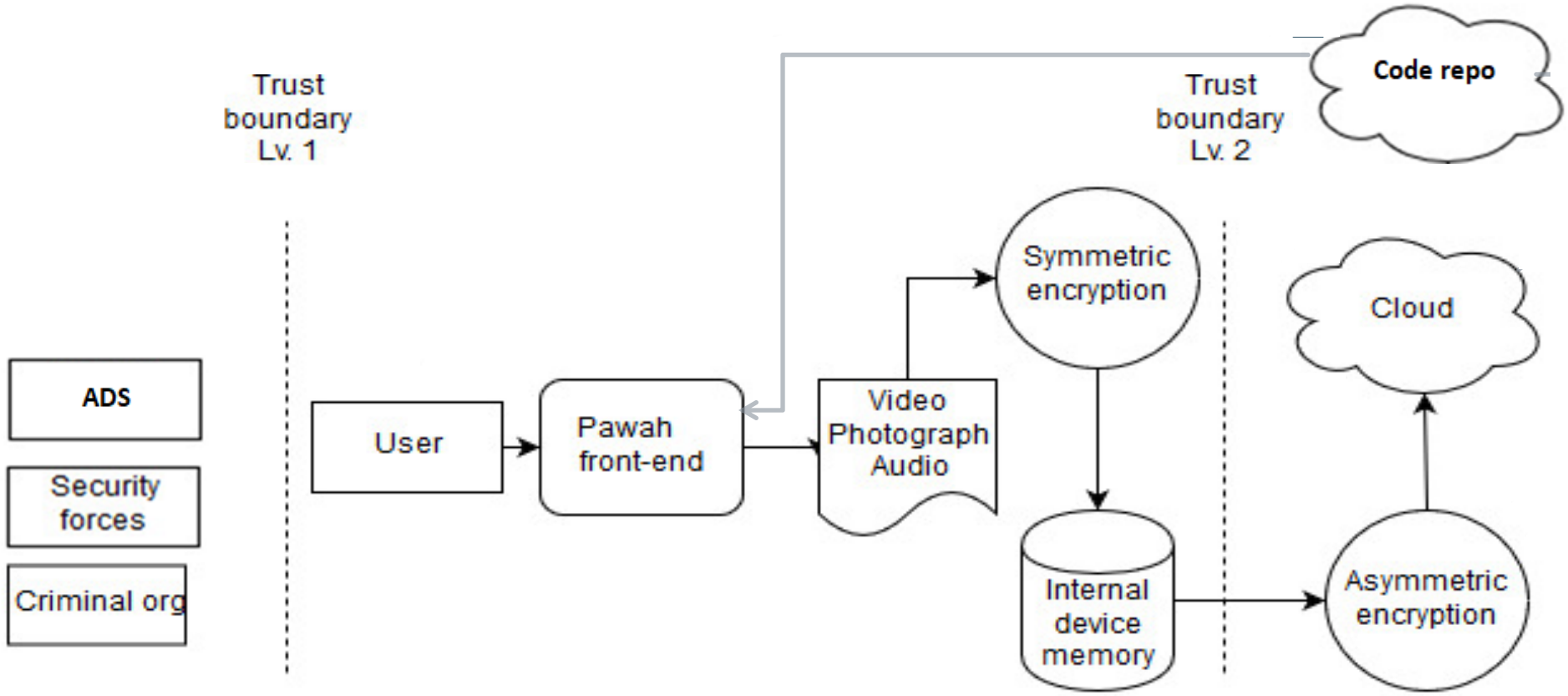
BUT WAIT, THERE'S MORE!



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

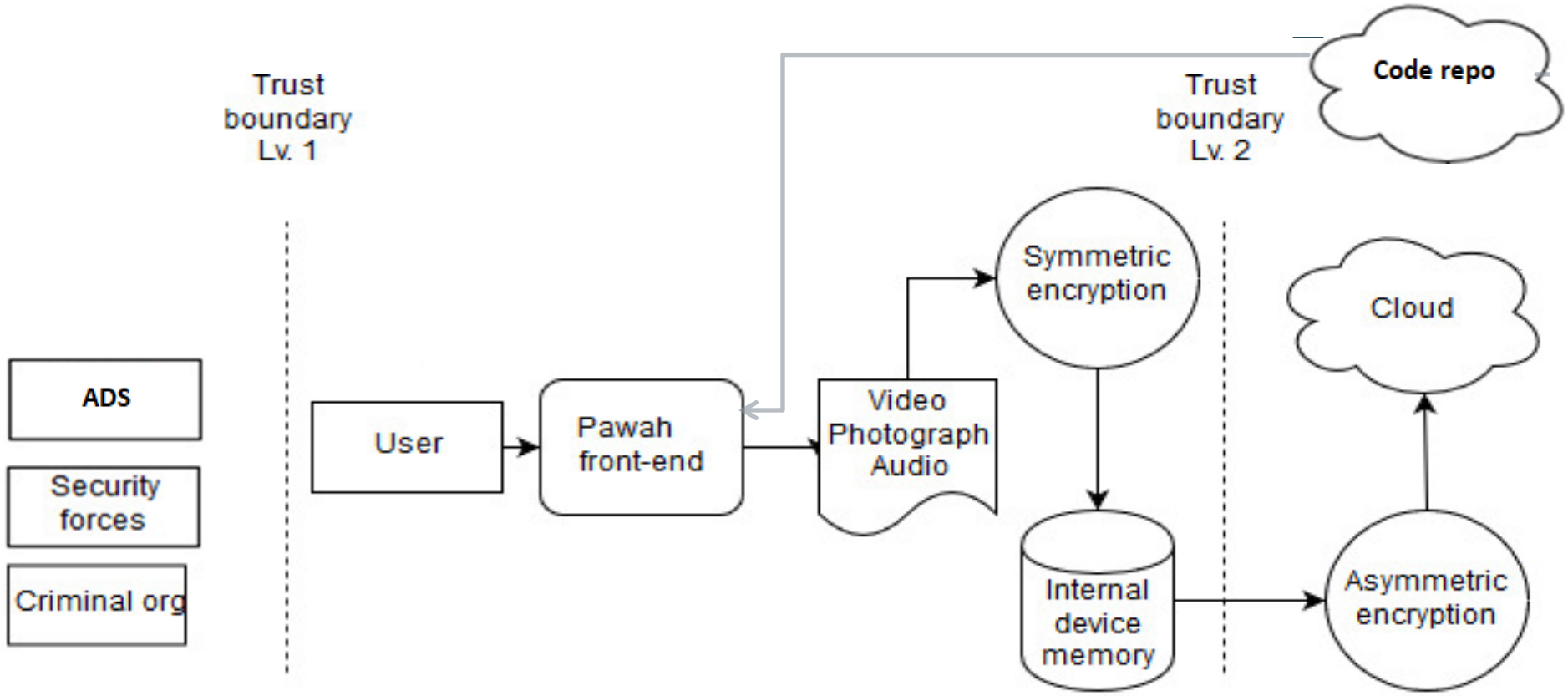
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

REMEMBER! BASIC THREAT MODELLING

- Hacked together from Microsoft's STRIDE threat modelling approach
- Three questions:
  - What are you building?
  - What can go wrong?
  - **What are you going to do about it?**



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

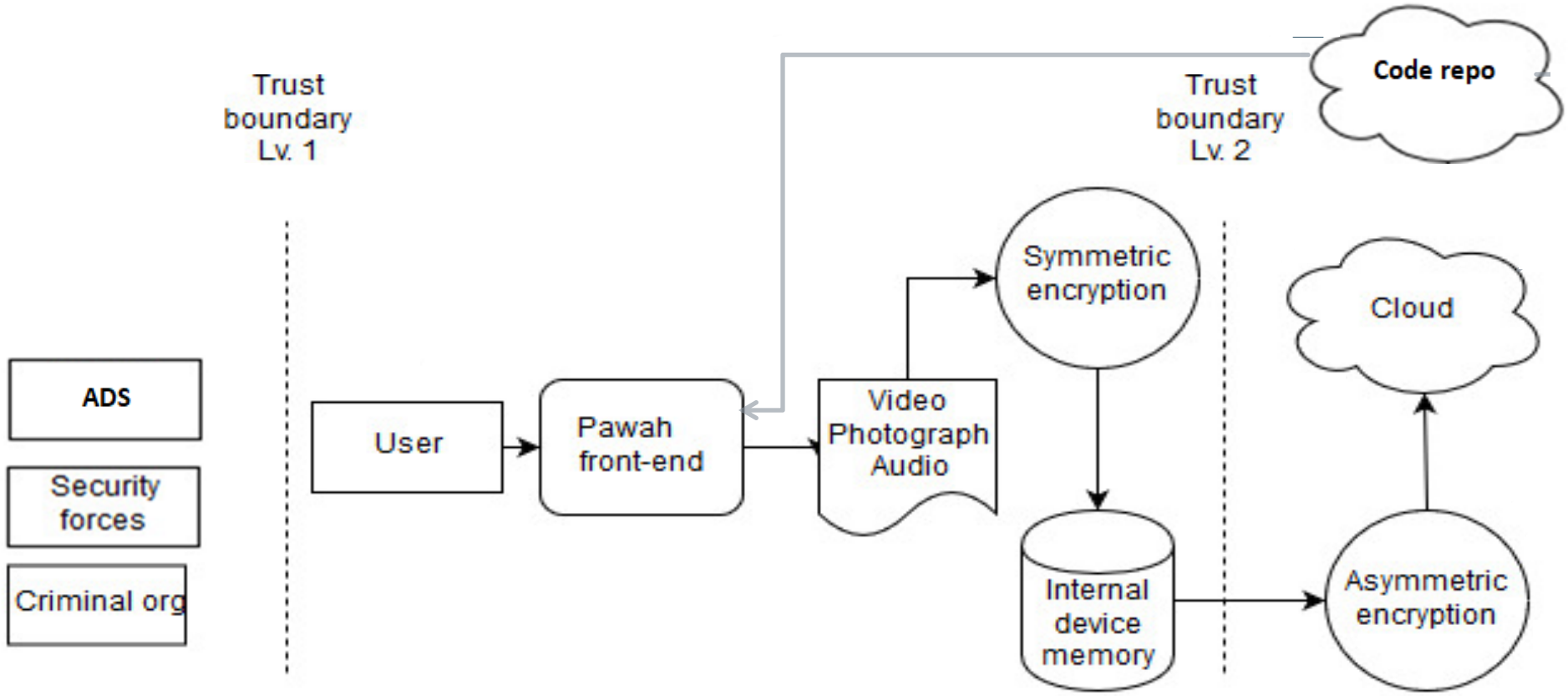
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – SPOOFING

- Someone impersonating a user to access data on phone, code repository, cloud storage
  - Credentials hashed with secure algorithm
  - Two factor authentication on code repository and cloud storage
  - IP whitelisting to access code repository and cloud storage if possible
  - Access Control Policy
    - Accounts are tied to identity
    - Permission only given if the user needs it
    - Accounts are revoked when user leaves
    - Accounts regularly audited
    - Someone is responsible for all this



Threats

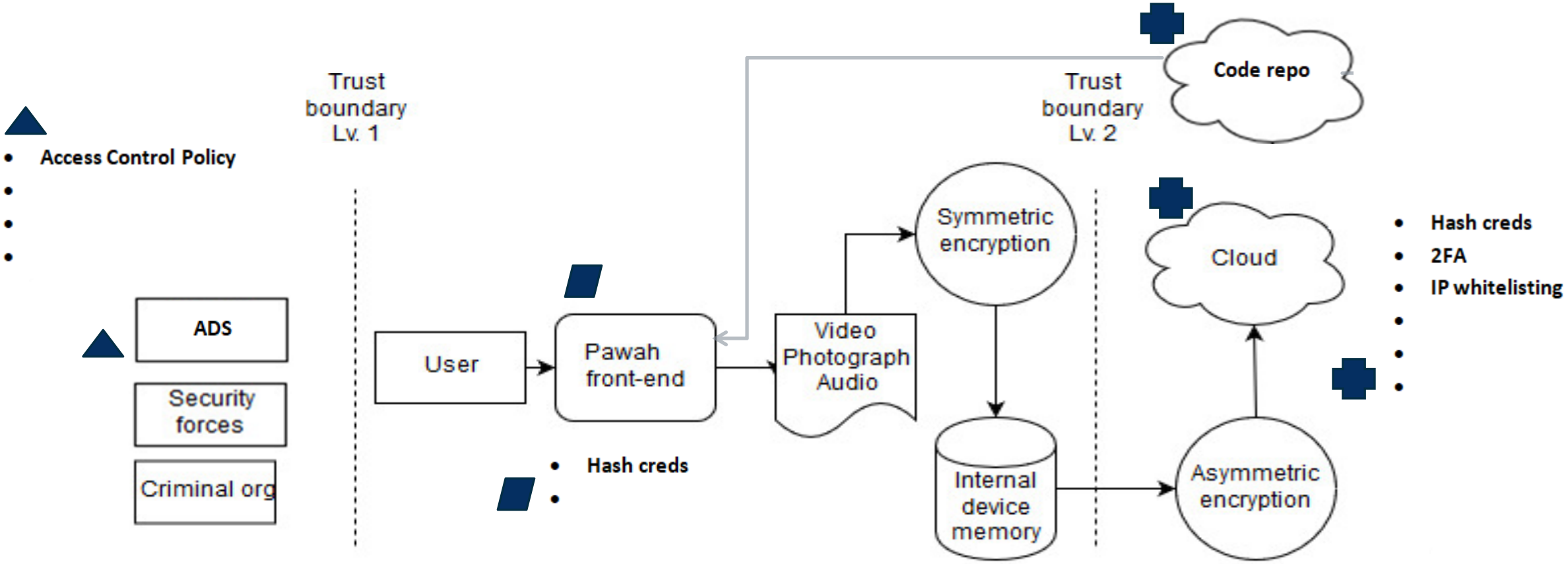
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

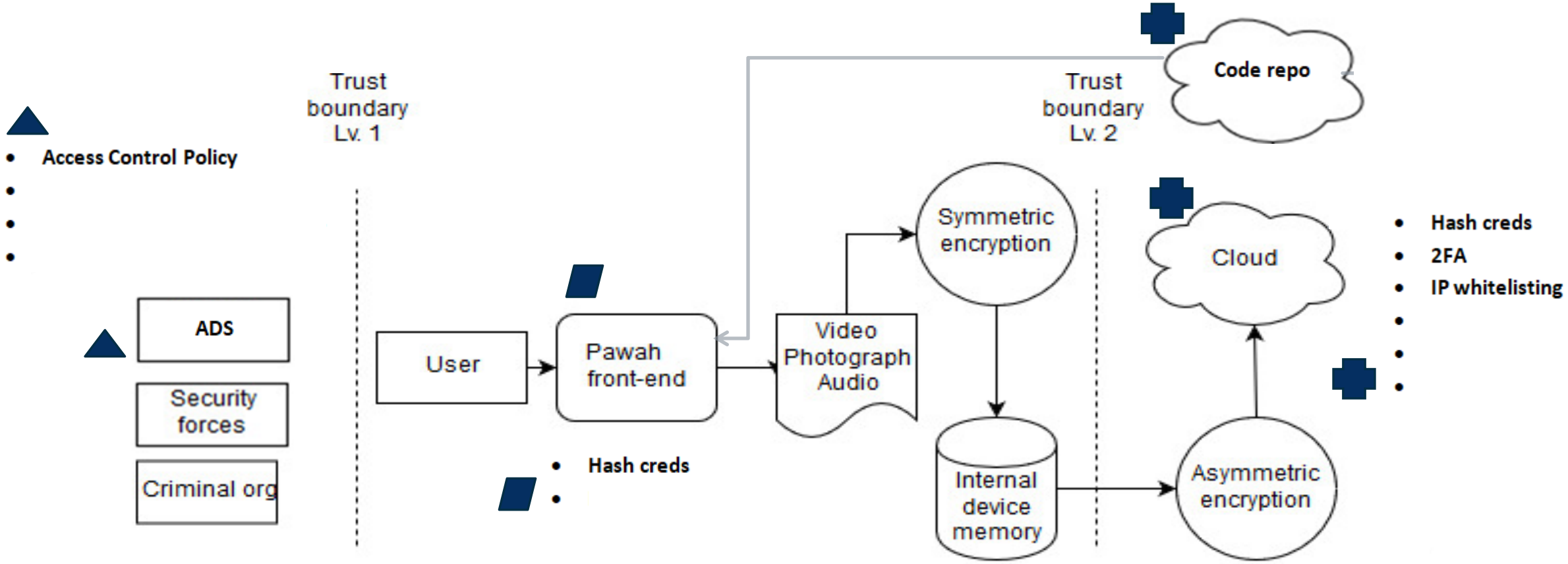
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – TAMPERING

- Data being modified on the phone, cloud storage, anywhere in between
  - File integrity by matching hashes of files at different stages
- Tampering with source code or logs
  - Log all actions of users
  - State in employee contracts what is unacceptable so they have no recourse
  - Forward logs to centralised, hardened log server with strong access control



Threats

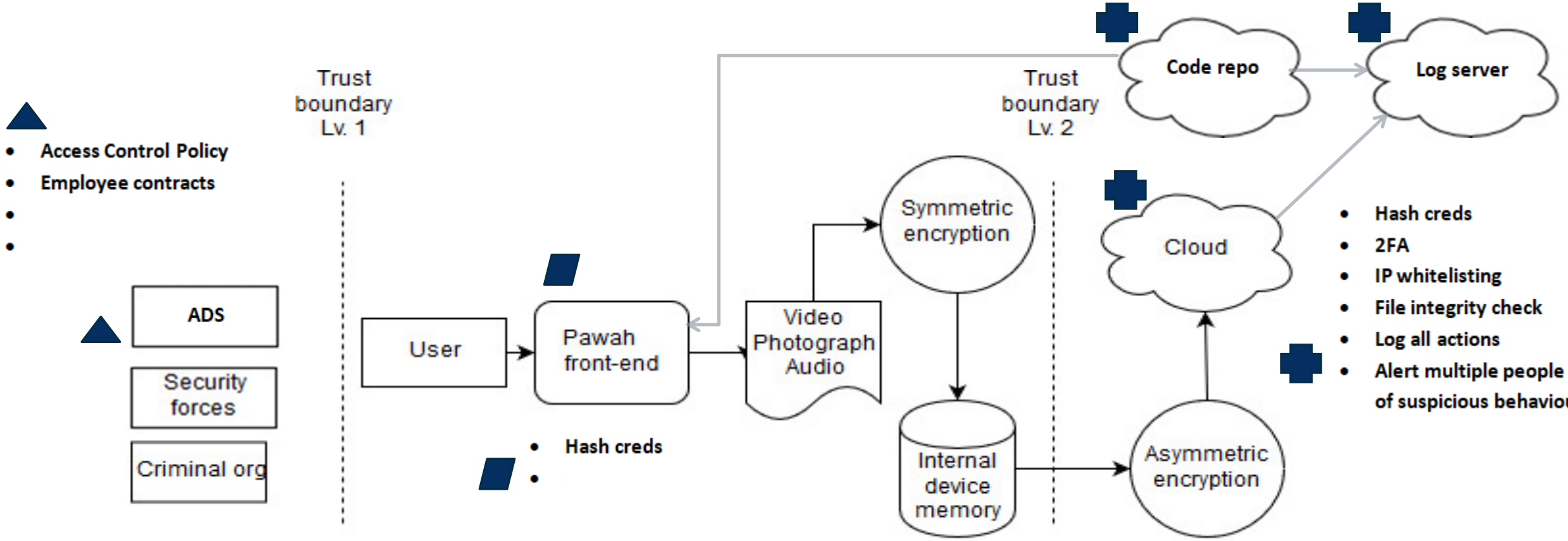
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

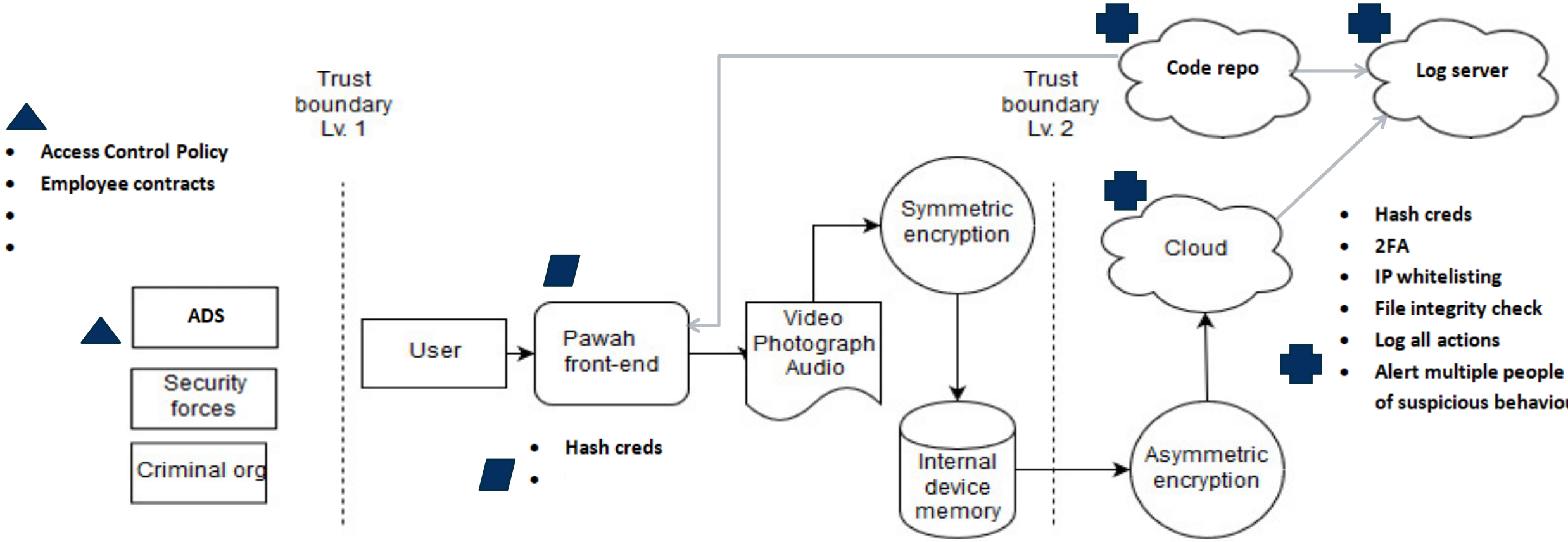
- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE - REPUDIATION

- Someone claims the footage is false or of someone else
  - Other than a forensic chain of custody we can't do much about that
- For your app could someone perform an action and claim it wasn't them?

STRIDE –INFORMATION DISCLOSURE

- Footage is tied to particular users
  - Policy to review footage with lawyers before being submitted as evidence
  - Remove metadata so footage can be posted online anonymously
  - Need further controls once done a deep dive



Threats

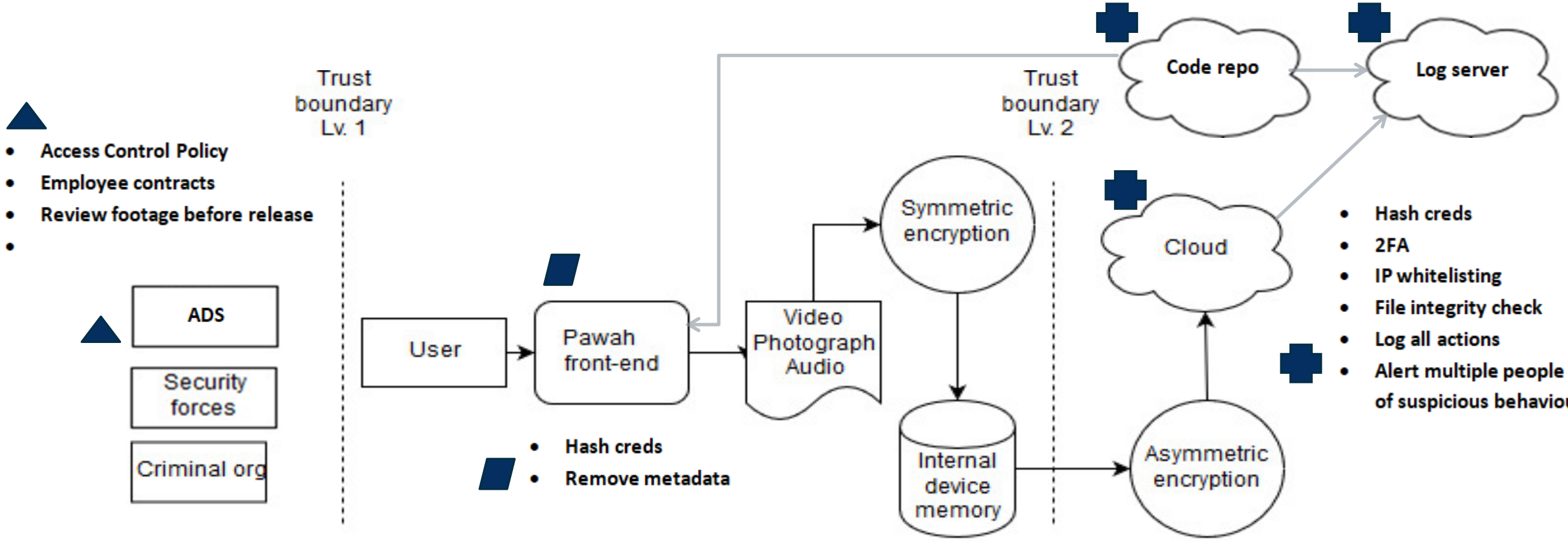
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

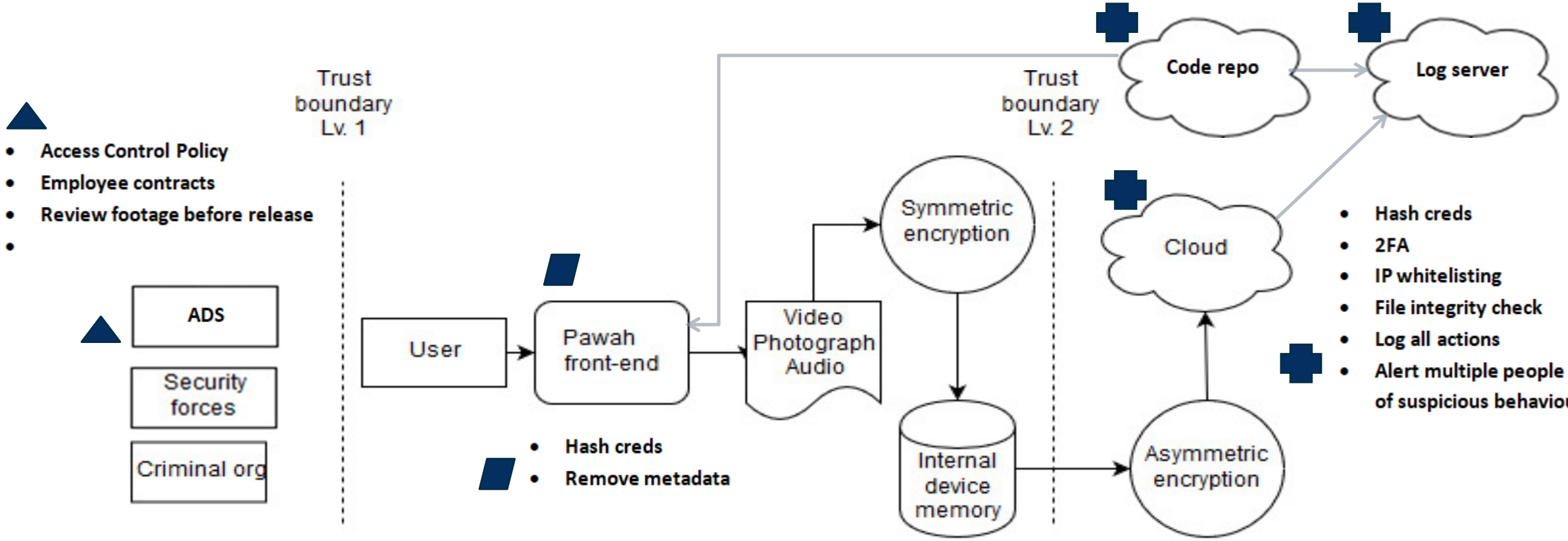
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – DENIAL OF SERVICE

- DDoS attack against the cloud storage (however that may be)
  - Employ DDoS mitigation services like Cloudflare
  - Cap how much footage a user can upload



Threats

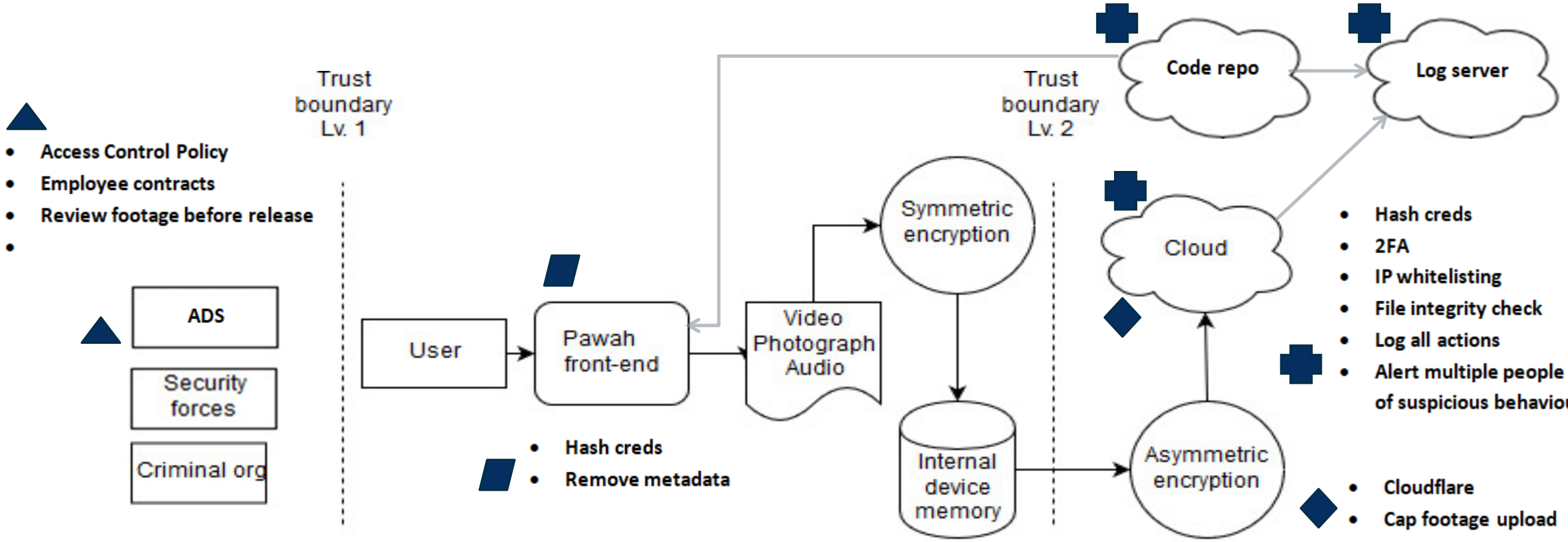
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – ELEVATION OF PRIVILEGES

- Someone gaining administrator rights to the code repository or cloud storage
  - Log all actions by users
  - Flag multiple people of new admins being created
  - Flag multiple people of admins performing anomalous behaviour like logging in outside of work hours.