devops security

Reduce Threat Modeling time in 90% | https://ds.kakugo.ch

What are we working on?

- **System context**
  - What's the system purpose?
  - What is the system made of? Which technologies?
  - With what other services does this system communicate?
  - What data is stored, processed or transferred in the documented interactions above?

- **Key Assets**
  - What must be protected in this system when it comes to Confidentiality, Integrity, Availability?

What can go wrong?

- **Threat agents**
  - Which attackers do you want to protect against?
    - Insiders
    - External attackers
    - Users with compromised devices
    - Governments

- **Threat Scenarios**
  - What are the *key threats* performed by *threat agents* that could lead to the compromise of the *key assets* considering the *system context*?
    - Start using STRIDE and/or Kill Chain to brainstorm
    - Consider previous security incidents as brainstorming sources
    - If you're fancy, you can use create a Knowledge Base (KB), but only after you master STRIDE

What are we going to do about it?

- **Impact Assessment**
  - What's the technical impact of exploiting the enumerated threats?
  - Don't use DREAD (not even MS uses it), keep it simple instead

- **Risk Assessment**
  - Classify threats in High, Medium or Low based on likelihood and business impact

- **Risk Treatment**
  - Should the identified risk be Avoided, Mitigated, Transferred or Accepted?

- **Derive Security Controls**
  - If the risk should be mitigated, what security principles and security controls can be applied?

- **Derive Security Detections & Responses**
  - What detection rules can be created to detect the materialisation of those threats?
  - What responses should we take to contain & recover from such incident?

- **Document**
  - Ensure a wiki page is created documenting every item
  - Create tasks to address the actions identified on *Risk Treatment*

Did we do a good job?

- **Compare the output of security tools**
  - Check SAST and DAST reports against the documented threat model

- **Compare the output of pentests**
  - Given the fact that pentests are manual, it's one of the best ways to challenge a threat model

- **Continuously Threat Model**
  - Threat model new features in your sprint
  - As threats evolve, redo the threat modeling at least 2x per year

- **Update your KB for future threat models**

- **Start/Stop/Continue**
  Ask participants of the threat modeling session what they should start/stop/continue doing