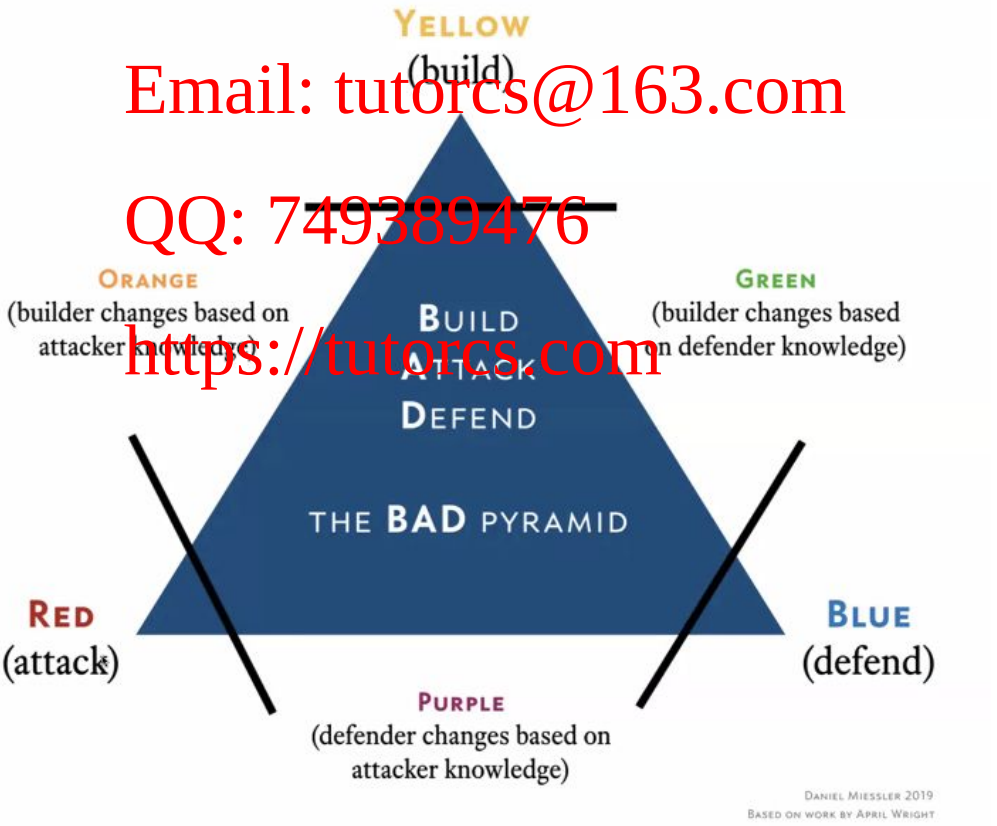
COMP 6448 - Week 7

Security Engineering Masterclass

Blue/Red Team

- A red team do ecks the blue team's processes.
- Red team: inte y dedicated to testing the effectiveness of a security program, emu niques of likely attackers in the most realistic way possible.
  - Testing properly.
- Blue team: Responsible for defending an organization's use of IS by continuously maintaining its security posture against the red team.
- Purple team: Not an actual team, but where the red and blue team interact as a team to integrate defensive tactics and controls from the blue team, with the threats and vulns found by the red team.



Yellow is almost the entire business. Anything that creates software/products etc. blue team is the SOC. Red team can be any team. Orange is reactive and green is proactive

Red Team vs Pen Testing:

- Red team has a granular focus. Specific attacks for an end goal.
- Pen testing is a much broader approach, trying to find any vulnerabilities.

Methodology:

- Scope:
  - Where can you access
  - What process and procedures do we want to test
  - Rules of engagement: what attacks can be carried out.
  - What i solutely not touch. E.g. payroll, AD
- Reconnaissan g
- Planning and r tacks
  - What s vant to accomplish?
  - ATT&C
- Launching the
  - What c
  - If it fails, what's the workaround? (This is why we plan)
- Documentation and reporting
  - Document the types and kinds of cyberattacks that were launched and their impacts. Financial liability? Data loss?
  - Discovery of vulns
  - If you deviated from a real attack, articulate this

Attack Emulations:

- Red teams should work based on their selected motive:
  - Organized crime:
    - More traditional threat vectors
    - Get tangible assets (usually to sell). Typically financial accounts.
    - Username/password leak is a key method.
  - Cyber espionage:
    - Don't want financial assets but rather information and learning more about the processes.
    - Attacks are slower, and very patient.
  - Cyber terrorism:
    - As much physical destruction as possible.
    - Includes, oil/gas, electricity, nuclear, plants, and water.
    - Red team would attack Industrial services.
  - Cyber activism:
    - Typically want to cause reputation damage

Outcome Benefits:

- Responses to attacks can be validated
- Create a security risk classification scheme
- Security weaknesses will be exposed and revealed.
- Maximising Security technology ROI.

Red team Plan

- **Game master:** Team lead that coordinates between attackers and defenders.
- **Managing Panic:** Panic can be useful and devastating.
- **Gamification:** Similar to CTFs, gamification prevents attacks from lasting months.
- **Red Team Cheating (Fourth Wall Sabotage):**
  - Allowed for time constraints
  - Come in the form of hints for us.

- Tips:
  - Positioning and alignment: Observe the ATT&CK framework when designing an exercise.
  - Keep a realistic effort for the given prep window.
  - Keep t[illegible]eadership should be the only ones in the know.
  - Follow[illegible] crisis go to waste. What could have prevented the attack.[illegible]xpected to do.
- What not to d[illegible]
  - Prove [illegible]her organization
  - Displa[illegible]
  - Prove [illegible]

- Define the stakeholders: Who has the most to lose?
  - Set up expectations.
  - Is the organization a willing participant? If not, how am I going to sell it to get them in.
  - Are the findings so predictable that we don't need a red team?
- Time estimations

- *Planning* (Weeks/Months): Planning the overall execution, filling in the gaps of this document.
- *Attack* (Minutes/Weeks): Onboarding of red team and active creation of the incident.
- *Response* (Hours/Weeks): If the incident is discovered, the length of the immediate response.
- *Tabletop* (Days / Weeks): If the incident is not discovered, the length of the forced response or tabletop.
- *Incident Response (Short Term)* (Days / Weeks): The time to remove red team access, plug any discovered vulnerability, elimination of the adversary.
- *Red Team Reveal* (Hours): Displaying the Red Team's actions to calibrate on IR realities.
- *Incident Response (Post Mortem)* (Hours / Days): Organization of the lessons learned and wide presentation.
- *Long Term Mitigation* (Weeks / Months): Completion of harder lessons learned, refactoring, and growth before you consider the next red team.

- Strategy:
  - Should the red team be expected?
  - Will there be an attack window?
  - Will there be cheating?
  - When do we call off the red team.
- Read team reveal:
  - Did the blue team understand what the red team was doing?
  - How good was IR?
  - How thorough was blue team investigation and containment.