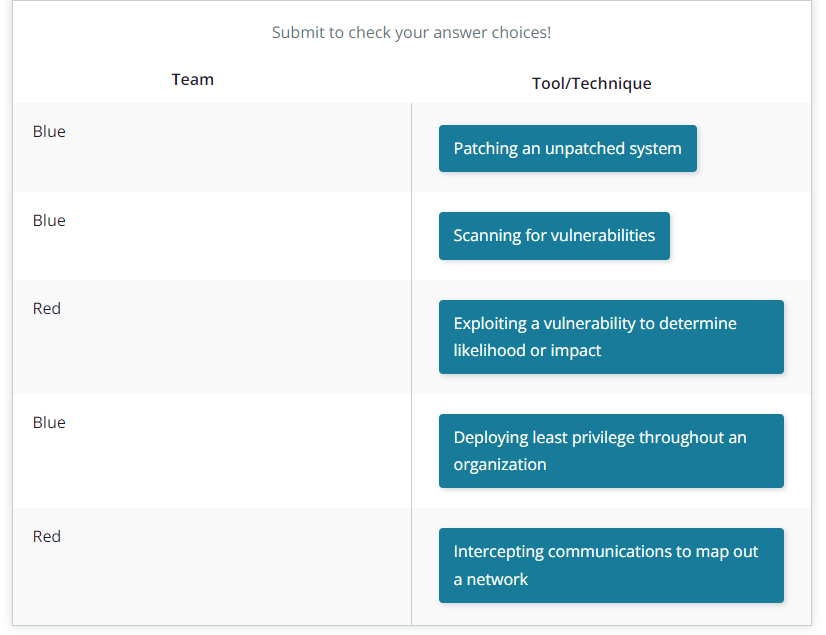
Risk = Threat + Vulnerability + impact

**Security Engineer:**

* Security Engineer thường là build system
* Security Analystic utilizing tool, proccess, system to protect organization from threat, preventing threats and detecting attack
* SIEM (Security Information and Event Management System)
  + SIEM with security engineer: get requirements, select tools, deploy, Integrate
  + SIEM with analyst engineer: provide input on requirements, utilize SIEM to analyze alert and logs, Tune SIEM
* Defense and ofense:
  + Defense: protect company by strengthening its defense. Establish security measure to protect the assets of an organization
  + With permission, approach security from the perspective of attacker (tiếp cận bảo mật công ty với quan điểm của kẻ tấn công để có thể ngăn chặn kịp thời các tình huống sẽ xảy ra)
  + Defense engineer:
    - Perform Vulnerability Scans
    - Analyze Logs
    - Deploy Security Tools (SIEM, Endpoint Protect)
    - Establish Security Process
  + Offensive Engineering
    - Penetration Testing
    - Scocial Engineers
    - Phising



Heartbleed: lỗ hỏng từ openSSL và thường là cần phải kiểm tra các request xác thực, thông thường thì server chỉ detect là đúng package 40Kb nhưng không xác thực rõ.

Ransomware: gửi một đoạn dữ liệu không sử dụng và mã hóa sau đó tống tiền để có thể có mã và mở khóa

Trong một tổ chức cần chú ý các vấn đề về:

* Từ phía người dùng cần tránh Phishing (mã độc thường lây lang thông qua click chuột vào các fake email), Ransomware (thường sẽ là bước tiếp theo sau khi click chuột vào fake email và bị đánh cắp thông tin), social engineer (sử dụng các phần mềm defense không legit và giả mạo)
* Từ phía application:
* Từ phía network/infrastructure: cần phải quan tâm đến vấn đề network và infra internal