



**irdeto**

Protect. Renew. Empower.

## **Dutch Guild 59 - Content Piracy Forensic Watermarking**

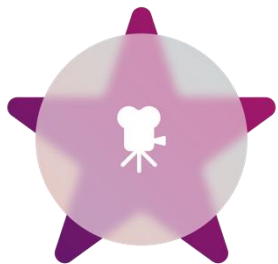
November 2024

Ronald Peters

# Why Forensic Watermarking



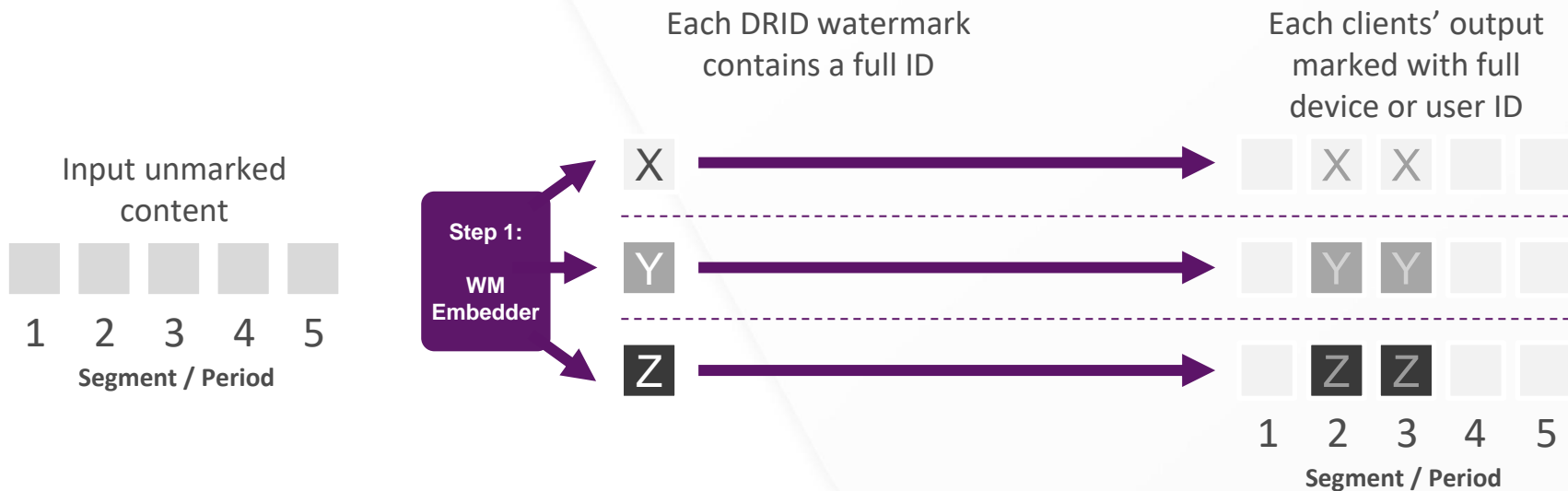
- Targeted at high-value (live) TV & movie content with support for 4K UHD
- Content owner compliance (MovieLabs, Premium Live Sports, VoD License owners)
- Identification of illegally distributed assets, reactive tool with deterrent effects
- Can be applied at B2B (distribution) or B2C level



FARNCOMBE SECURITY AUDIT™ WATERMARK	
Company	IRDETO
Product	IRDETO TRACEMARK™
Date	JULY 2021

Cartesian, Inc.

## Every receiver a unique copy



- In use for short clips (DWM/Headend), Broadcast Client, OTT Client
- Embedded in multiple frames
- Detected from a single frame

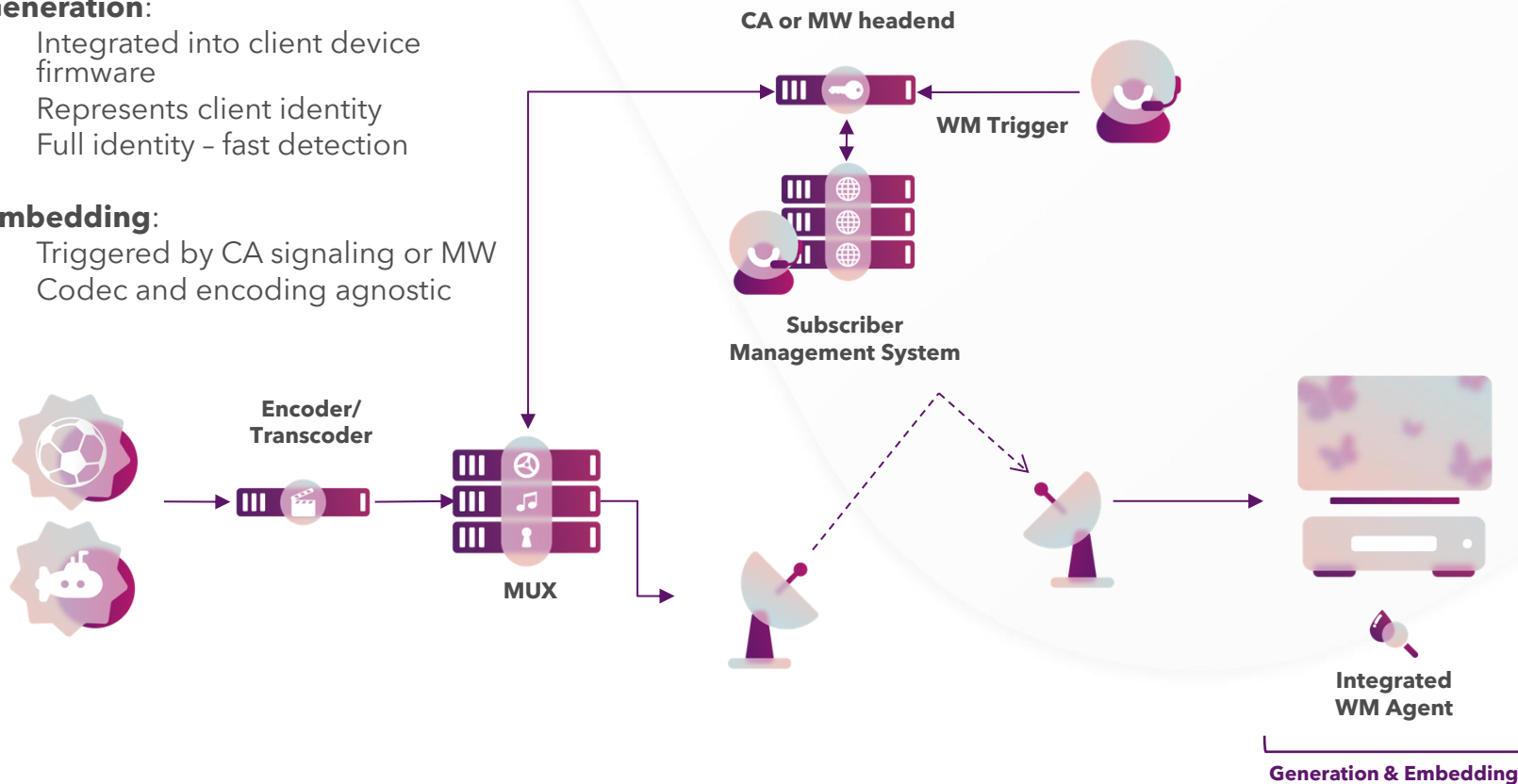
# Broadcast Client-Side Watermarking

## Generation:

- Integrated into client device firmware
- Represents client identity
- Full identity - fast detection

## Embedding:

- Triggered by CA signaling or MW
- Codec and encoding agnostic



# OTT Client-Side Watermarking

## Generation:

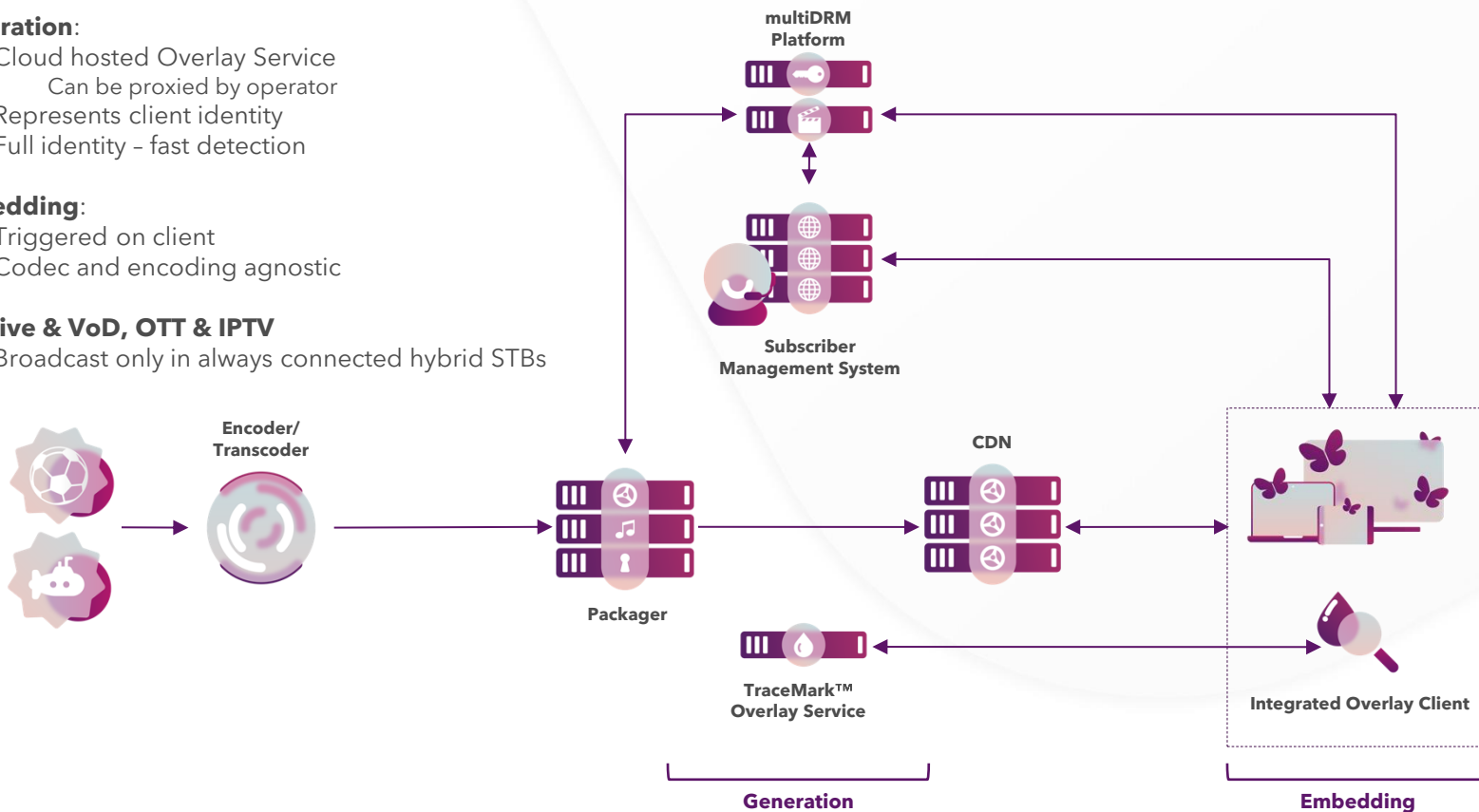
- Cloud hosted Overlay Service
  - Can be proxied by operator
- Represents client identity
- Full identity - fast detection

## Embedding:

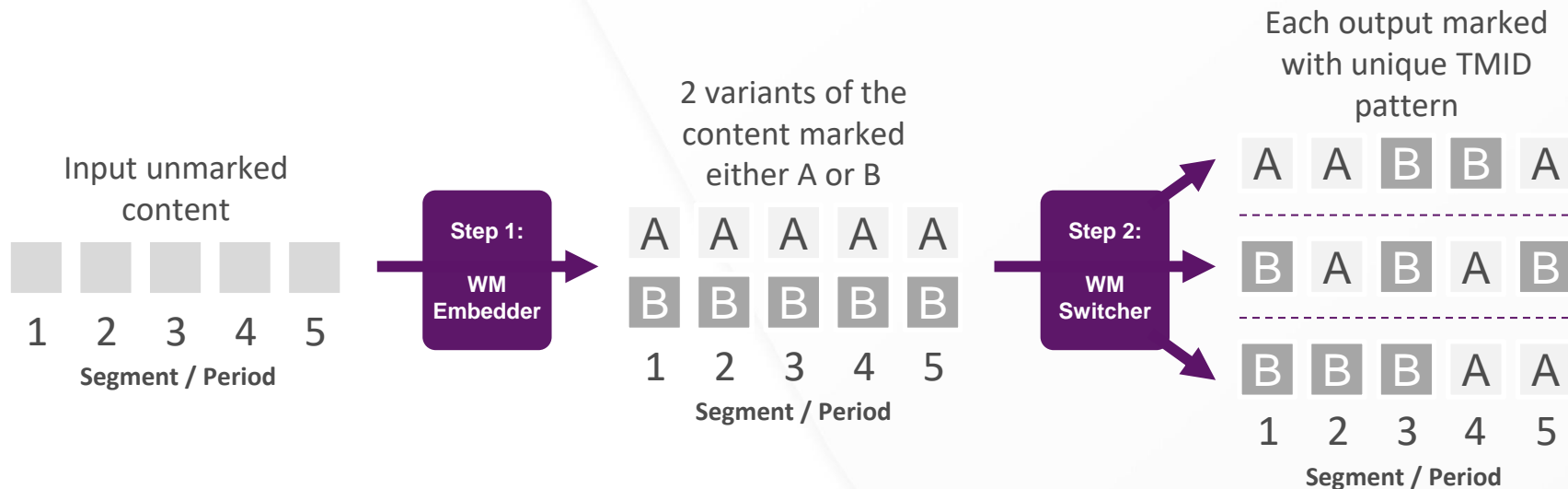
- Triggered on client
- Codec and encoding agnostic

## Fits Live & VoD, OTT & IPTV

- Broadcast only in always connected hybrid STBs



## Every receiver a unique copy, over time



- Used to reach many users from only two segment copies (A/B)
- In use for longer clips (>10 minutes) DWM/Headend

# B2C A/B watermarking for OTT Server-Side

## Generation

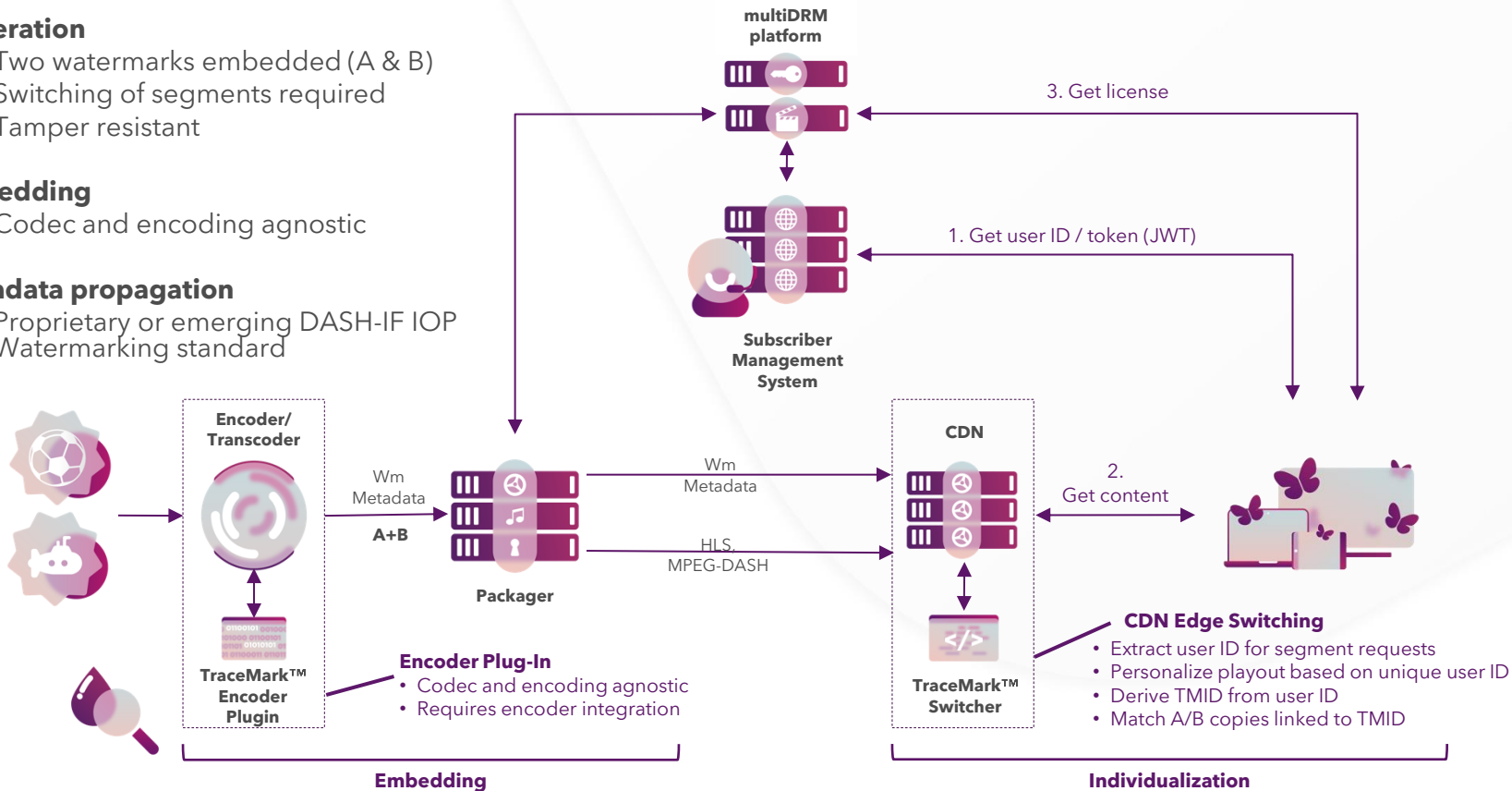
- Two watermarks embedded (A & B)
- Switching of segments required
- Tamper resistant

## Embedding

- Codec and encoding agnostic

## Metadata propagation

- Proprietary or emerging DASH-IF IOP Watermarking standard



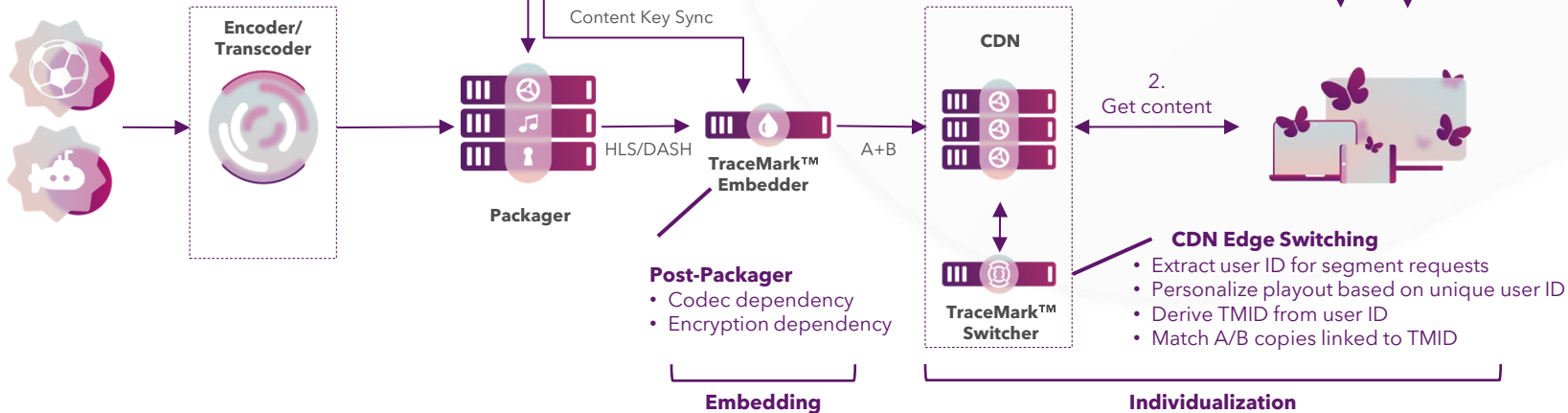
# What if you can't get into the encoder/transcoder?

## Generation:

- Introduce extra node
  - WM Embedding Origin
- Switching of segments
  - Embedding on the fly
  - A and B can be cached (BAU)

## Embedding:

- Codec, encoding & encryption dependent
- Mostly suited for Live





# OTT: Head-End vs Client-Side Watermarking



Head-End Watermarking	Client-Side Watermarking
<i>Reach both managed and unmanaged devices</i>	Generally, only for closed, managed devices
<i>Less prone to reverse engineering</i>	Vulnerable to circumvention attacks
<i>Less visible to end-users</i>	More visible to end-users
Requires more video to identify the watermarking identity	<i>Less video required for watermarking detection</i>
<i>Upgrades to the watermark easy to perform centrally for all devices</i>	Difficult and costly to upgrade and maintain, especially as device type base diversifies over time
Additional infrastructure required for additional content and channels	<i>Available for all content streamed by the platform</i>
<i>Strong against collusion attacks</i>	Weaker against collusion attacks
<i>Compliant to all content owners</i>	Compliant to some content owners
<i>Best architecture to catch pirates</i>	Less suitable for catching (today's) pirates



- AWS based managed service, accessible by GUI and API's
- (Blind) Detection from files and live feeds, returns detected id from the CDN token
- Needs minimum of 1 minute video for A/B WMing, 5-10 recommended, longer in case of collusion
- Optional integration with CDN revocation services (blocklist)

The screenshot displays the IRIS Watermarking Detection Jobs interface. The main content area shows a job titled "Control Panel" with a video thumbnail containing the URL `http://ore-tlsa-captured-streams.s3-website-us-west-2.amazonaws.com/31261/89894/a8e4d3b`. Below the thumbnail, the video profile is listed: Size: 0 MB, Duration: 00:02:00, Fps: 25/1, Codec: h264 (Main) 1920x1080 (yuv420p) 0 Mbps.

The "Detection Results" section shows the following summary:

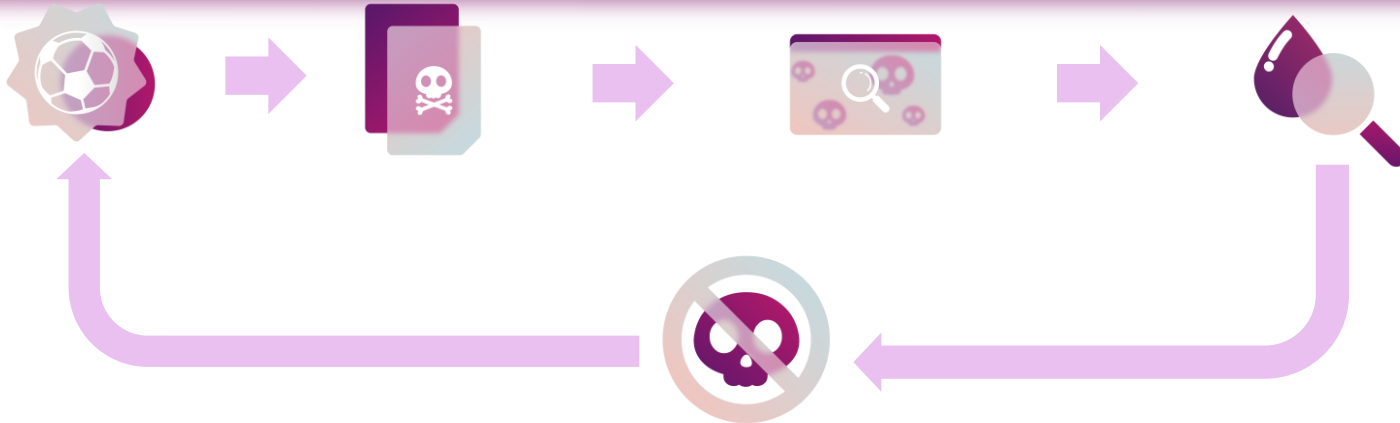
- Detected symbols: 59
- Unique symbols: 59
- Collusion: No

A bar chart below the summary shows the detection count over time, with a legend for symbols A (purple) and B (orange). The x-axis represents frame number (time) from 00:00:00 to 00:01:48.

The "Accused User ID(s)" section lists the user `YzlhZThiOWEtyWY1` with a "Block" button. Below this are buttons for "Show detailed accusation results" and "Show detected tmid details".

The bottom of the interface shows a progress bar at 100% and a "COMPLETED" status.

# Demo Introduction





# irdeto

Protect. Renew. Empower.