DESIGN CONFERENCE

JULY 9-13, 2023 ◆ SAN FRANCISCO, CA

Establishing Trust in IP through Automated Attestation

Serge Leef - June 12, 2023

Since IP is commonly managed and transmitted in the source form, it is particularly vulnerable to, for example, malicious functionality insertions. An attacker can easily modify the IP blocks to include unintended functionality. Considering that IP blocks could contain thousands of lines of code and are very difficult for non-authors to understand, hiding additive features is not particularly difficult. Thus, there need to be tools for vulnerability assessment and scoring along with methodologies to assure the IP end user that the block is authentic and has not been modified by anyone other than the original author.

IP Re-use Today

- **Basic building block** – re-used IP represents upwards of 90% of modern SoCs
- **Multiple sources** – can be custom, bought, re-purposed and crowd-sourced
- **Viability confirmation** – functionality/performance confirmed via simulation
- **Variable provenance** – in many cases, the origins and functionality are unknown
- **Ideal Trojan host** – intentional or un-intentional exploitable flaws are common
- **Unpublished capabilities** – there is no easy way to determine “what else” it does
- **Establishing trust** – out-of-the-box usage is unlikely as security and vulnerability factors are not objectively verifiable

Possible Approach

Capability to objectively and automatically attest IP to enable smooth and efficient discovery, deployment and integration

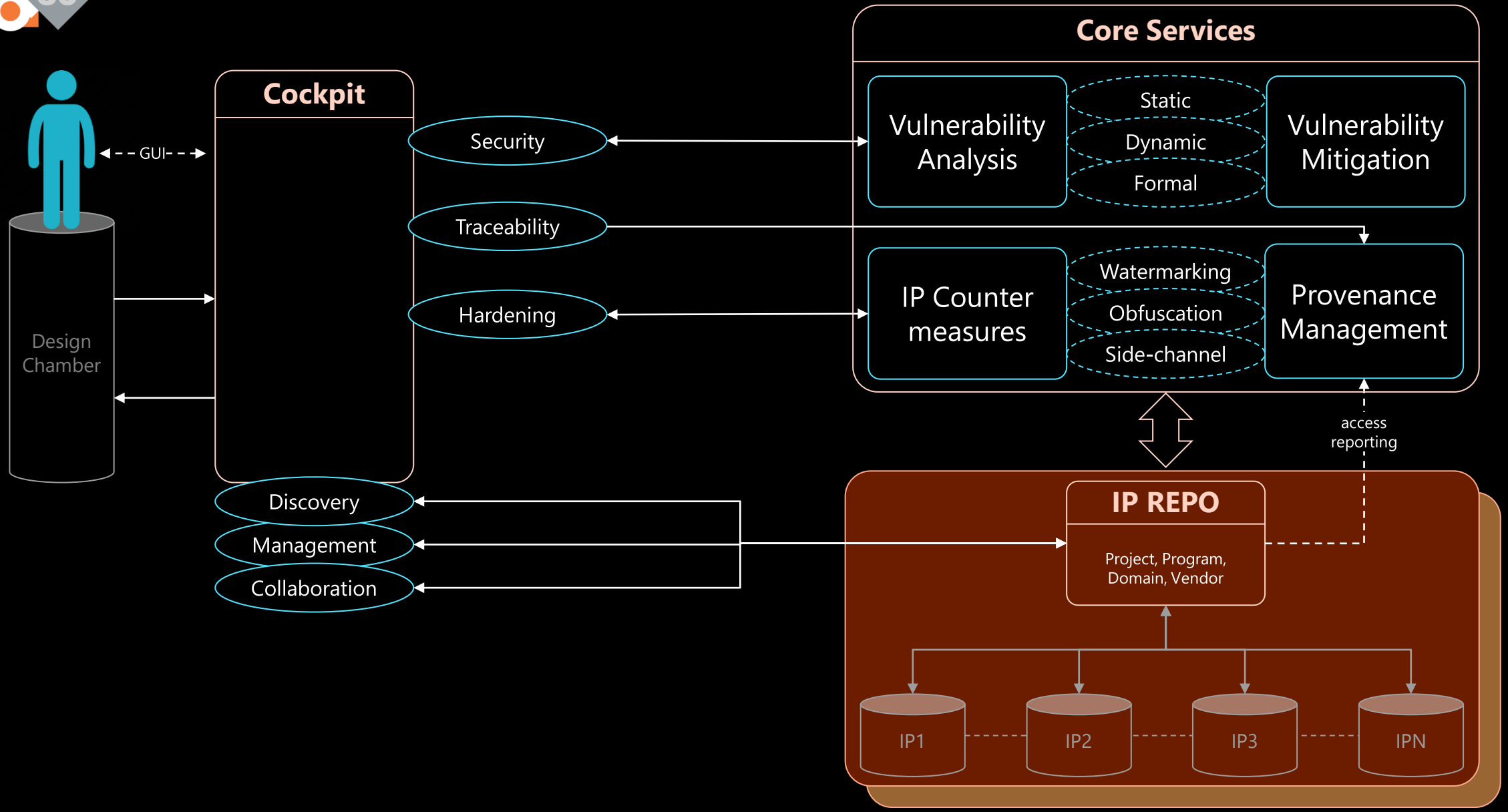
- **Incorporate** IP re-use capabilities into a cloud-service capable of supporting all commonly used methodologies and tools
- **Utilize** advanced IP security technologies that evolved over past decade
  - Static, Dynamic & Formal IP analyzers, Vulnerability mitigation (counter-measure) tools, IP hardening technologies
- **Capitalize** on enterprise scale and related technical assets
  - Cloud-based design, quantitative assurance, community code repositories, data governance
- **Partner** with Government to enable implementation and deployment
  - IP management, security, and distribution are imperative to US competitiveness and are recognized in the CHIPS Act

Repository Types {Project, Program, Domain, Vendor}

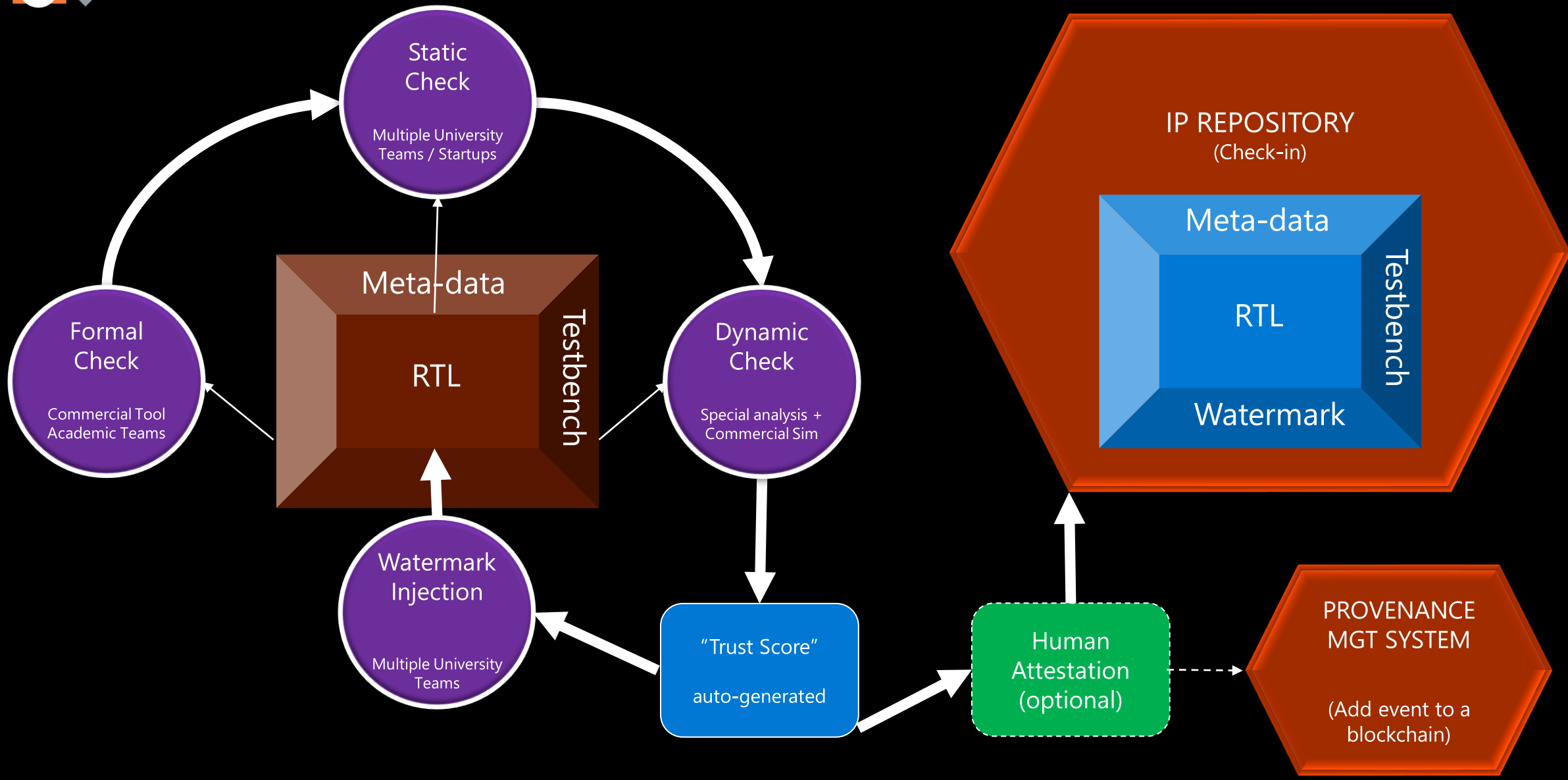
Assumption: Repositories can host any mix of legacy, open-source, and commercial IP

- **Project** – IP for execution of specific project within organizational boundaries (ex: Network Processor SoC)
- **Program** – IP to enable multiple organization working collectively and collaboratively toward a common design goal (ex: Gov-funded collaboration of a university, DIB, and a startup)
- **Domain** – IP library consisting of titles expected to be used together for designs in specific application spaces (ex: Electronic Warfare)
- **Vendor** – Commercial IP vendor making a subset of their offerings available in a secure/trusted form resulting from automated attestation (Ex: Memory Interface IP titles)

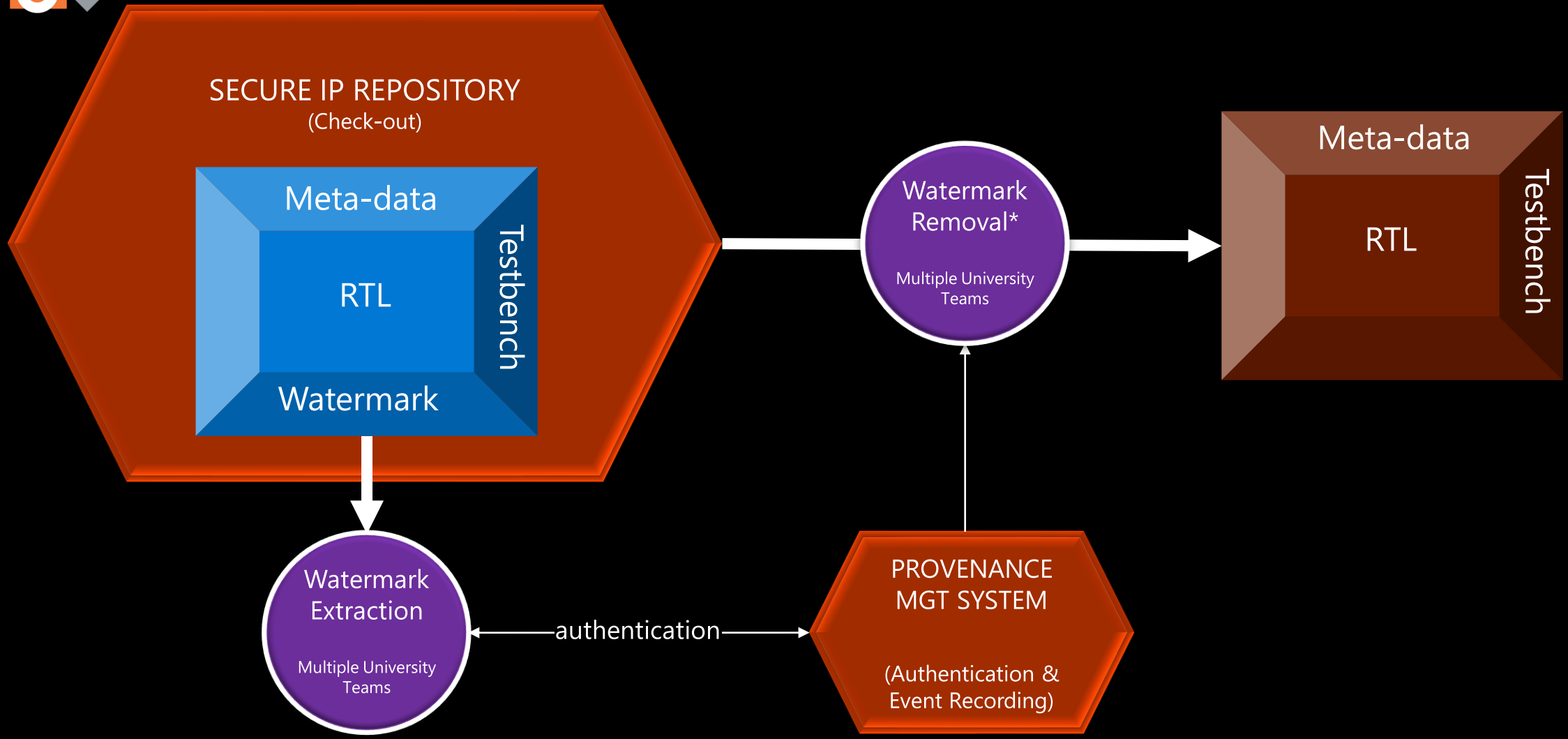
Secure IP Repository Concept



A Suite of Checkers can Derive a Trust Score

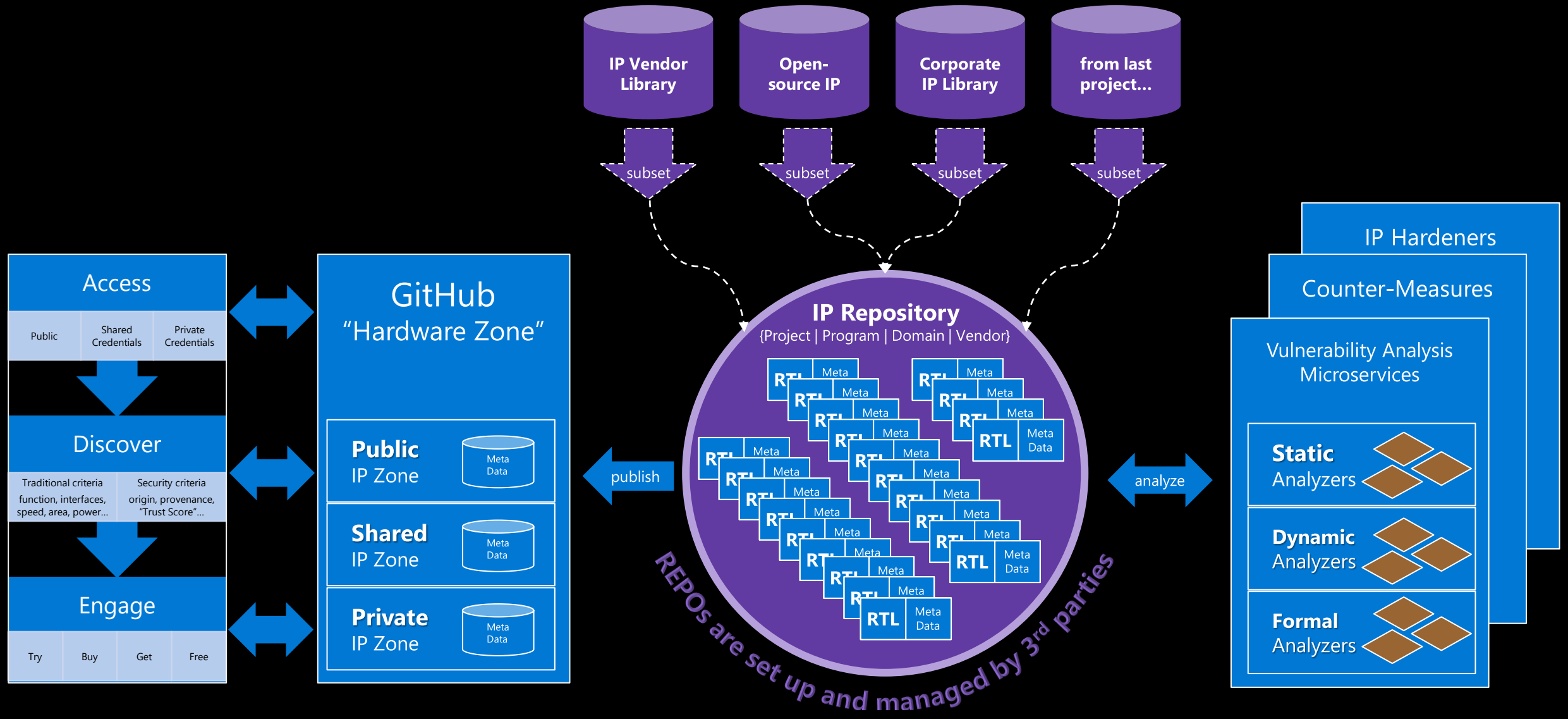


Watermark Removal



*Watermarks left in place can survive transformations all the way to silicon

Diagram

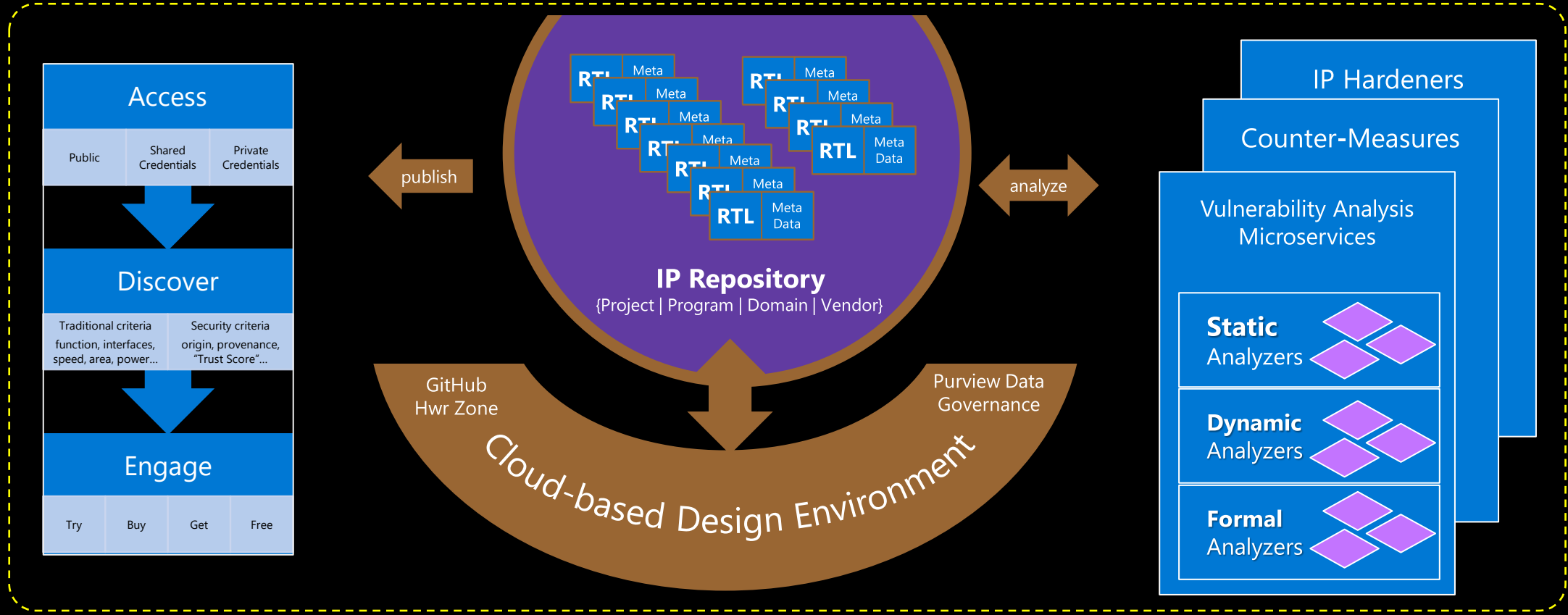

IP Vendor Library
Open-source IP
Corporate IP Library
from last project...
subset
subset
subset
subset
Access
Public
Shared Credentials
Private Credentials
Discover
Traditional criteria
function, interfaces, speed, area, power...
Security criteria
origin, provenance, "Trust Score"...
Engage
Try
Buy
Get
Free
GitHub
"Hardware Zone"
Public IP Zone
Shared IP Zone
Private IP Zone
Meta Data
publish
IP Repository
{Project | Program | Domain | Vendor}
RTL
Meta
Data
analyze
IP Hardeners
Counter-Measures
Vulnerability Analysis Microservices
Static Analyzers
Dynamic Analyzers
Formal Analyzers
REPOs are set up and managed by 3rd parties

Foundation for Secure IP Exchange

U/X Partner(s)

Repository Partner(s)

Security Partner(s)



Summary

Trusted IP repository concept

Design IP repositories (classified, commercial, open-source, legacy)

Watermarking services to maintain integrity and provenance

Trojan detection analysis capabilities on importation

The bigger picture vision…