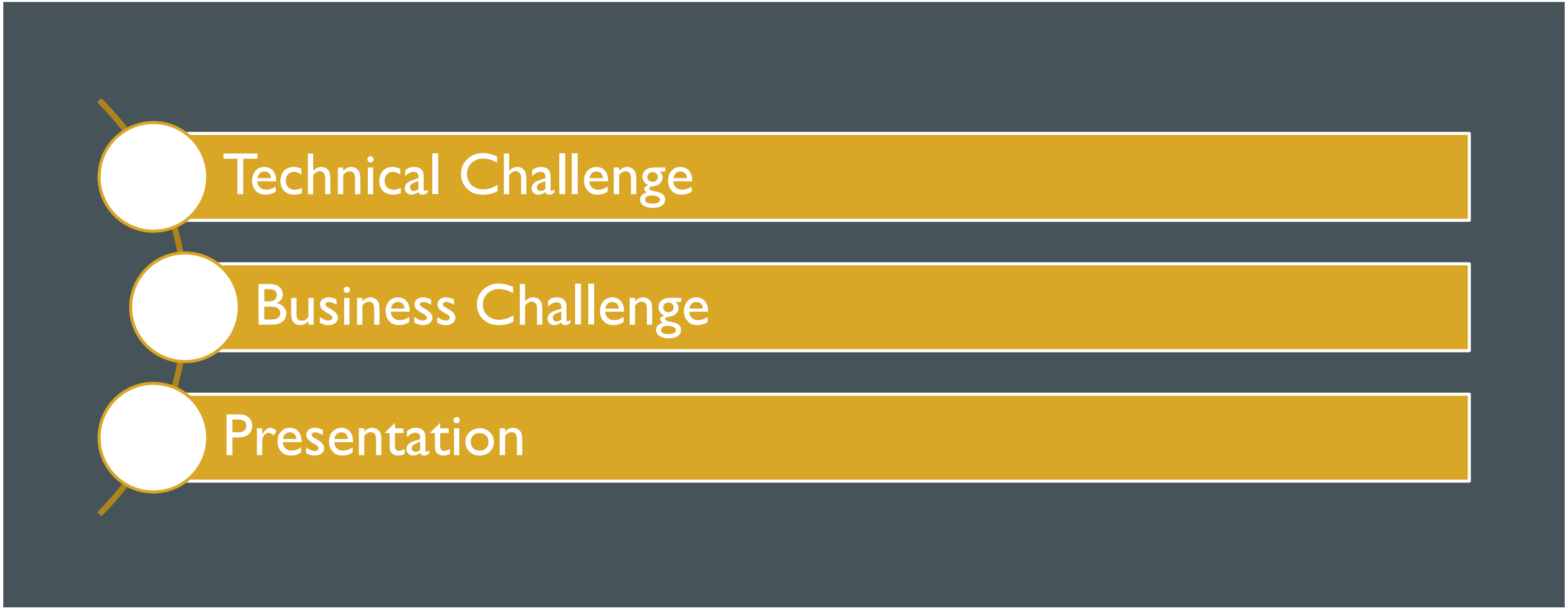
CANADIAN CYBER DEFENCE CHALLENGE (CCDC)

STUDENT PREPARATION PACKAGE

CYBER DEFENCE
CHALLENGE
EDUCATE | EMPOWER | ENGAGE

OUR MISSION

- Ensure that all Canadian students have the appropriate knowledge and skills required to make empowered decisions regarding the safe use of technology and this challenge is a key component of our strategy in realizing that vision.



OVERVIEW

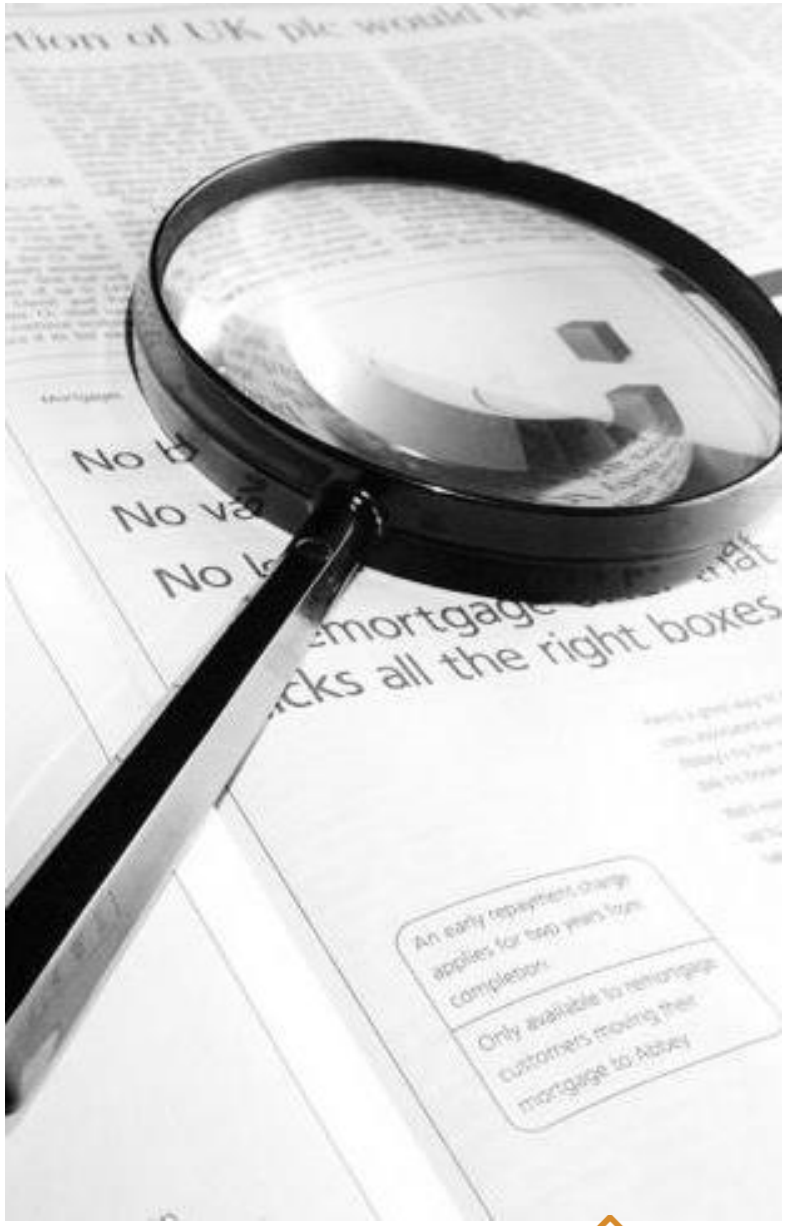
YOUR GOAL

- Throughout the day you will be bombarded with clues and facts by way of a business case scenario. Your job, as cyber security analysts is to try and pull these facts together to solve the business challenge.

CLUES

- Will come to you in three ways:
  - Solving cyber problems on your computer
  - Listening to insights from Cyber Defence Coach

- The cyber challenges will not necessarily come to you in the right order
  - Keep track of all your cyber forensics targets and discoveries
  - Utilize the Forensic Business Analysis sheet and the Briefing Report Outline on your table as guides to document your findings and prepare your Briefing Report – so you are not rushing when you have been notified of your briefing



SCORING (EXAMPLE)

Team Scores

2016 **2017**

Team Name	School Name	Sponsor	Score
Westgate Wings	Westgate Mennonite Collegiate	Portage Mutual Insurance	950
Dakota BetaGamma	Dakota	(ISC)² / (ISC)² Chapter Manitoba / Saskatchewan	890
JH Bruns BTY	JH Bruns	Portage Mutual Insurance	690
Sisler High Stack Ovf.	Sisler	ISACA Trust in, and value from, information systems Winnipeg Chapter	640
River East Kodiaks	River East		590
Bev Facey Sr.	Bev Facey Sr	Cisco	580

2017 CCDC Scoring Results

- Scoring will be awarded based on four areas of challenge:
  - Solving cyber problems on your computer
  - Listening to insights from your Cyber Defence Coach
  - Presenting to an executive panel.

AWARDING POINTS

- Technical points will be automatically scored and posted to the website
  - Scores will be shown at the competition event (See TECHNICAL CHALLENGE)
- Technical points that are tallied throughout the day account for two-thirds of the total points awarded
- The other third of your points are awarded through presentation to an executive panel (See PRESENTATION).

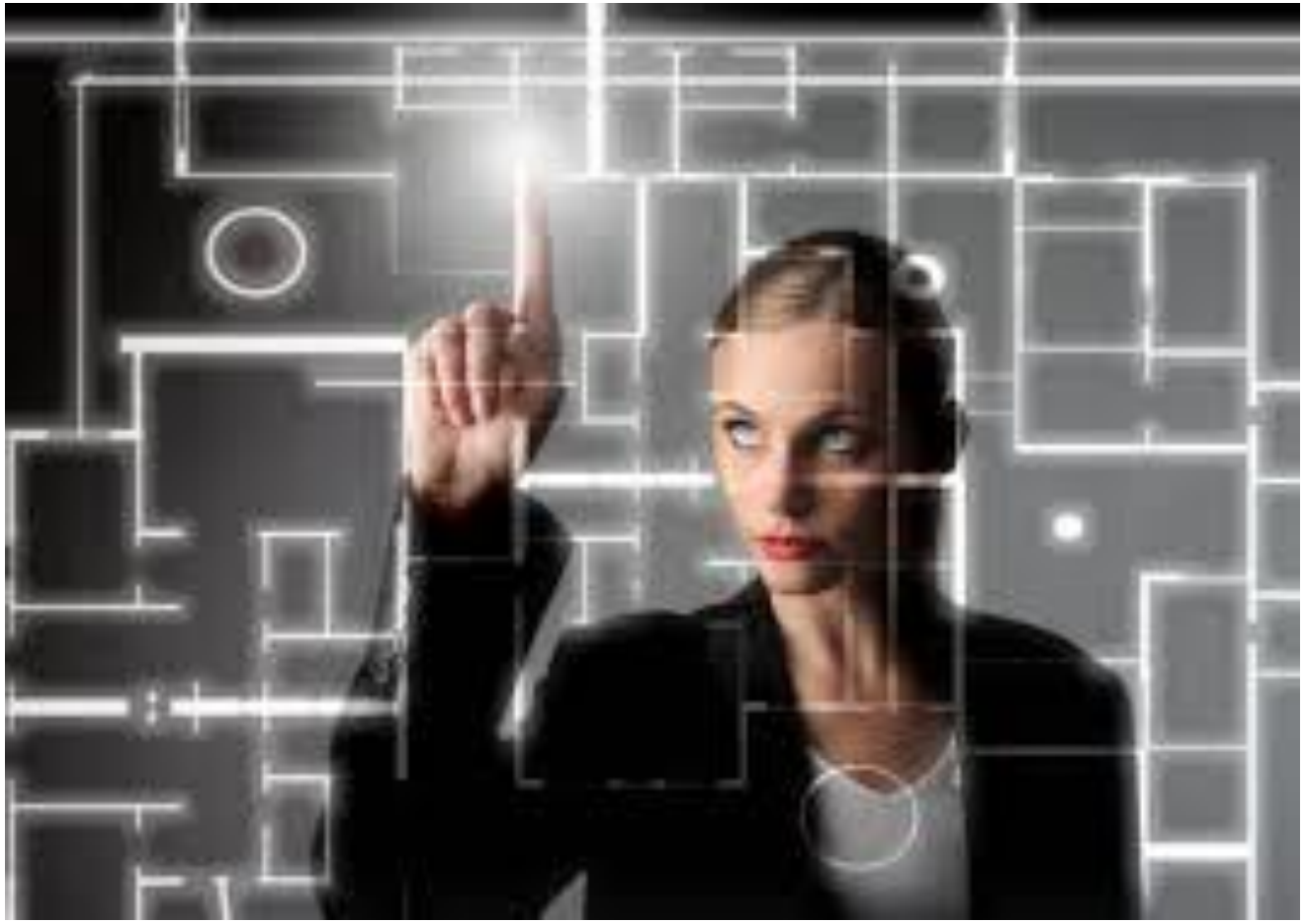
TECHNICAL CHALLENGE

- Windows, Linux, Cisco hardening
- Password cracking
- Cryptography
- System administration
- File system forensics
- Network forensics

TECHNICAL FORENSICS

- Close as many security holes as you can in the assets under your control
- If you encounter any flags hidden in puzzles or challenges (identified by "FLAG: sometext")
  - Enter that text string in the flag submission
- Public-facing services hosted on your assets (such as public web sites) must remain available to the public so that your business can keep running
  - Outages may result in negative points

BUSINESS CHALLENGE



- Business forensics analysis
- You will also learn **about the human side** of cyber defence and security
- Never forget that people are the ones who are ultimately responsible for the dysfunctions, flaws, errors, hacks, problems and insecurities we encounter each day.

BUSINESS FORENSICS

- While you are working through the technical cyber exercises, you will be guided by a Cyber Defence Coach that helps to explain motives and conspirators as part of the business challenge. scenario. Your job is to figure out the business challenge as you receive clues and insights from your digital discoveries:
  - The facts of the business situation will be brief a broken into a series of different scenarios which will be presented on the day of the event.
  - You will need to take notes. For this purpose we have a **Forensic Analysis and Briefing Report work sheet on your table. Keep track of clues that are provided by the different scenarios using the work sheet.** Someone should be in charge of jotting down what the team learns and drafting the briefing report.
  - Be careful not to share your discoveries with other tables. All information is worth points. No sense in giving away your discoveries to others, especially since you're in a competition.
  - You will be called upon to present your discoveries/findings about the narrative in the afternoon (see PRESENTATION).
  - Your Cyber Defence Coach will be available throughout the day to offer guidance (but not direct answers) if you need an extra hand (see Help and Aid - COACHES)

HELP AND AID

- Full access to internet throughout the competition
  - Google is your friend
- Game or environment specific questions, please call upon the coaches or volunteers
  - We're here to help
  - We choose to be here – because we take tremendous satisfaction in giving back to the future of our industry (i.e. YOU).

COACHES

- Throughout the day the teams will be guided by a Cyber Defence Coach – who is a senior consulting technical supervisor
- The Cyber Defence Coach has a wealth of knowledge and industry expertise that they're willing to share with you
  - Assist you and your team in working through the business and technical challenges – by challenging each of you and the way think and approach problems
  - Serve as an invaluable resource in helping you appreciate the cyber security industry and may even assist you in deciding your career path.

PRESENTATION

- You will be scored on your ability to:
  - Present the information
  - Identify the facts and analysis
  - Plan for your next steps.

BRIEFING EXECUTIVES

- 7-minute oral presentation/briefing that you will provide to a panel of executives
  - 15 minutes to prepare your findings and to organize your facts → Status update
  - Teams will be presented with a Briefing Report Outline at the competition to help organize their facts and present their findings
- The presentations will begin @ set time to be announced at the start of event.
- You will be in the middle of solving your challenges
  - You are not expected to have solved all of the challenges
  - You are expected to provide a status update of your work to that point in time – just like in the industry!
  - You will continue to work through your challenges after your presentation.

RULES OF ENGAGEMENT

- Do not hinder progress of other teams
- Do not attack CCDC infrastructure
  - Excess CPU, memory, bandwidth, etc
- Please follow the warnings
  - “Do not enter” & “Welcome”
- Any system you’re to analyze, explore freely
  - Please no DDoS attacks
- Abusing resources outside your network are forbidden
- Internet access should be used in accordance with your home school’s Acceptable Use Policy.
- This network environment is monitored. Conduct yourselves accordingly.

COMPLIANCE

- Violation of any rules of conduct as stated above or action in violation of ethical standards may result in disqualification.