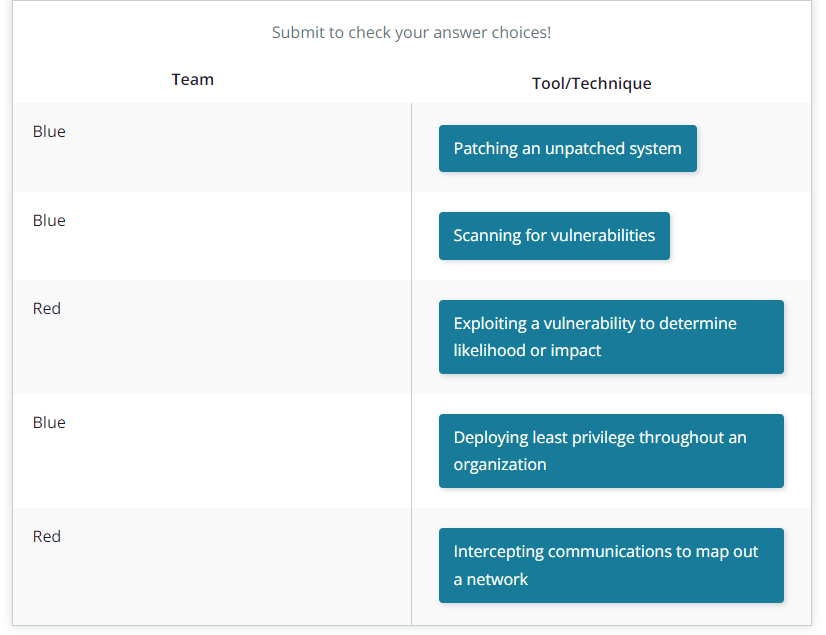
Risk = Threat + Vulnerability + impact

**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

**CIA Traid:**

* Confidentiality: Keeping data secret or private
* Integrity: Ensuring the legitimacy of data so it can be trusted
* Availability: Ensuring network, systems, and applications are up and running

**Authentication and Authorization**

***Authenticaiton*** is the act of confirming the identity of a user. Have 5 factors:

* Knowledge: (password, …)
* Possession: (Smart card, application security – Google authentication)
* Inherence: something just only you have (fingerprint, face recognition)
* Location: Geolocation, IP address
* Behavior:

***Authorization*** what an authenticated user can, and cannot do

Repudiation 🡪 to deny something (từ chối một gì đó)

Non-repudiation 🡪 to not allow someone to deny something

Non-repudiation = AuthN + AuthZ

**Principles of Secure Design**

* ***Minimize Attack Surface Area:*** is restricting the asccess of function within an application.
* ***Establish Secure Defaults:*** set to a high level of security out of the box, if user set lower then default, they must make a conscious decision
* ***Principle of Least Privilege:*** we must provide right resource, application for user, and after that we need to limit the permission of user in resource or application
* ***Fail Securely***: Errors shouldn’t affect unrelated systems, shouldn’t reveal sensitive data
* ***Don’t Trust Services***:don’t trust any incoming data to your system, should verify data that you are receiving will not have unintended consequences
* ***Separation of Duties***:separate the key that using to access resource or application, asset
* ***Avoid Security by Obscurity:***  about some hidden input, the developer neglected proper sucerity and then attacker can use that vulnerable.
* ***Fix Security Issues Correctly:*** Think of it as treating the disease and not the symptoms

**Security Strategies**:

* Policy: A formal written statement. States what can and cannot be done
* Standards: Mandatory set of actions or rules that support the policy
* Procedures: Step by step process for achieving a mandate
* Guidelines: Non mandatory set of best practices or recommendation

**PRACTICAL CRYPTOGRAPHY**

**Encrypting and Hashing**

***Encrypting:*** process of scrambling information so that it can only be read by someone with ability to decrypt the information.

* Modern Encryption:
  + Sysmmetric: 1 key use for encrypt and decrypt 🡪 private key (use case: less overheaad, data storage)
  + Asymmetric: use two keys, including: one for encrypting and another for decrypting 🡪 public key (use case: stronger form encryption, Digital Signatures, PKI)

**Signing, Certificates, and PKI**

***Signing***:

***Certificate:*** is a digital file that contains a public key along with other information that proves identity and ownership of that key

**Risk Evaluation**

***Vulnerability:*** weakness in system or software that can be exploited

***Threat:*** hypothetical (giả định) event wherein attacker can use or exploit

***Asset Valuation:*** Crucial (quan trọng) step, asset including data, system

Risk formula:

* Risk = Thread (Potential Event) x Vunerability (Weakness) x Impact
* Likelihood = Potential Event x Weakness
* Risk = likelihood (low) x Impact (high) 🡪 low risk
* **Impact -** Measures the consequence of a successful attack.

CVSS: Common Vulnerability Scoring System

**Threat Models**

* Threats and Vulnerabilities
* Evaluating Risk
* Mitigation Plan
* Prioritizing
* The famous framework of threat models is STRIDE
  + Spoofing: someone masquerade as a person or systems
  + Tampering: someone alters data
  + Repudiation: the ability to deny something
  + Information Disclosure: threat of leaking privileged or sensitive data
  + Denial of Service: aims to render a service or system unusable
  + Elevation of Privilege: Người dùng thực hiện các hành động không dành cho cấp độ quyền của họ

Another notes:

* XSS (Cross-site scripting): hacker chèn mã độc vào lỗ hỏng bảo mật web để có thể lấy tokens, session, cookies và các thông tin khác