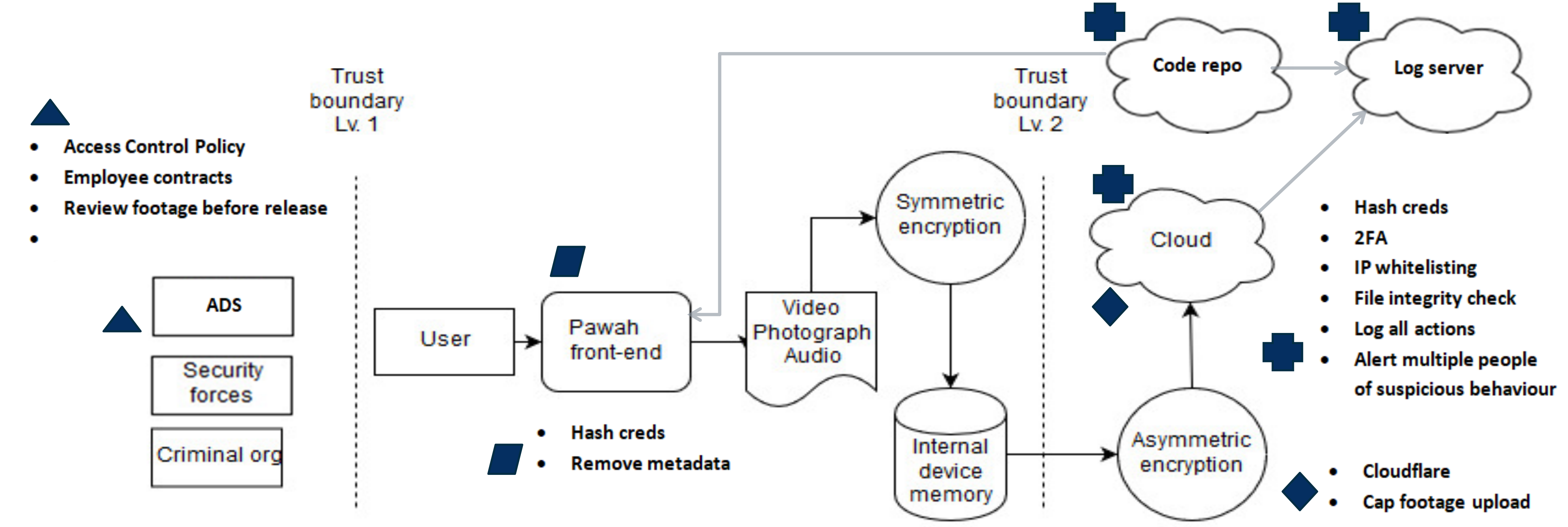


▲

- Access Control Policy
- Employee contracts
- Review footage before release

▰

- Hash creds
- Remove metadata

✚

- Hash creds
- 2FA
- IP whitelisting
- File integrity check
- Log all actions
- Alert multiple people of suspicious behaviour

◆

- Cloudflare
- Cap footage upload

Threats

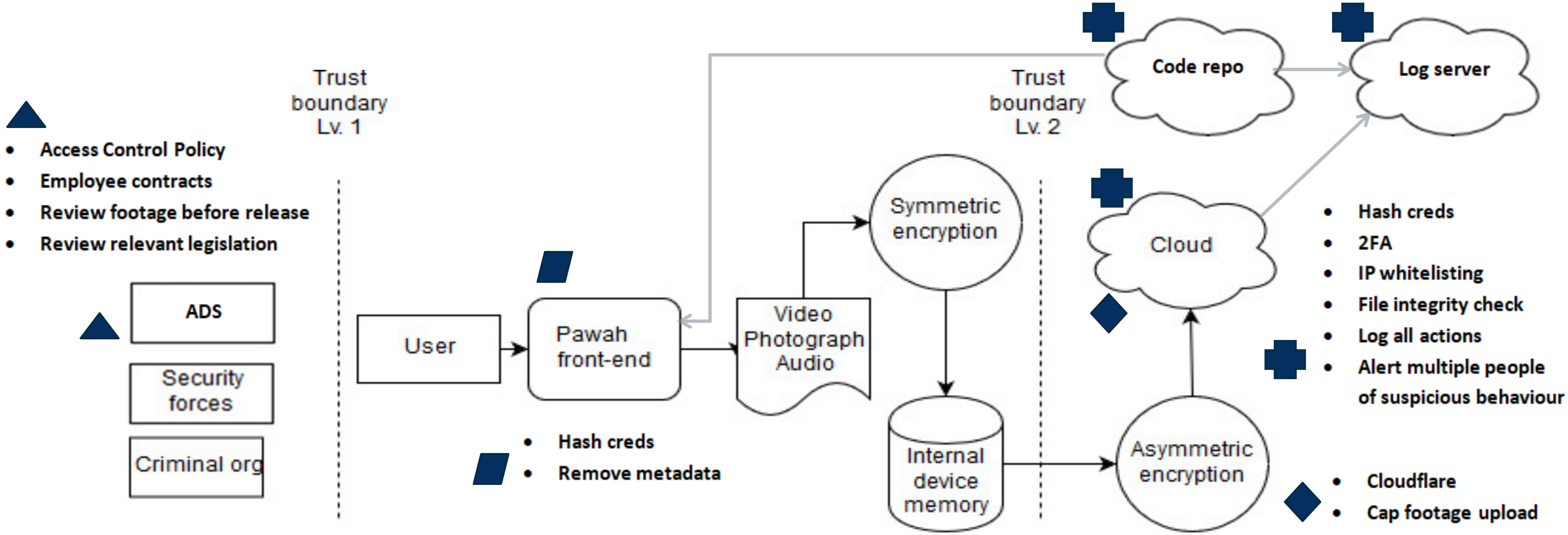
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

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



▲

- Access Control Policy
- Employee contracts
- Review footage before release
- Review relevant legislation

▰

- Hash creds
- Remove metadata

✚

- Hash creds
- 2FA
- IP whitelisting
- File integrity check
- Log all actions
- Alert multiple people of suspicious behaviour

◆

- Cloudflare
- Cap footage 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

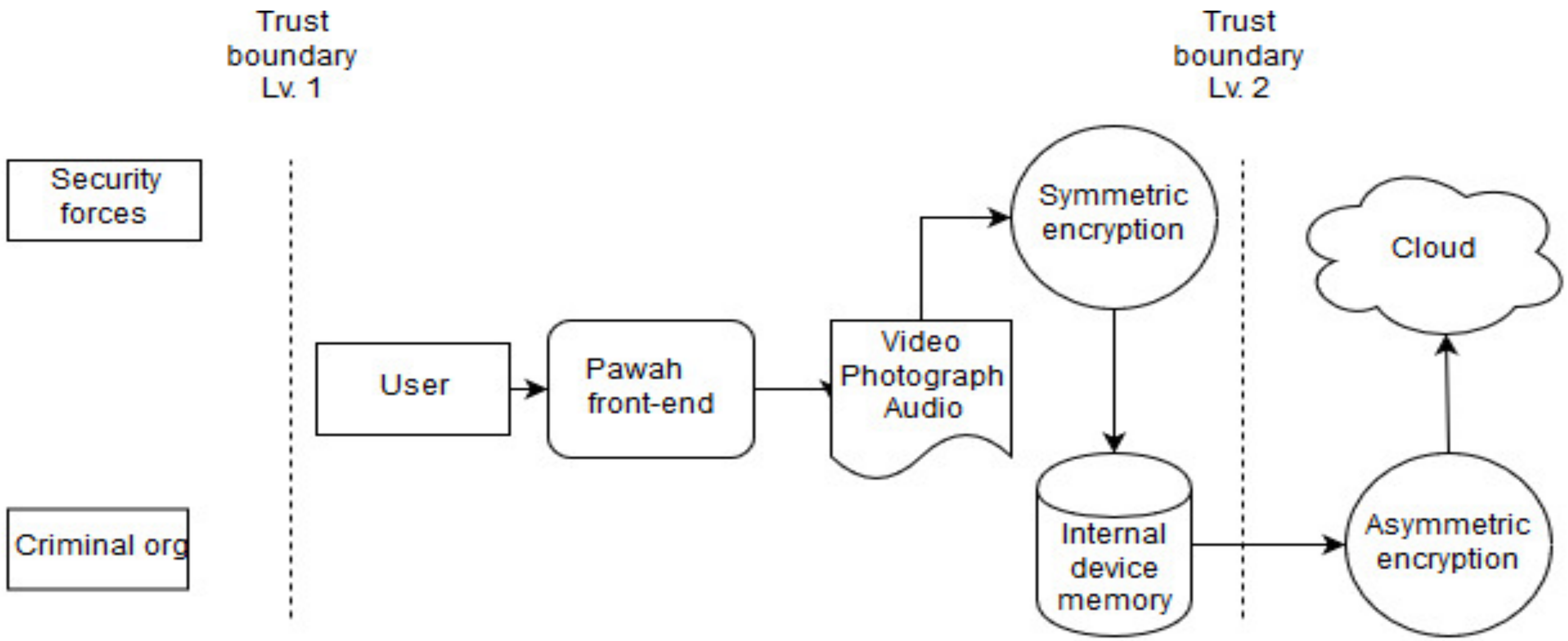
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

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

TAKING THIS FURTHER

- These are basics
- Need to go lower
  - Technology
  - Protocols
  - How can each functionality be abused?
- How can attackers bypass the controls we already have?
- Make threat modelling iterative
- Assign responsibility



Threats

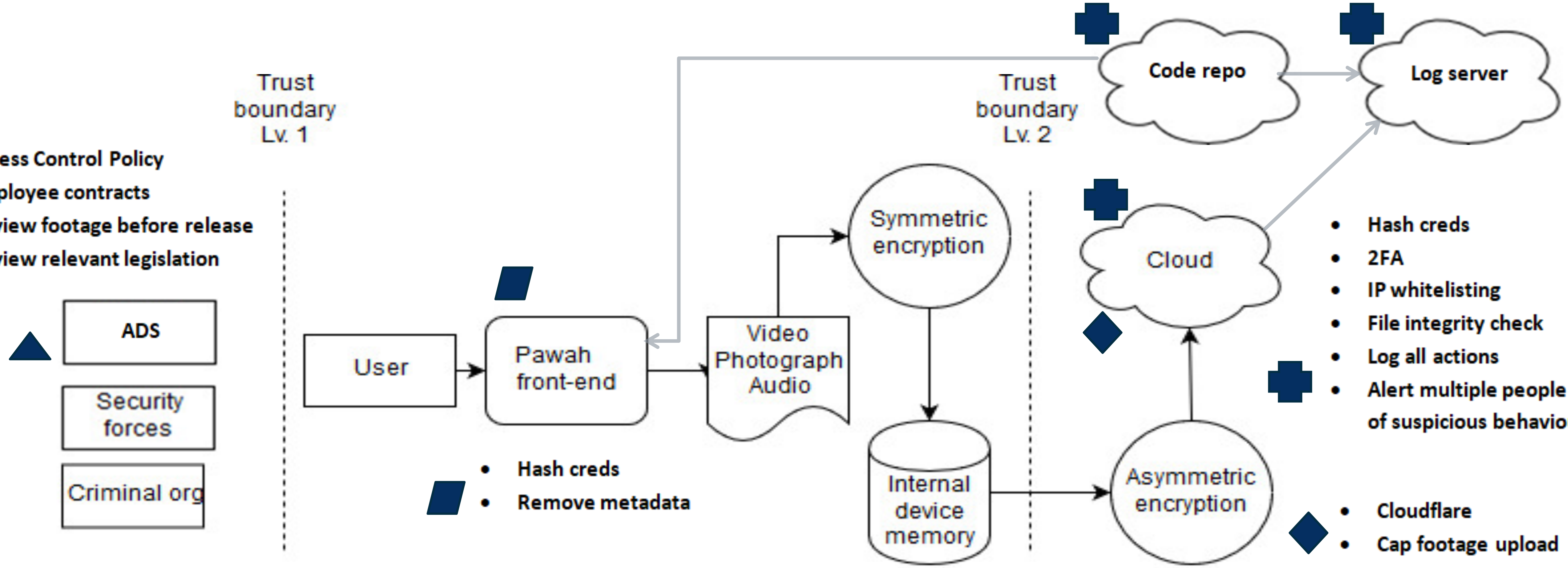
- Violent repression
- Intimidation
- Physical attack
- Kidnapping
- Imprison

Threats

- Device seizure
- Intimidation
- Device hacking

Threats

- Network intervention
- Cloud hacking
- Impersonation
- Social engineering
- DDoS



▲

- Access Control Policy
- Employee contracts
- Review footage before release
- Review relevant legislation

▰

- Hash creds
- Remove metadata

✚

- Hash creds
- 2FA
- IP whitelisting
- File integrity check
- Log all actions
- Alert multiple people of suspicious behaviour

◆

- Cloudflare
- Cap footage 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

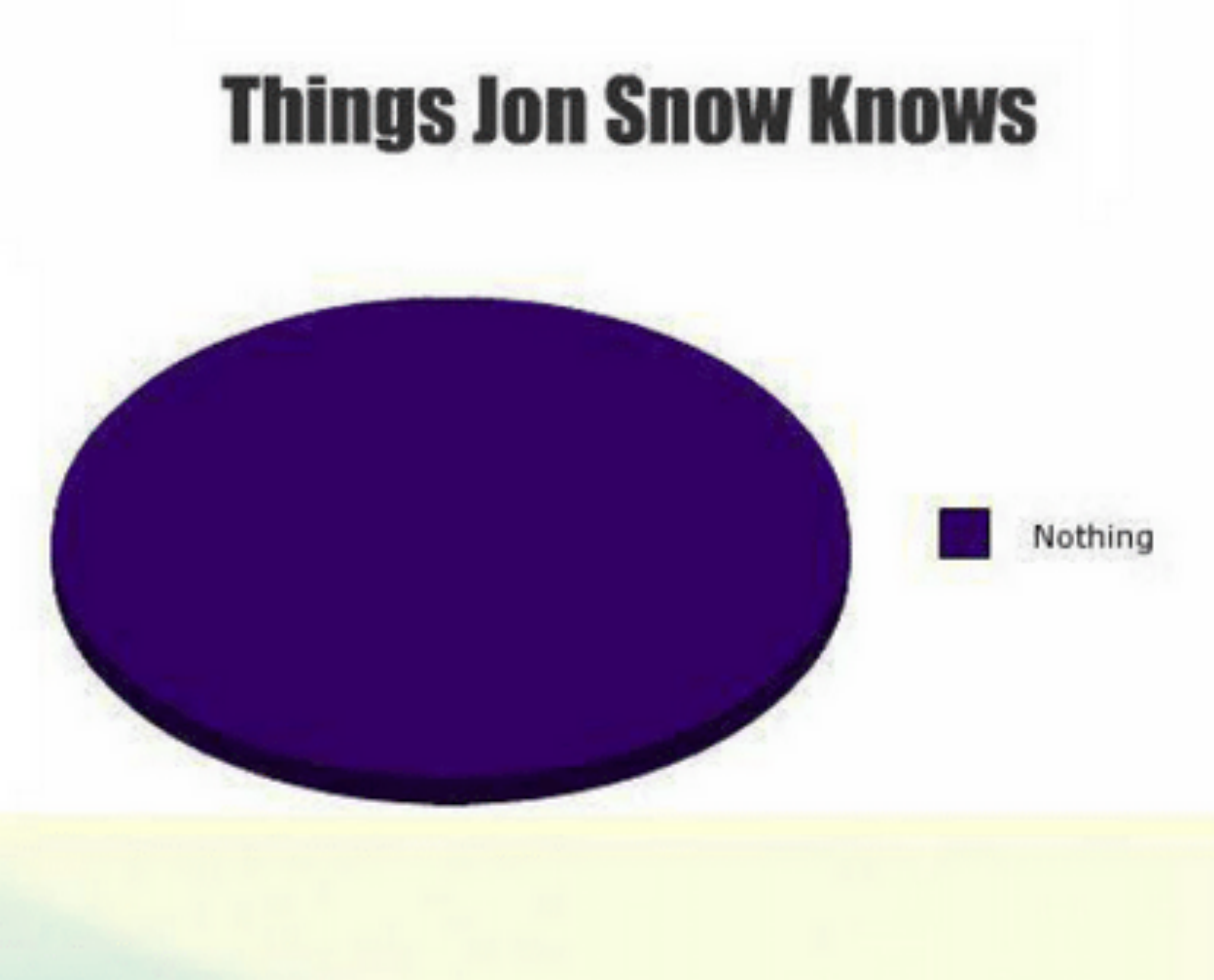
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

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

IF YOU KNOW NOTHING…

- What are we building?
- What can go wrong? STRIDE
  - Spoofing
  - Tampering
  - Repudiation
  - Denial of Service
  - Elevation of Privileges
- What are you going to do about it?
- This is the beginning but not the end



RESOURCES USED

- https://users.encs.concordia.ca/~clark/courses/1601-6150/scribe/L04c.pdf
- Threat Modelling with STRIDE adapted from Threat Modelling: Designing for Security (Wiley, 2014) by Adam Shostack
- https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649749(v=pandp.10)
- Walkthrough: Creating a Threat Model for a Web Application