Trust and Resilience in Modern Sovereign Infrastructure

Karanbir Singh, Senior Distinguished Engineer
Red Hat (UK) Ltd

Red Hat

Trust me when I tell
you not to trust anyone !

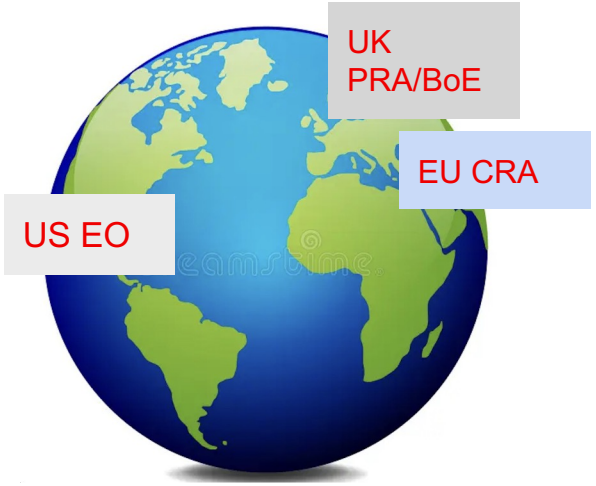
Red Hat

Open Source Won

And with it comes the winners burden

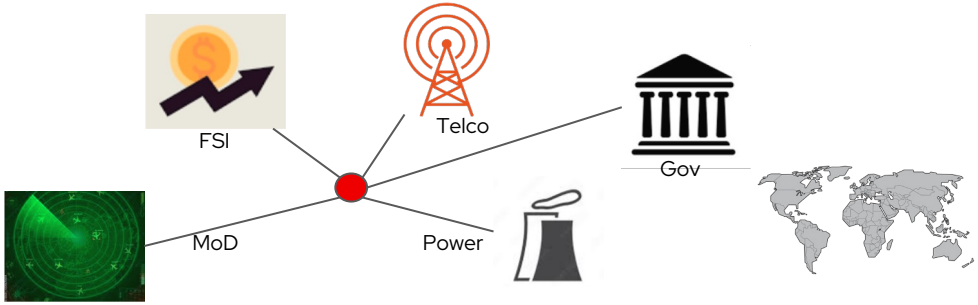
Why Trust & Resiliency Matters?

- Every industry runs on IT
- Growing **regulatory pressures**
- **Geopolitical** Pressure & Risks
- Continuity and confidence = **business critical**



Red Hat

Regulated Consumers are well entrenched in the Open Source ecosystem today



It Is

- Regulated
- Defined / Assertable
- Dynamic

It Can be

- Geo / Political
- Industry Specific
- Posture Driven

It is not just (*)

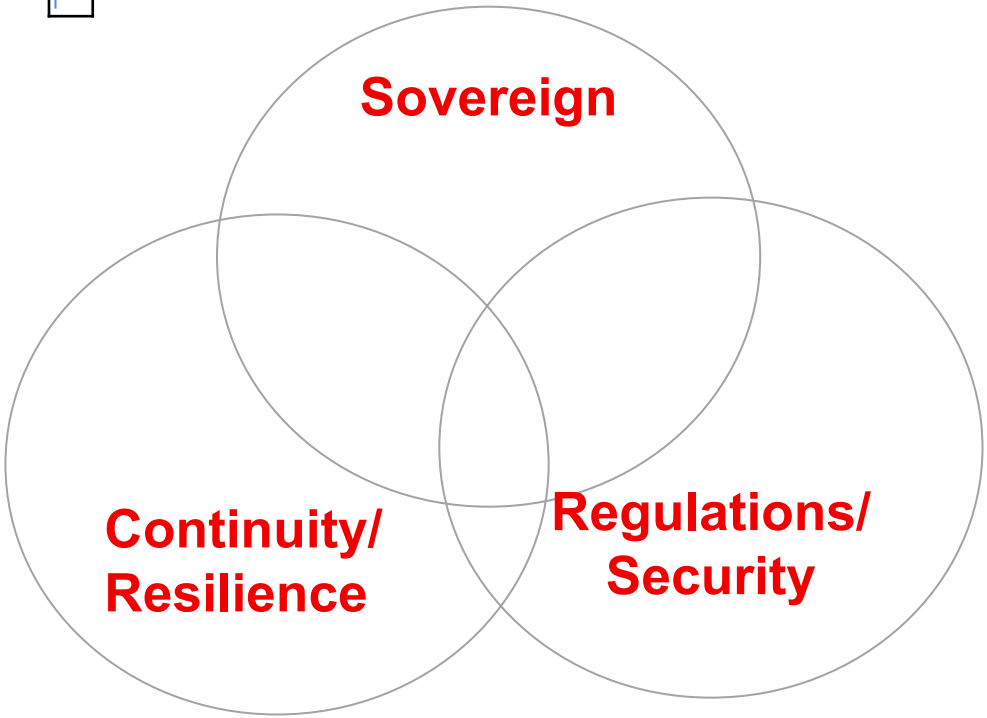
- Private
- Disconnected
- On Prem

Enabling, at reducing cost { people, time, tooling }, is a key aspect of maturity.

Cascading value, Realisation of common context, Consistently

(*) : We get private, disconnected and on-prem as a by product of execution, but these are not goals in themselves

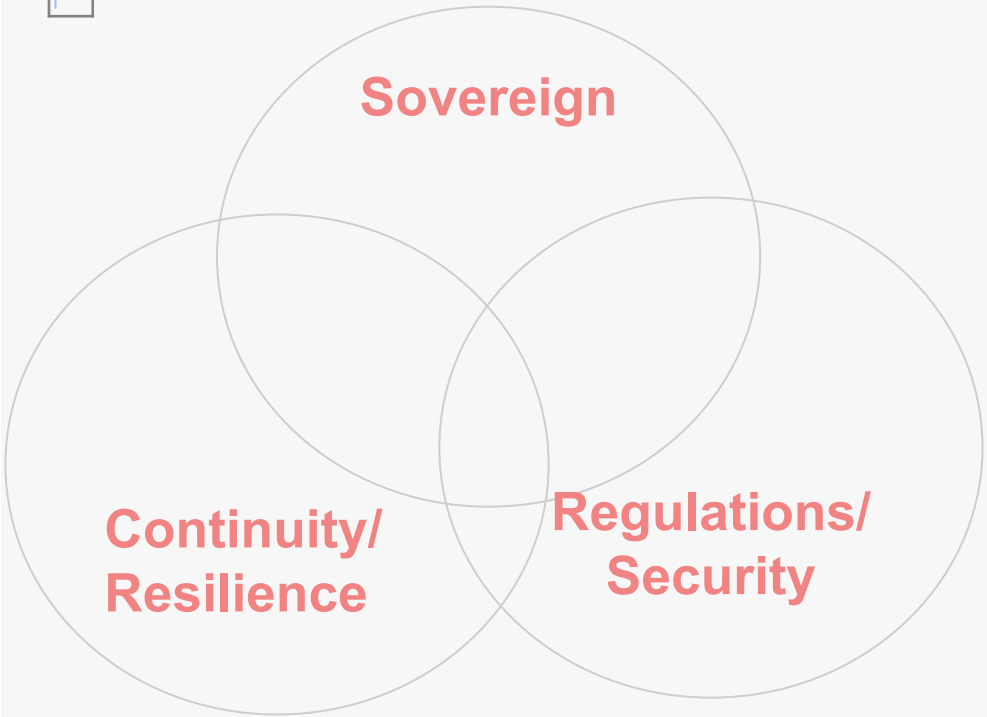
Multi-Dimensional Challenges



- Sovereign: Who controls data/code?
- Critical infra: Can I recover at scale?
- Regulations: Can I prove compliance?

Always under cost & speed pressure

Multi-Dimensional Challenges



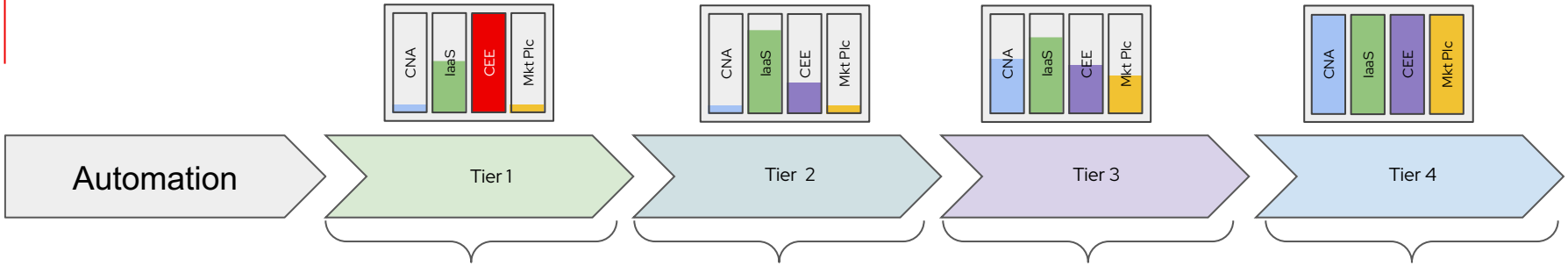
- Sovereign: Who controls data/code?
- Critical infra: Can I recover at scale?
- Regulations: Can I prove compliance?

Always under cost & speed pressure

What's your Malware Story ? Your Ransomware push back ?

Red Hat

IT Systems are getting complex



Dependent of customer journey - where they are and desired outcome —>

Self Service

Cost Management

Compliance

Observability

Continuity

CNA : In Cloud Assets

Failure Domains

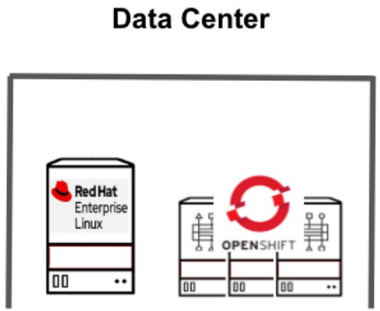
Ecosystem

High order : eg. GPUaaS

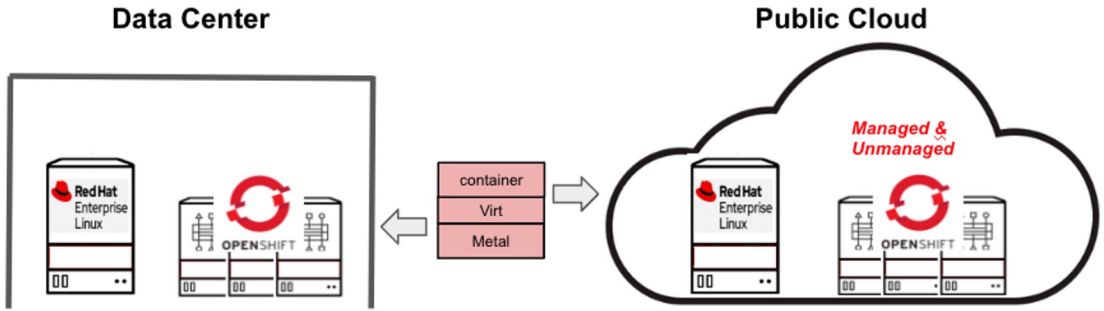
Global Availability

Red Hat

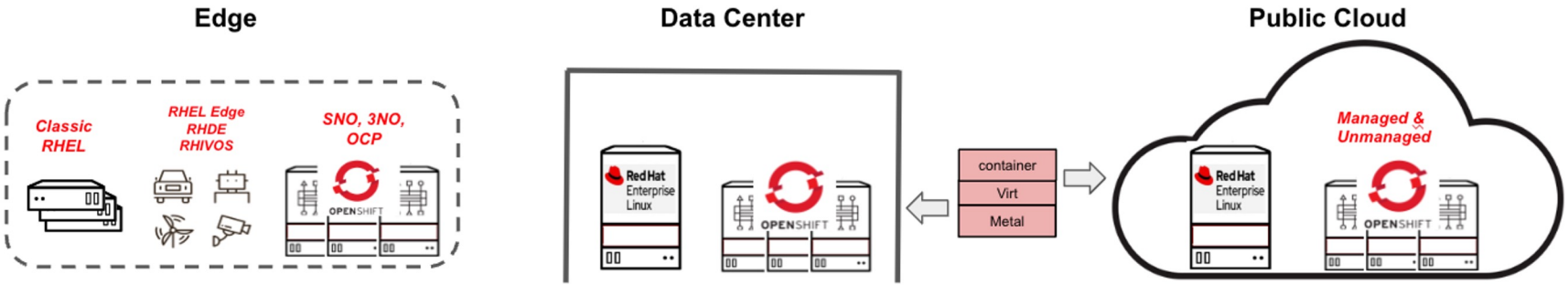
Management Topology - Hybrid Infrastructure & Hybrid Cloud



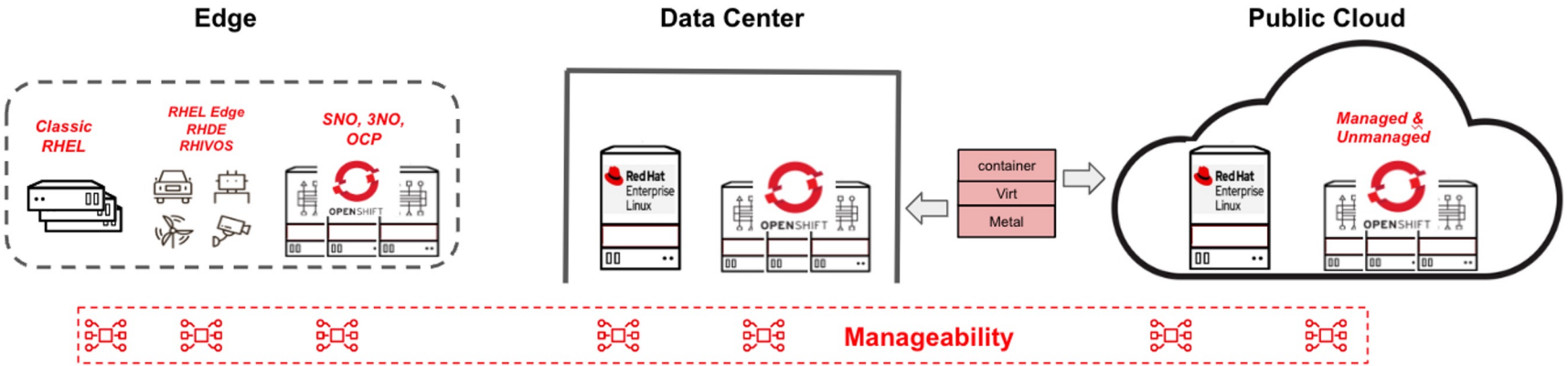
Management Topology - Hybrid Infrastructure & Hybrid Cloud



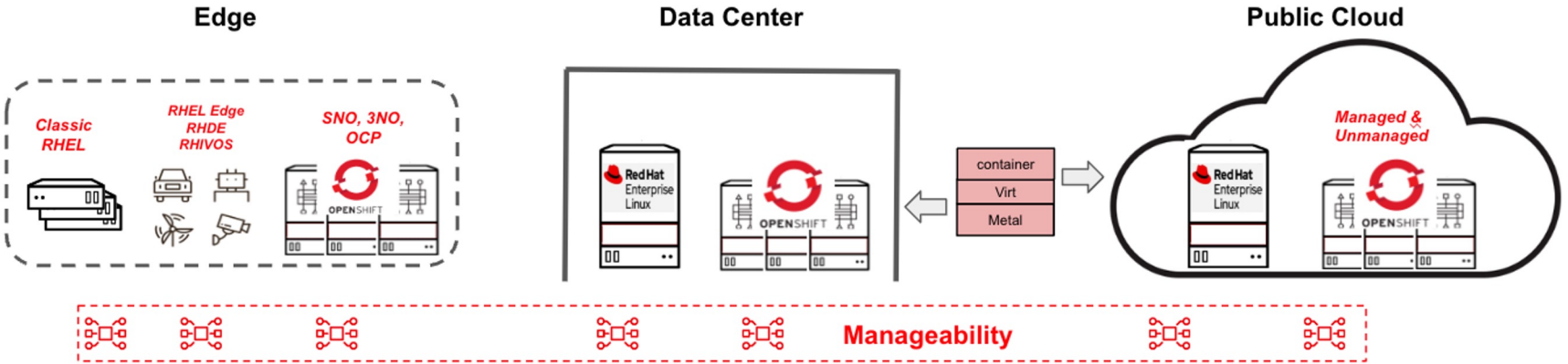
Management Topology - Hybrid Infrastructure & Hybrid Cloud



Management Topology - Hybrid Infrastructure & Hybrid Cloud



Management Topology - Hybrid Infrastructure & Hybrid Cloud



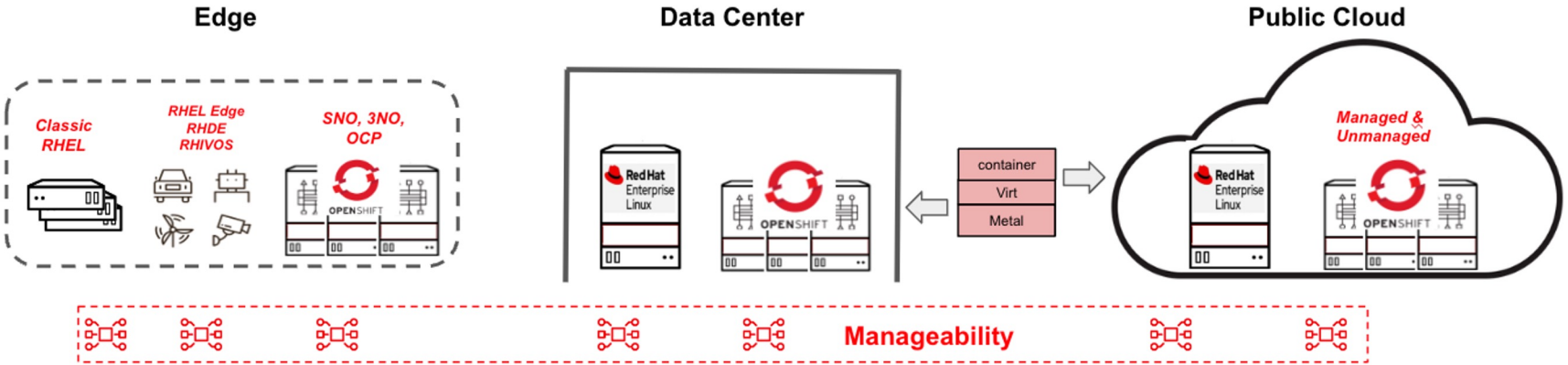
Management Capabilities

Lifecycle	Inventory	Configuration	Security	Automation	Continuity	Observability	Cost

Integration / Ecosystem

Operations
(IT Operators, Infrastructure Engineers, SREs, etc.)

Management Topology - Hybrid Infrastructure & Hybrid Cloud



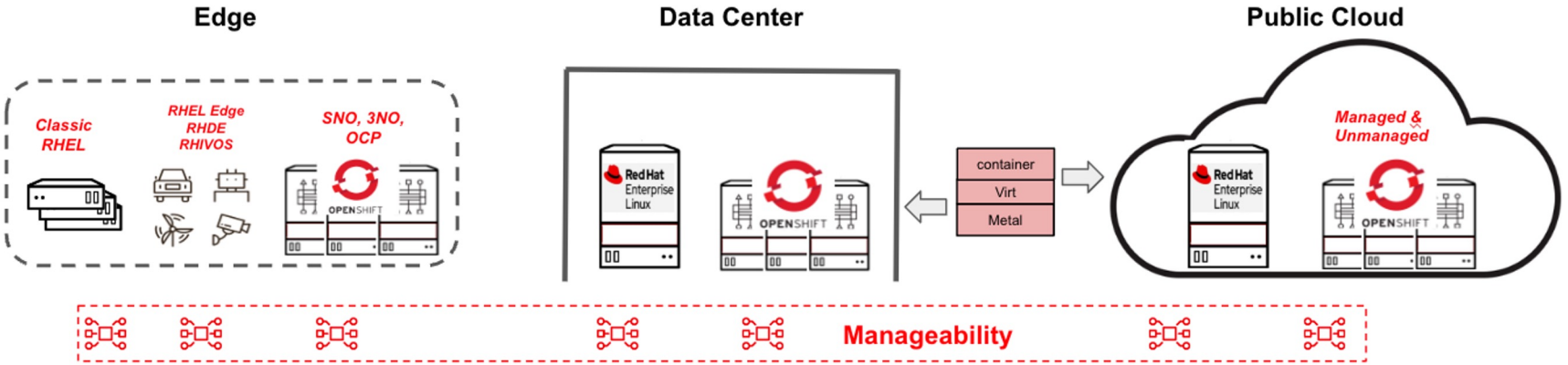
Management Capabilities

Lifecycle | Inventory | Configuration | Security | Automation | **Continuity** | Observability | Cost

Integration / Ecosystem

- Resilience
- Reliability
- Availability
- Supportability

Management Topology - Hybrid Infrastructure & Hybrid Cloud



Management Capabilities

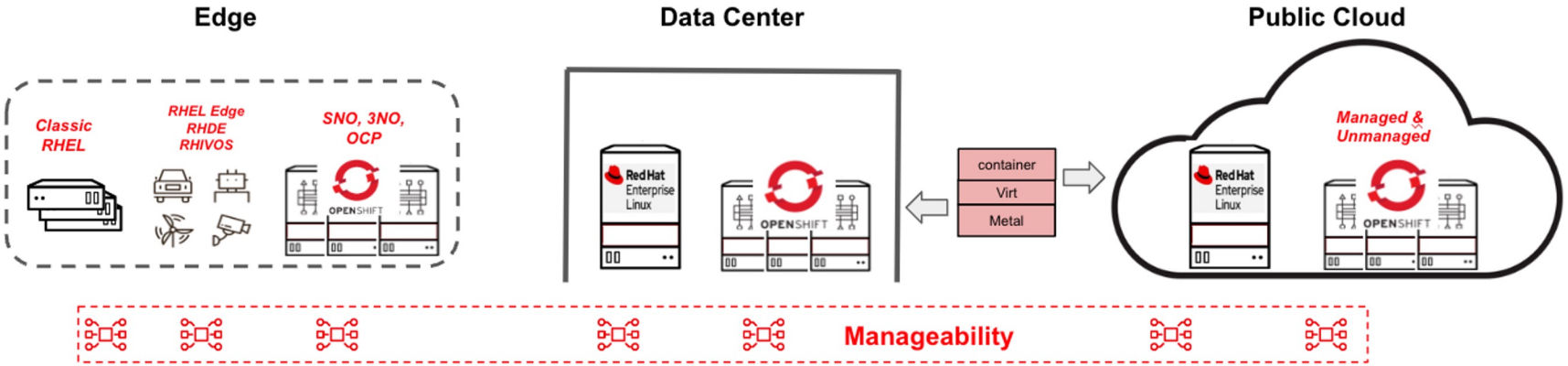
Integration / Ecosystem

Lifecycle | Inventory | Configuration | Security | Automation | **Continuity** | Observability | Cost

- Resilience
- Reliability
- Availability
- Supportability

Efficiency & Productivity

Security



Management Capabilities

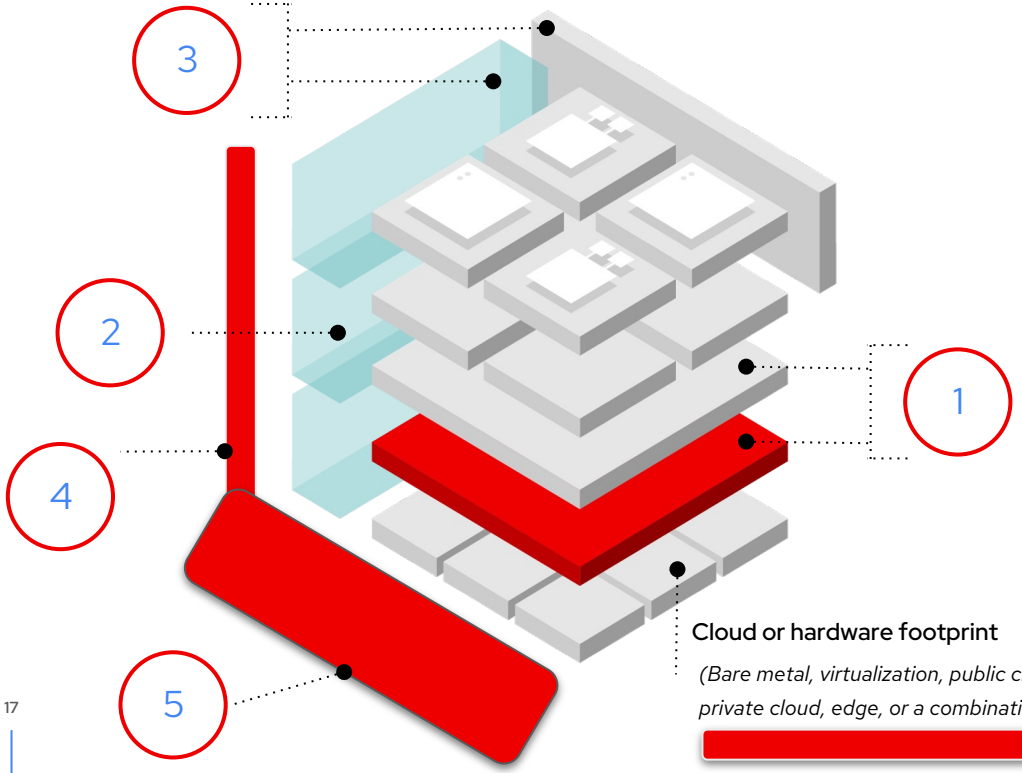
Integration / Ecosystem

Lifecycle | Inventory | Configuration | **Security** | Automation | Continuity | Observability | Cost

- Governance
- Risk
- Evidence
- Control

Security

Think of a layered approach for e2e security

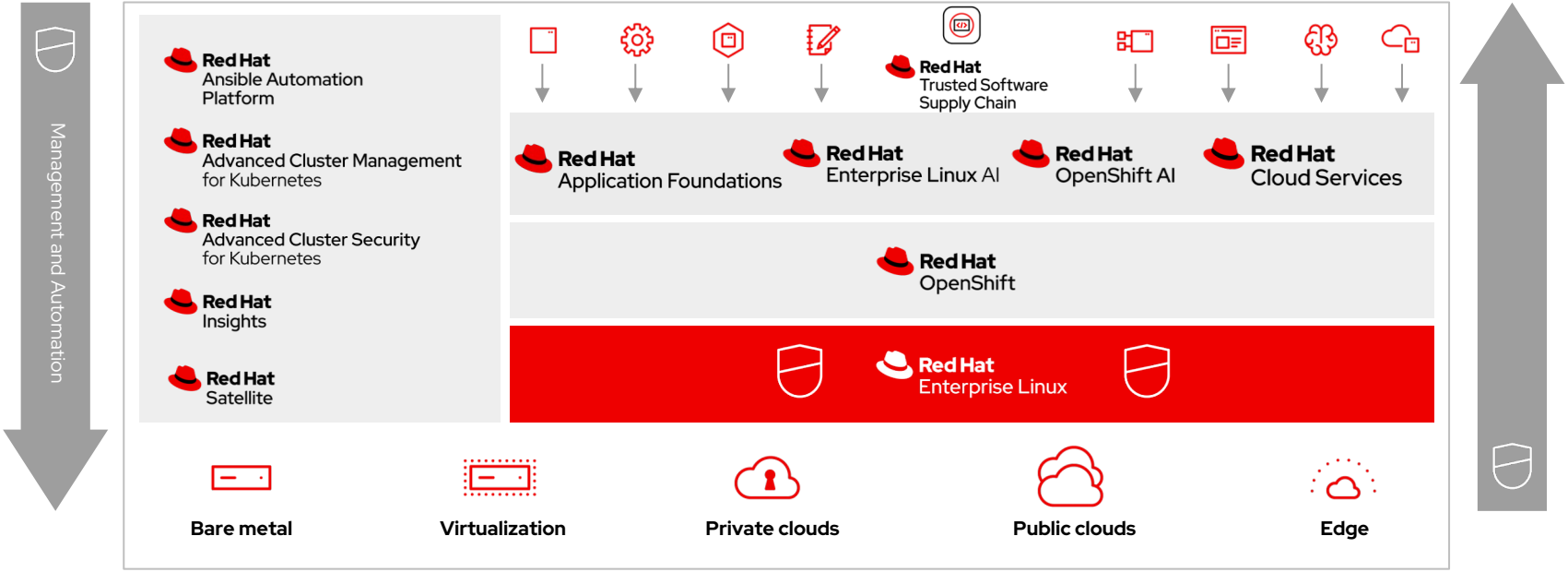


1. Strong, complete foundation
2. Trusted software supply chain
   DevSecOps practices
3. App-Dev Enablement
4. Manage, automate, secure, compliant
5. Reduce Cost and time, increase confidence in : Gov, Risk & Compliance
6. Confidential Computing

Red Hat

Layered security throughout the stack and lifecycle

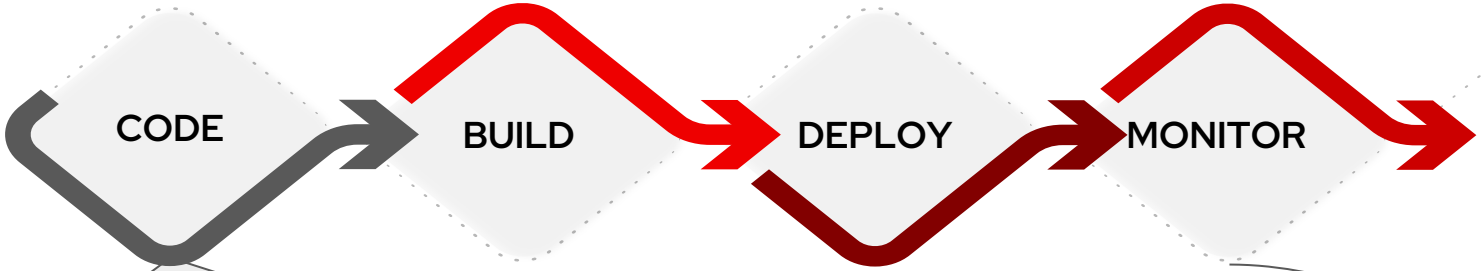
Build, deploy, and run applications on top of a hybrid cloud using DevSecOps practices



Red Hat

Application Lifecycle & Risk

Idea → Build → Deliver → Run → Govern



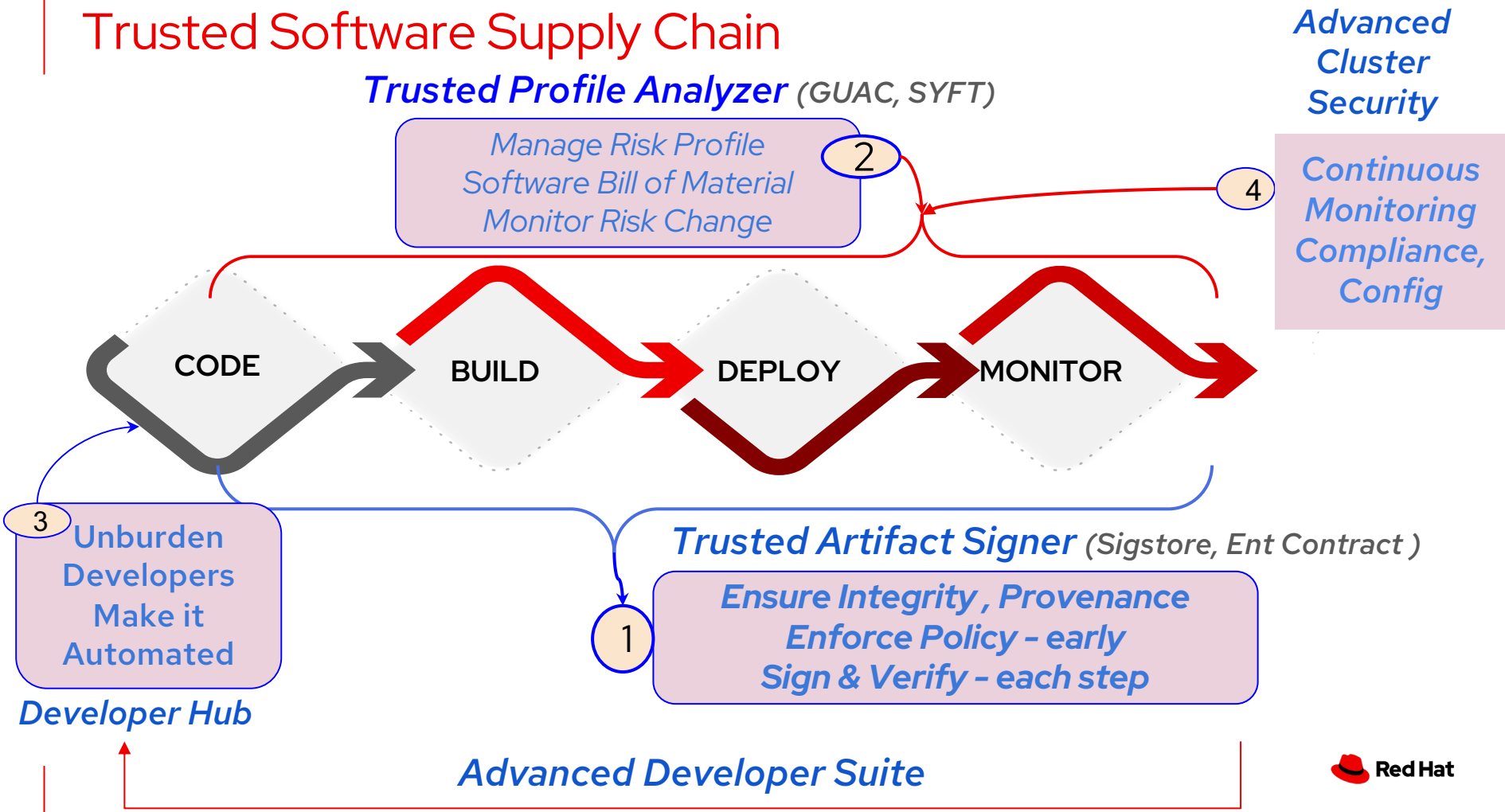
September 8, 2025 - 18 widely used npm packages - malicious code check-in using hacked maintainer account, ***2.6 billion downloads each week since 9/8/25***

Traditional Industry Focus

Year 2000 → 1000 CVE's → Year 2023 → 29000 CVE's

Red Hat

Trusted Software Supply Chain



Trusted Software Supply Chain

End to End Security Guardrails

CODE	BUILD	RELEASE	DEPLOY	MONITOR
Dependency Analytics	Reproducible Builds	SLSA Policy	Security Policy	Runtime
CVE & License	SBOM create and capture	Enforcement	Enforcement	Ongoing Registry
Policy Enforcement	Vulnerability Scanning	Signing Released	Signature Verification	Scanning
Sign & Verify	Provence Metadata	Artifact	(admission controller)	SBOM Analysis
	Signing & Attestation			

RH Trusted Profile Analyzer

RH Trusted Artifact Signer

RH Advanced Developer Suite

RH Advanced Cluster Security

Red Hat

Trusted Software Supply Chain - (

Trusted Content

Application Libraries

Language Runtime

Universal Base Image

Provenance, Attestation of Curated Content

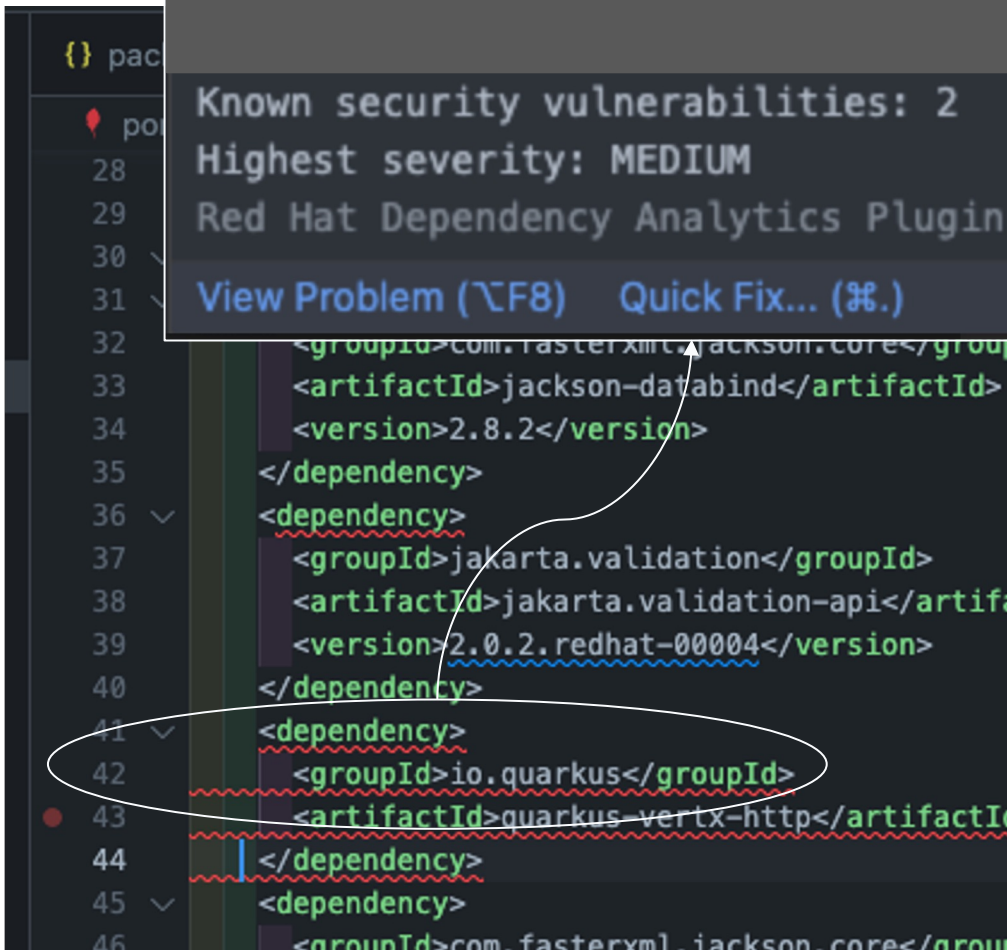
CODE

Dependency Analytics

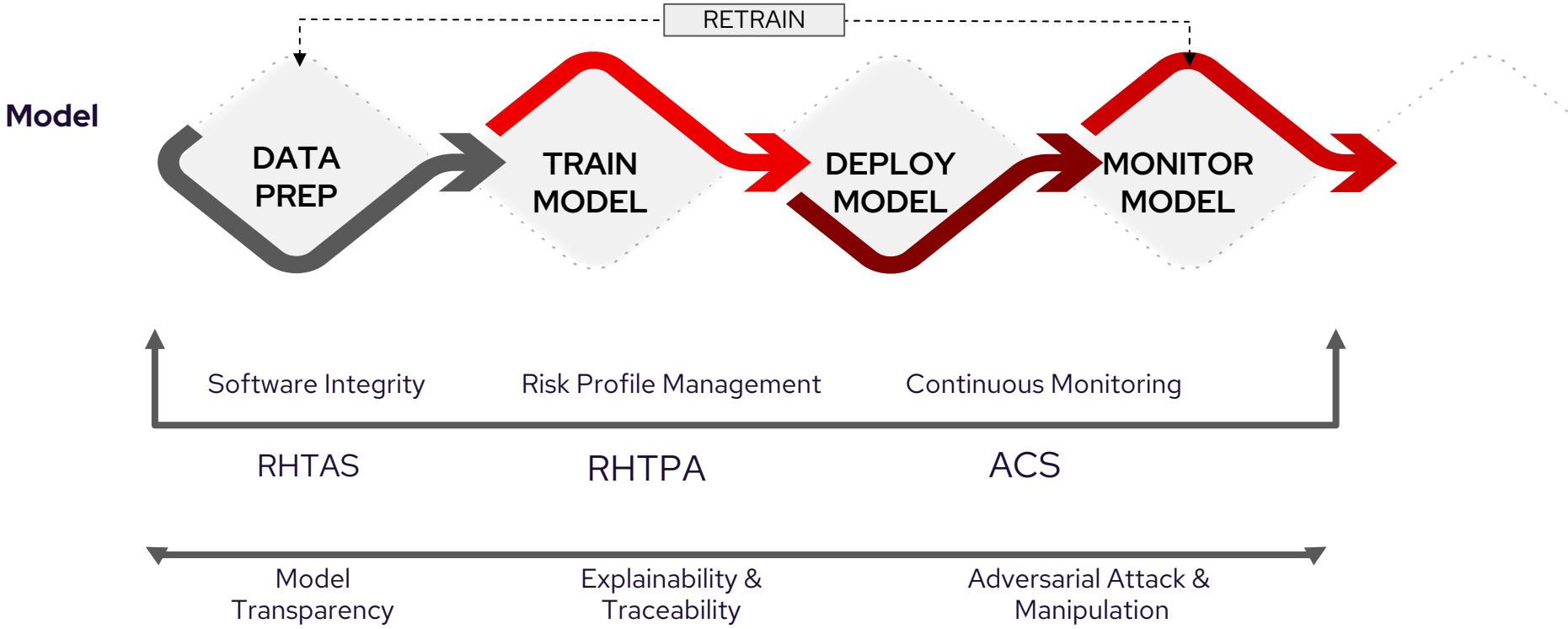
CVE & License

Policy Enforcement

Sign & Verify



Model Development Lifecycle



Red Hat

AI Safety & Security - GenAI

Security

Defending from malicious actors and adversaries

- Software Integrity - Tampering, modifications, Provenance, Data Lineage
- Risk Profile - Vulnerability & License, Malicious Pkg
- AI SBOM Trusted Content/Models
- Model stealing, Poisoning (prompt, data)

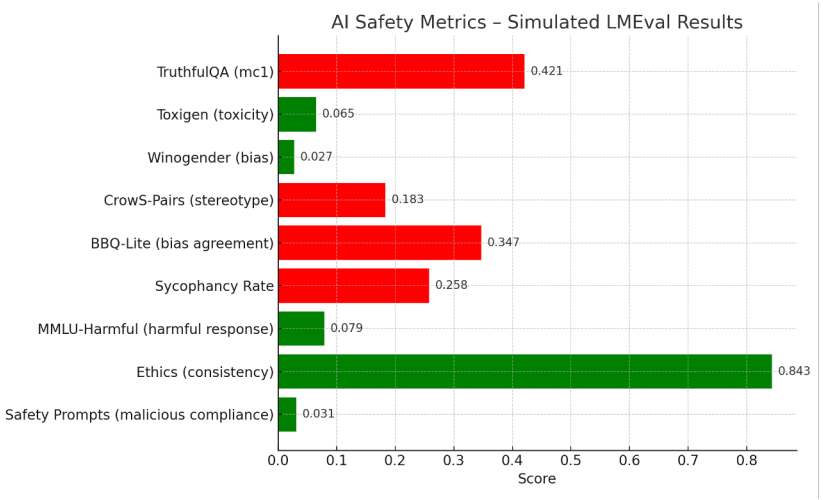
Safety

Preventing AI from causing unintentional harm

- Correctness & unintended behaviour
- Bias and Fairness
- Hateful Contents
- Explainability & Interpretability
- Hallucination/Misinformation
- PII, Data, System leakage

TrustyAI – LLM Eval : Model quality & explainability

AI Safety Context: **truthfulness**, **toxicity**, **bias**, and **reasoning errors**



Metric Descriptions:
- *TruthfulQA: Measures factual accuracy.*
- *Toxigen: Scores model's tendency to produce toxic content.*
- *Winogender: Tests gender bias in pronoun resolution.*
- *CrowS-Pairs: Evaluates stereotypical bias.*
- *BBQ-Lite: Tests agreement with biased assumptions.*
- *Sycophancy Rate: Measures blind agreement with user statements.*
- *MMLU-Harmful: Detects harmful content in multiple-choice responses.*
- *Ethics: Assesses alignment with ethical decisions.*
- *Safety Prompts: Checks for compliance with malicious instructions.*

- lm-eval --model gpt2 --tasks truthfulqa_mc,winogender,toxigen,sycophancy_qa

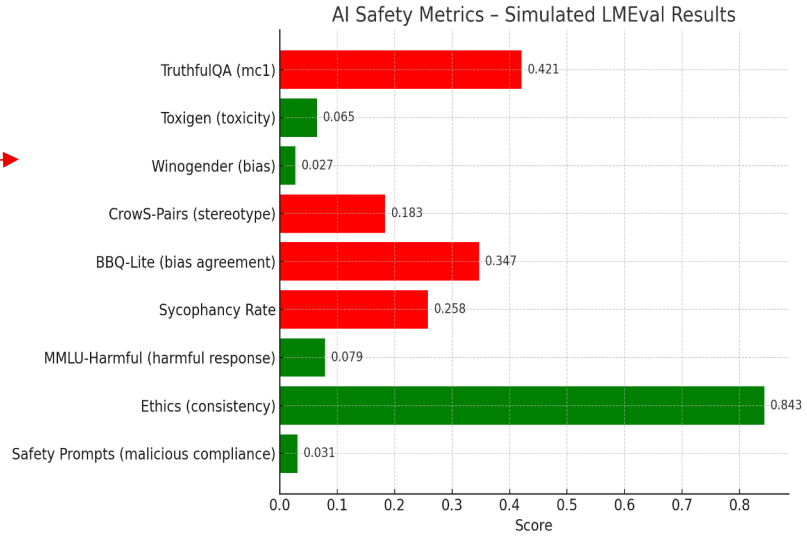
Red Hat

Red Hat Trusted Profile Analyzer- Dependency Analytics

llama-stack-tutorial / 1-models-add.py

Code | Blame | 35 lines (26 loc) · 886 Bytes

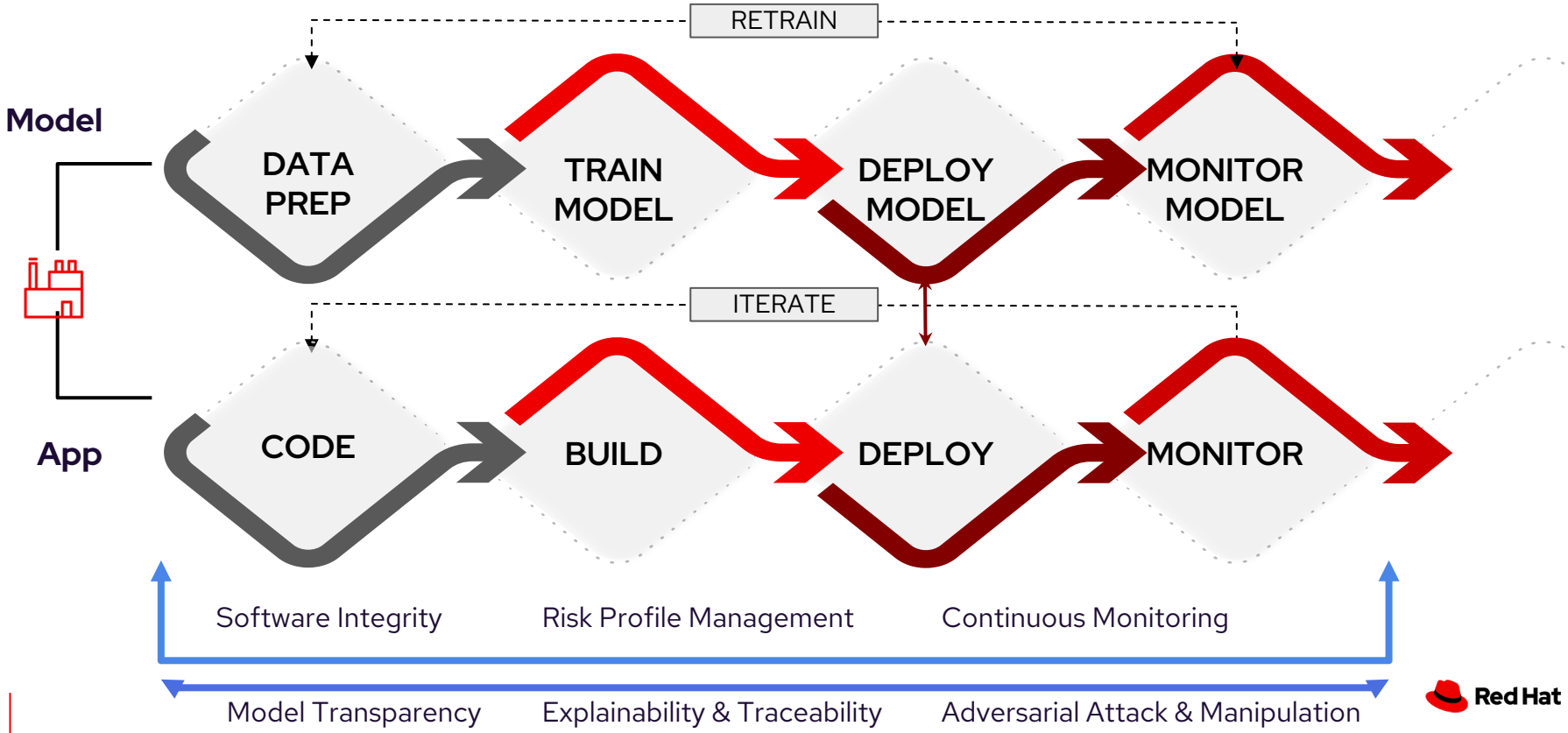
```
8
9   # Configure logging
10  logging.basicConfig(
11      level=logging.INFO,
12      format="%(asctime)s - %(levelname)s - %(message)s",
13      datefmt="%Y-%m-%d %H:%M:%S",
14  )
15  logger = logging.getLogger(__name__)
16
17  LLAMA_STACK_SERVER=os.getenv("LLAMA_STACK_SERVER")
18
19  from llama_stack_client import LlamaStackClient
20  client = LlamaStackClient(base_url=LLAMA_STACK_SERVER)
21  # from llama_stack import LlamaStackAsLibraryClient
22  # client = LlamaStackAsLibraryClient("ollama")
23  # client.initialize()
24
25
26  # Make sure to `ollama run llama3.1:8b-instruct-fp16 --keepalive 60m`
27
28  # Register a model
29  model = client.models.register(
30      model_id="meta-llama/Llama-3.1-8B-Instruct",
31      model_type="llm",
32      provider_id="ollama",
33      provider_model_id="llama3.1:8b-instruct-fp16",
34      metadata={"description": "llama3.1:8b-instruct-fp16 via ollama"}
35  )
```



Recommendation : Add **Output Shields Guardrails**

Content moderation (e.g., Detoxify, Perspective API): Toxicity, hate speech
Bias detection layers (CrowS-Pairs, Winogender): Gender, racial, religious bias
Ethical correctness modules: Unethical or harmful outputs

Software Development Life cycle with Model Development Lifecycle



Red Hat

Confidential Computing

Existing Encryption

Data At Rest

Data Encryption and System Attestation

- Protect Data on Disk using LUKS and Network Bound Disk Encryption (NBDE)
- Attest system state on boot, ensuring that system packages have not been compromised with IMA and Keylime
- Attest container workloads with Key Brokering Service (KBS)
- Ensure data remains unreachable in case of unauthorized access to the storage

Data In Motion

Encrypt Traffic Leveraging Strong, Future Proof Cryptography

- Protect data moving through the environment using strong, smart and validated cryptography
- Centralized management and establishment of secured connections native part of workflow for Red Hat Platform
- Automation provided allows consistent deployment and security configuration

New

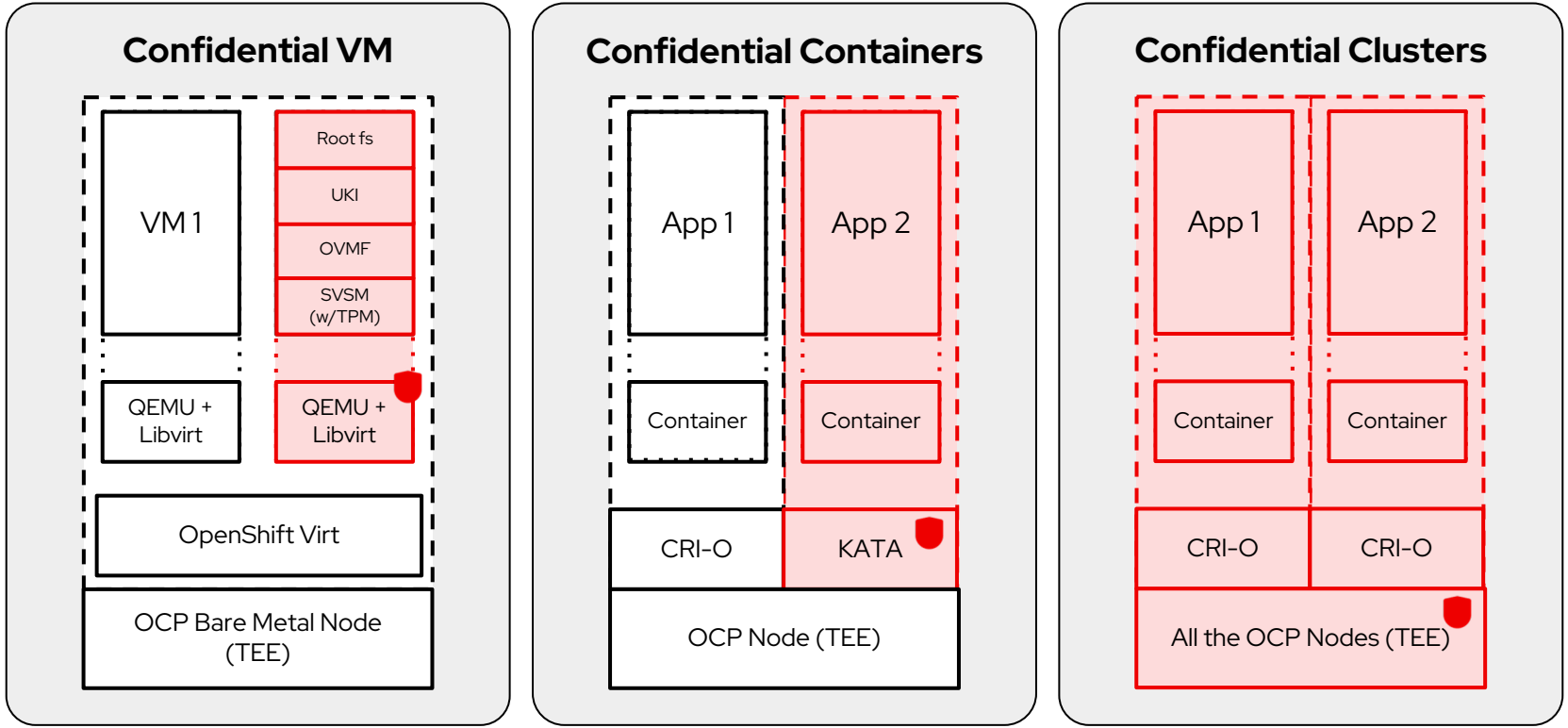
Data In Use

Confidential Computing Use Trusted Execution Environment Capabilities

- Protect data and workloads in use with Trusted Execution Environments as Confidential Computing is enabled on the major hardware platforms for AMD, Intel and NVIDIA
- Leverage these Trusted Execution Environments on prem or in the major cloud platforms
- Increases the security level of organizations that manage sensitive and regulated data

https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf

Trust Boundaries



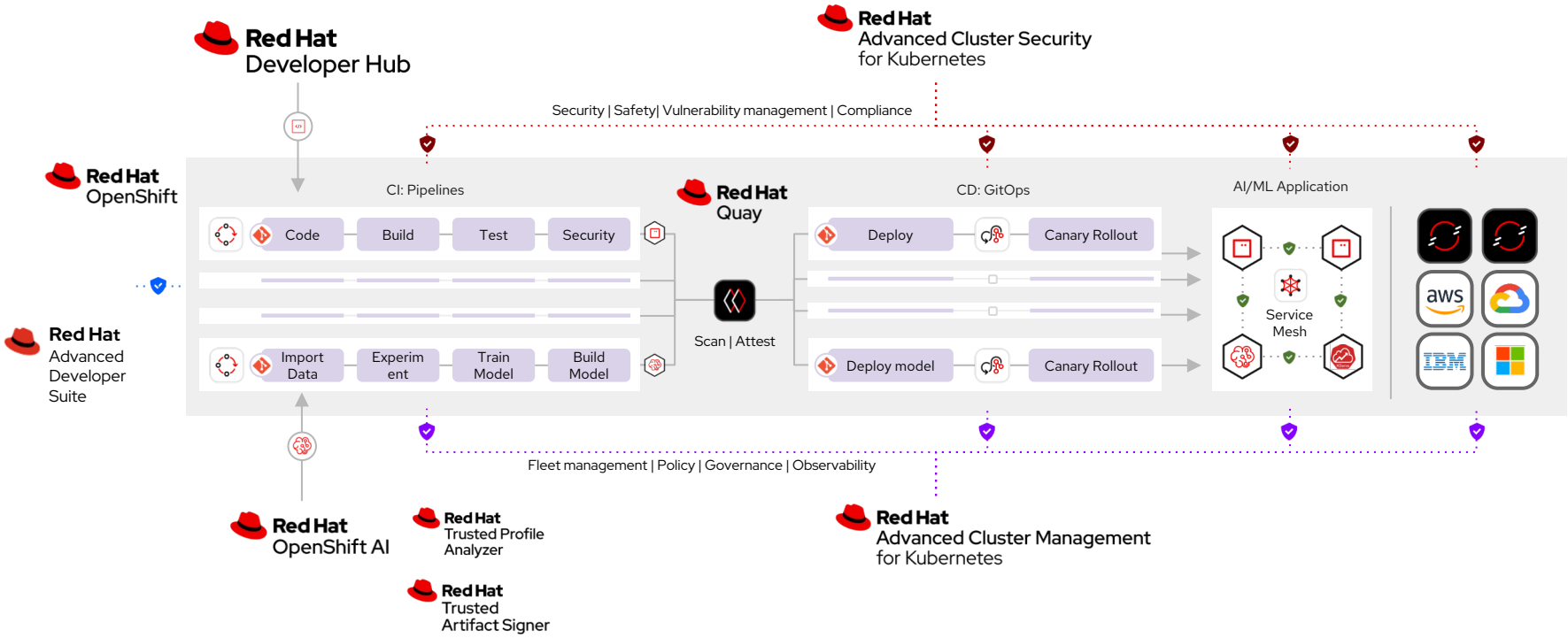
Customer

Confidential context - *Guest Owner*

Red Hat

Red Hat
Trusted Software
Supply Chain

Securely build, deploy, run applications at scale



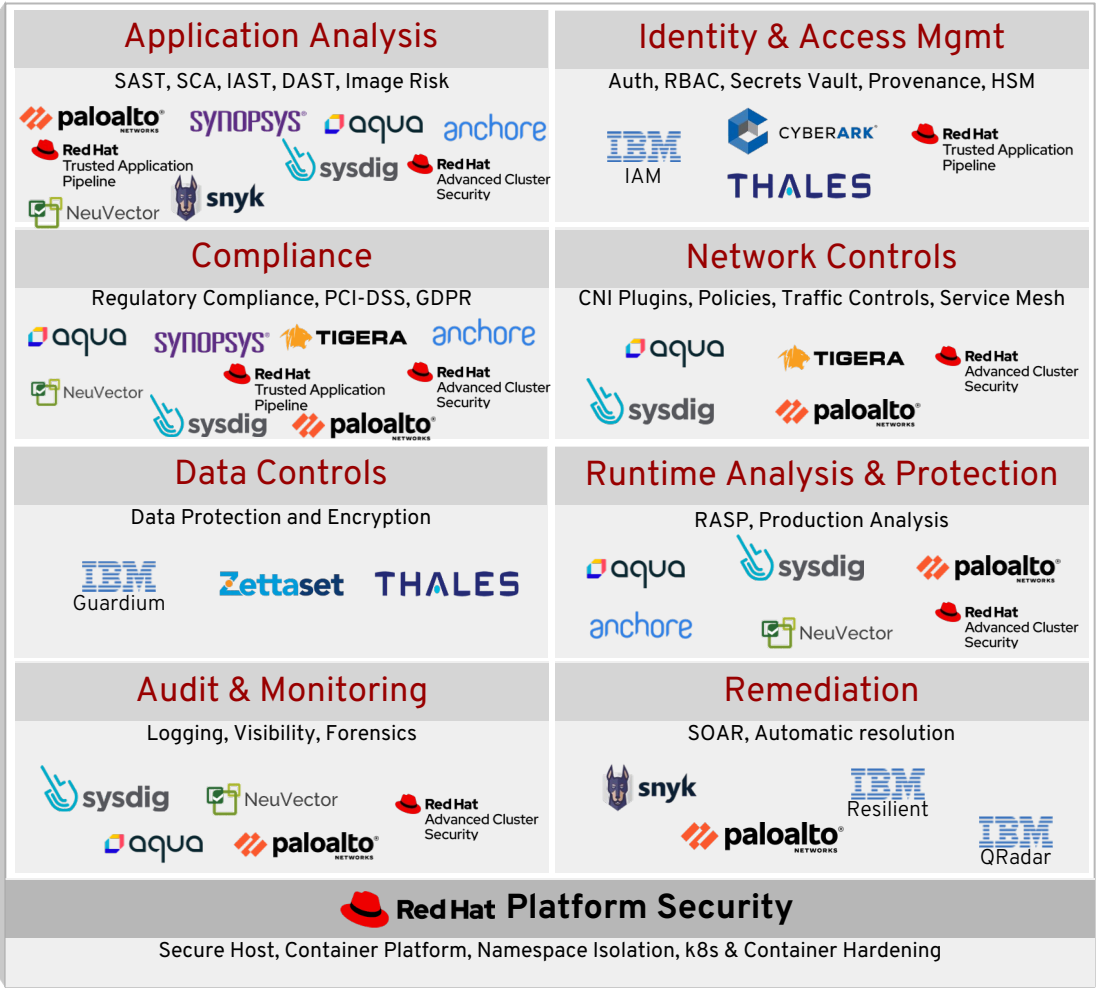
Red Hat

The Security Ecosystem

Partner Ecosystem extends and enhances Red Hat functionality

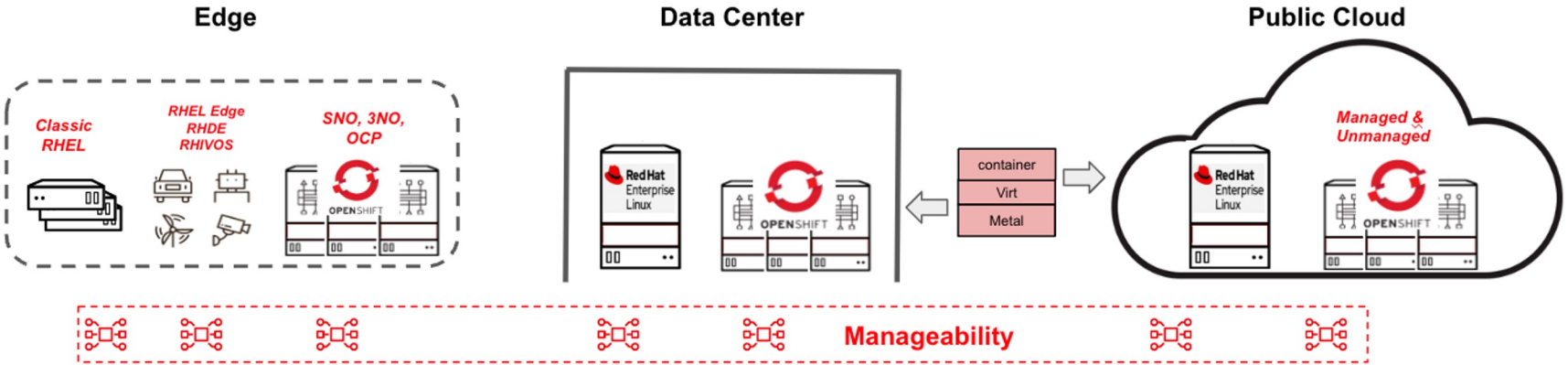
Easily add capability with IDE Plug-ins

Provide Developers a single interface with built-in security guardrails



Let’s draw a picture

Trust and Resilience in Modern Sovereign Infrastructure



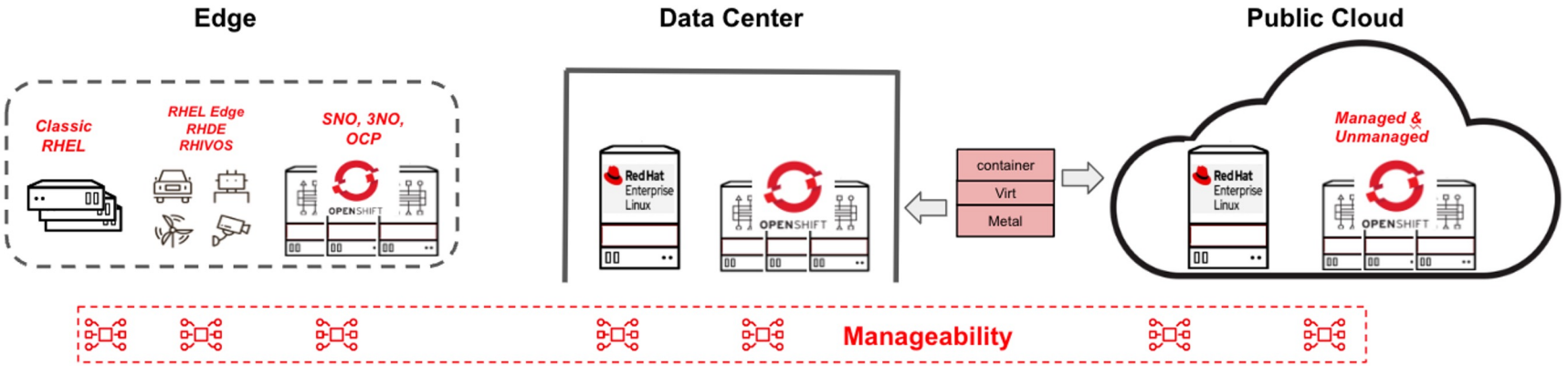
Management Capabilities

Lifecycle	Inventory	Configuration	Security	Automation	Continuity	Observability	Cost

Integration / Ecosystem

Operations
(IT Operators, Infrastructure Engineers, SREs, etc.)

Trust and Resilience in Modern Sovereign Infrastructure

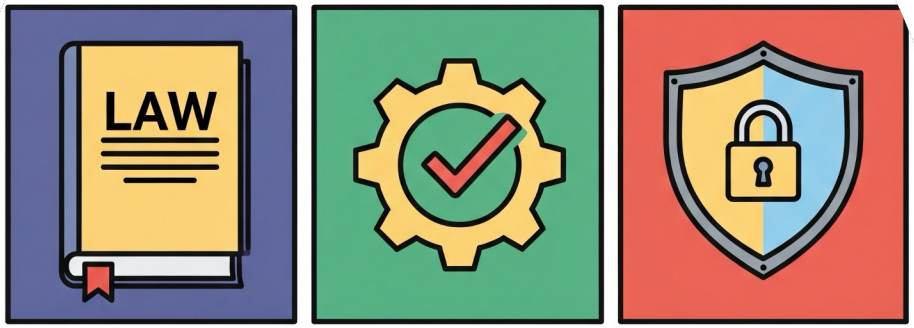


Management Capabilities

Lifecycle	Inventory	Configuration	Security	Automation	Continuity	Observability	Cost

Integration / Ecosystem

Operations
(IT Operators, Infrastructure Engineers, SREs, etc.)



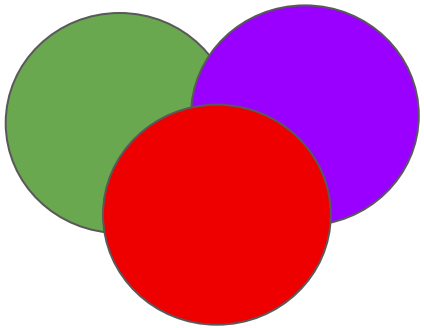
Regs, Comp, Sec

- Regulation sets the rules and requirements to be followed.
- Compliance ensures adherence to established regulations and policies.
- Security focuses on protecting systems and data from threats.
- Overlap exists as security posture often support compliance.

Red Hat

GRC is the driving force

Governance provides strategic oversight and direction.

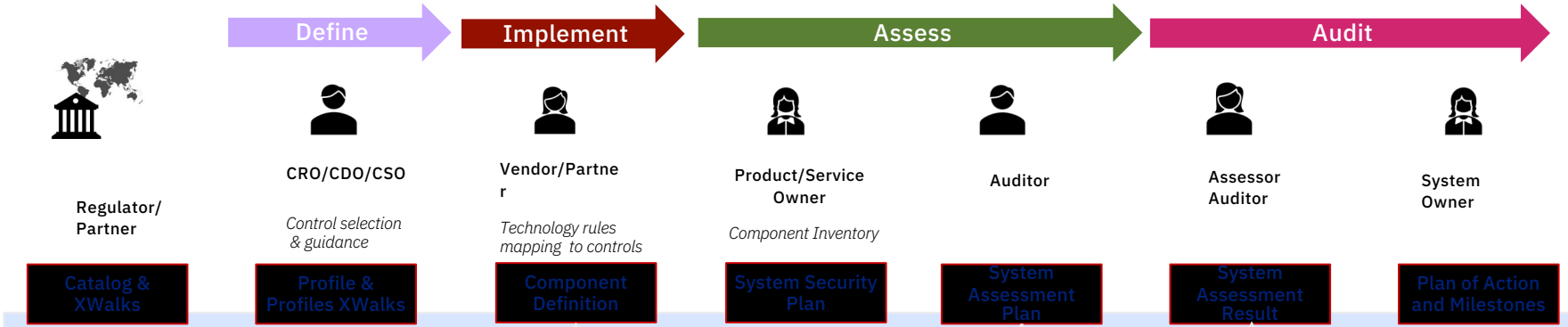


Risk management identifies and enables mitigations for potential threats.

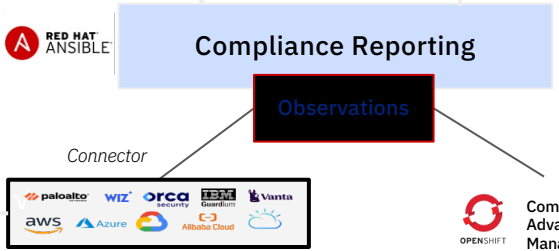
Compliance ensures adherence to rules and regulations.

Regulatory Compliance : Data / Process flow

Enhancing management tooling and integration patterns, enables reduction in friction for e2e posture delivery



Red Hat



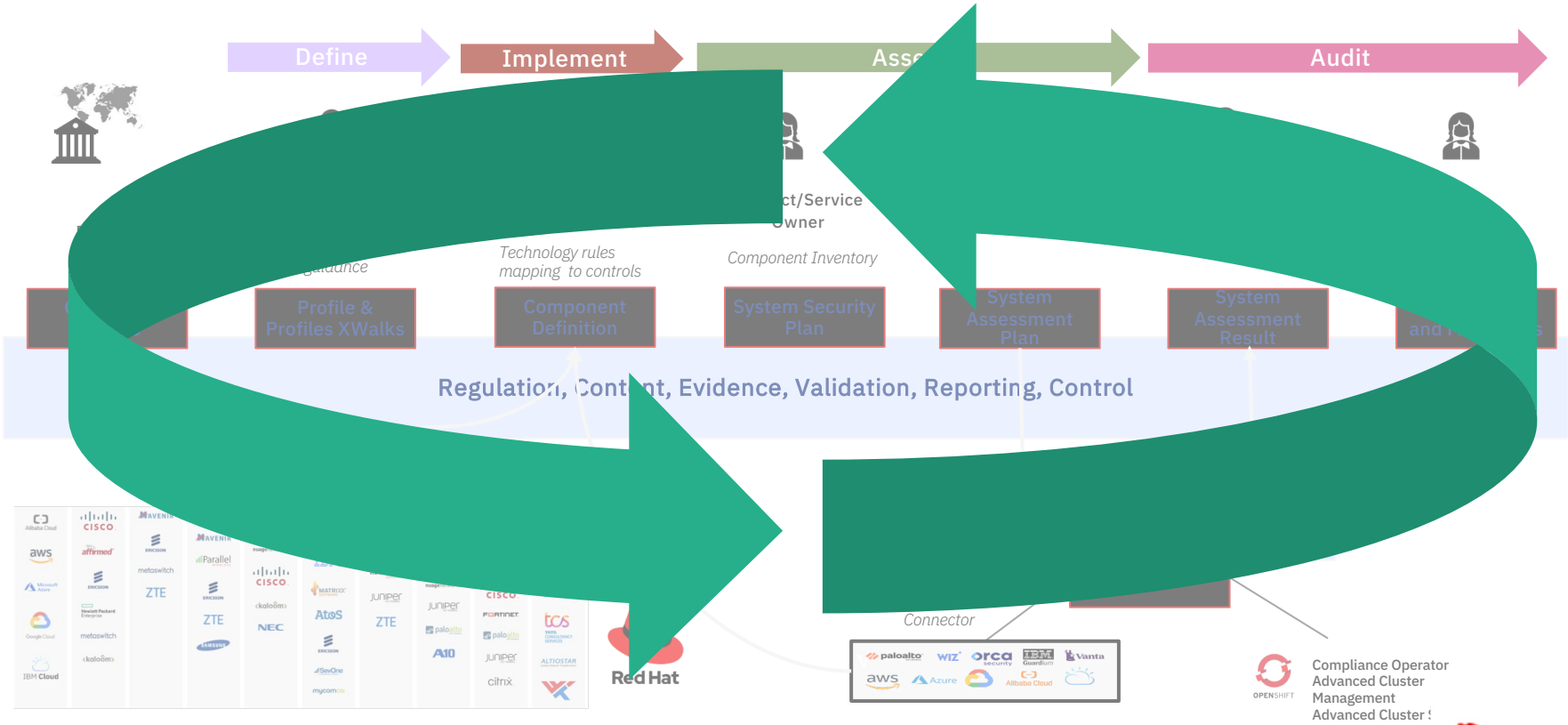
OPENSHIFT

Compliance Operator
Advanced Cluster Management
Advanced Cluster S

Red Hat

Regulatory Compliance : Data / Process flow

Enhancing management tooling and integration patterns, enables reduction in friction for e2e posture delivery



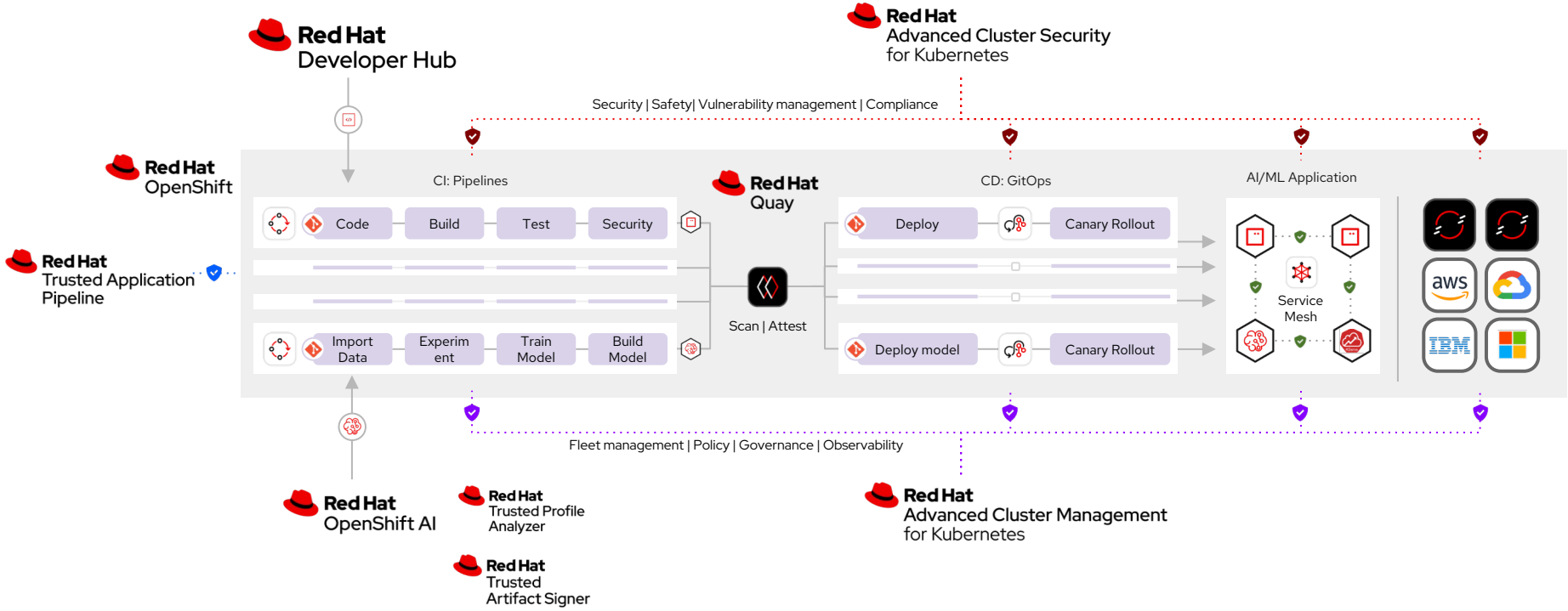
Red Hat

Two types of regulation controls

Process

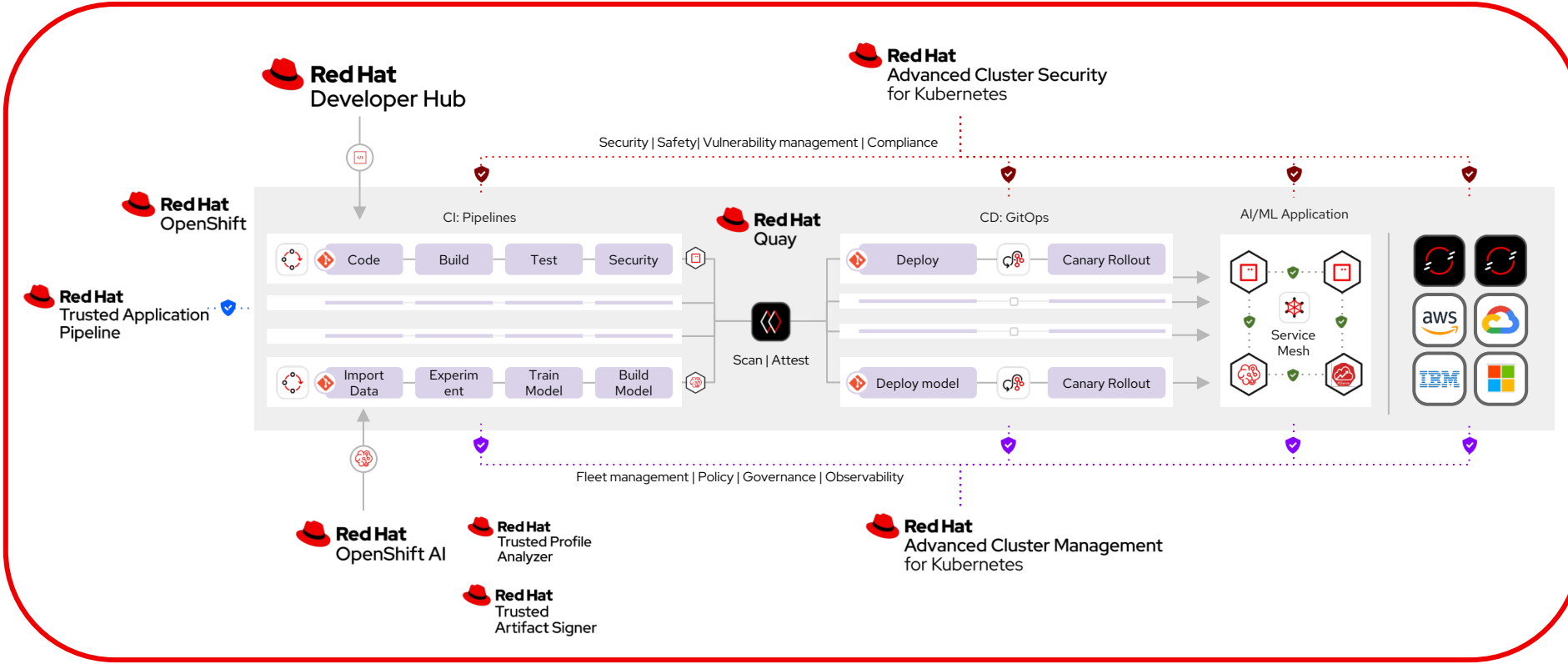
Qualified

Build, deploy & run at scale



Red Hat

Build, deploy & run at scale : in Boundary



Red Hat

EU Digital Operational Resiliency Act (EU-DORA)

Promoting the economic sovereignty of the EU by protecting its financial sector from external threats

- **Risk Management** [1] → Detection, recovery, business continuity policies and disaster recovery plans
- **Incident Management**[2] **and Intelligence sharing** [5] → NIS Directive, cybersecurity & (harmonised) reporting
- **Digital Operational Resilience Testing** [3] → Concentration risk analysis, pen testing including remediation plans
- **ICT third-party risk** [4] → Critical ICT 3rd parties subject to an EU oversight framework
  - amazon web services
  - Microsoft Azure
  - Google Cloud
  - IBM Cloud
- **Exit-Strategy** [6]

"Consolidate and upgrade ICT (information and communications technology) risk requirements across the financial entities to ensure all are subject to a common set of standards to mitigate ICT risks."

Source: DORA Proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1

(1) Section II- art 5-14
(2) Section III- art 15-20
(3) Section IV- art 21-24
(4) Section V- art 25-39
(5) Section VI- art 40
(6) Section V- art 25-27

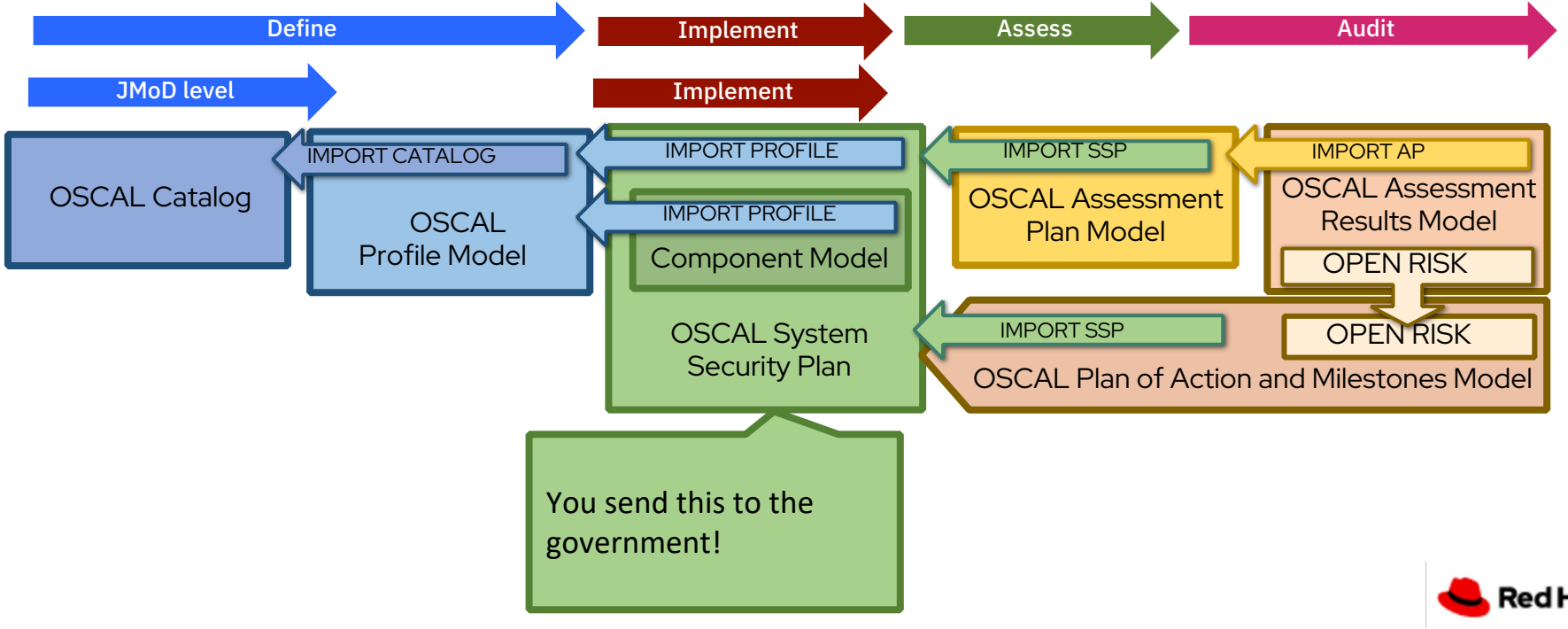
NIST 800 53 : Security and Privacy Controls for Information Systems and Organisations

- **AC**: Access Control
- **AT**: Awareness and Training
- **AU:** Audit And Accountability
- **CM**: Configuration Management
- **CP**: Contingency Planning
- **AI**: Identification and Authentication
- **IR**: Incident Response
- **MA**: Maintenance
- **MP**: Media Protection
- **PS**: Personnel Security
- **PT**: PII Processing and Transparency
- **PE**: Physical and Environmental Protection
- **PL**: Planning
- **PM**: Program Management
- **RA**: Risk Assessment
- **CA**: Security Assessment and Authorization
- **SC**: System and Communications Protection
- **SI**: System and Information Integrity
- **SA**: System and services acquisition
- **SCRM**: Supply Chain Risk Management

Definition at https://github.com/usnistgov/oscal-content/tree/main/nist.gov/SP800-53

OSCAL Makes It Manageable

OSCAL provides a higher level data models designed for cloud compliance

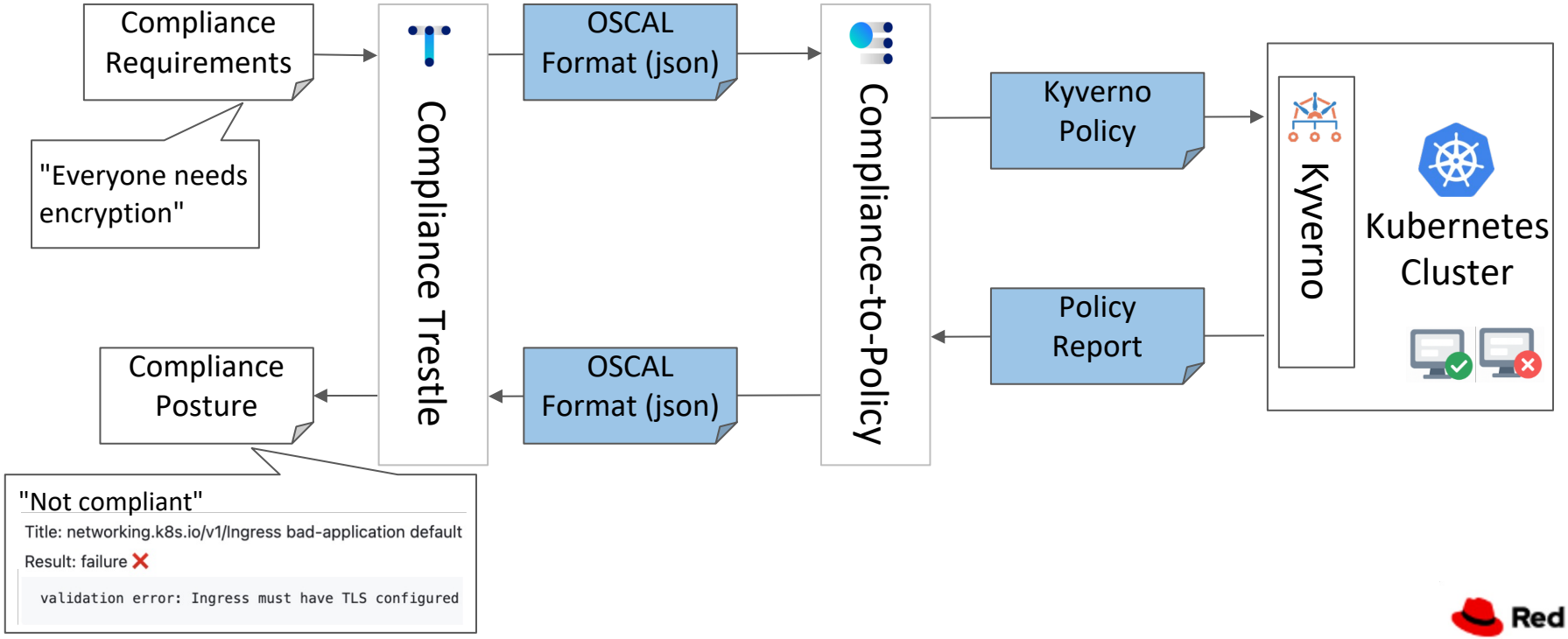


Red Hat

From Compliance Requirement to Policy Enforcement

Handle bidirectional conversion between human-readable formats and OSCAL

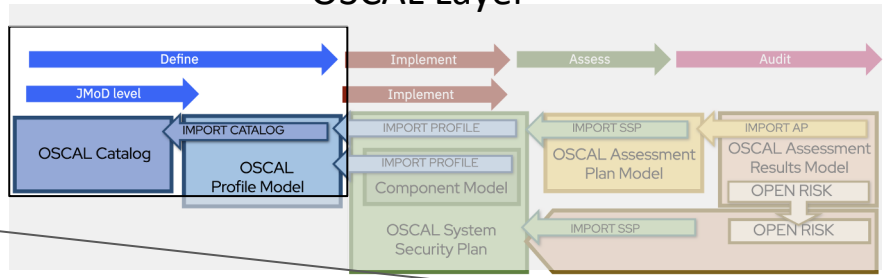
Bridge OSCAL and actual enforcement (Kyverno), and feeds the result back into OSCAL.



Red Hat

NIST 800-53 Catalog for Encryption Control

OSCAL Layer




```
{
 "id": "sc-13",
 "class": "SP800-53",
 "title": "Cryptographic Protection",
 "params": [{
     "id": "sc-13_prm_1",
     "label": "organization-defined cryptographic uses"
   },{
     "id": "sc-13_prm_2",
     "label": "organization-defined types of cryptography for each specified cryptographic use"
   }],
 "parts": [{
   "id": "sc-13_smt",
   "name": "statement",
   "parts": [{
       "id": "sc-13_smt.a",
       "name": "
       "props":
           "name
           "valu
         }],
       "prose":
     },{
       "id": "sc
       "name": "
       "props":
           "name
           "value
         }],
       "prose": "Implement the following types of cryptography required for each specified cryptographic use: {{ insert: param, sc-13_prm_2 }}.
       "
     }]
   },{
     "id": "sc-13_gdn",
     "name": "guidance",
     "prose": "Cryptography c
     controlled unclassified
     separation when authoriz
     also be used to support
     cryptography and NSA-app
     NSA-approved cryptograph
     cryptography. Cryptograp
     standards, and guidelines."
   }]
}
```



```
"id": "sc-13",
"class": "SP800-53",
"title": "Cryptographic Protection",
```



```
"prose": "Implement the following types of cryptography required for each specified cryptographic use: {{ insert: param, sc-13_prm_2 }}."
```

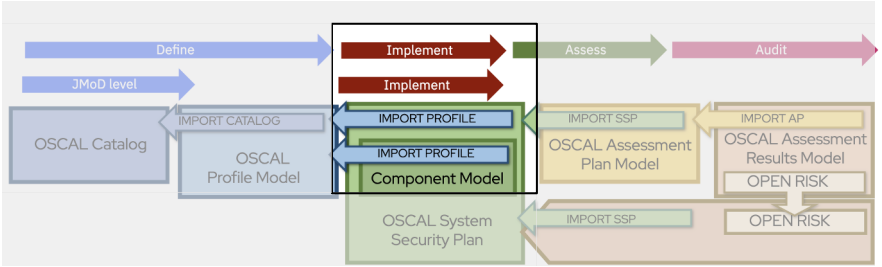

Red Hat

Implementation of Enforcement Policy

Here is the Kyverno Policy to enforce TLS configuration on Ingress

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: enforce-tls-on-ingress
spec:
  validationFailureAction: Enforce
  background: true
  rules:
    - name: require-tls
      match:
        resources:
          kinds:
            - Ingress
      mutate:
        patchStrategicMerge:
          metadata:
            annotations:
              nginx.ingress.kubernetes.io/force-ssl-redirect: "true"
          spec:
            tls:
              - secretName: my-cert
```

OSCAL Layer



Target is Ingress

```yaml
match:
  resources:
    kinds:
      - Ingress
```

Mutating annotation and tls secret field

```yaml
patchStrategicMerge:
  metadata:
    annotations:
      nginx.ingress.kubernetes.
      io/force-ssl-redirect:
      "true"
  spec:
    tls:
      - secretName: my-cert
```

EU cyber resilience Act

December 10, 2024

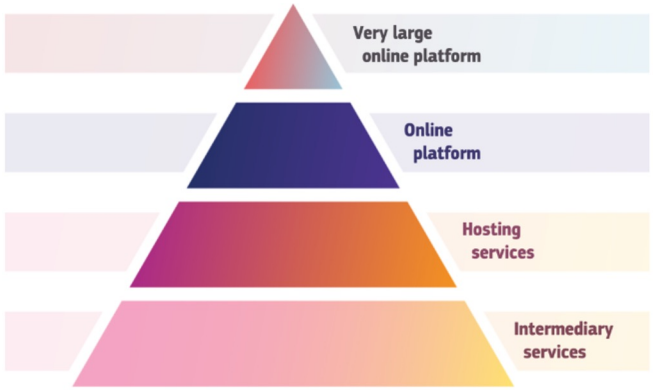
- Secure by design
- Enforced Lifecycle
- Clear, complete Vulnerability Mgmt
- Deliver use-case models
- Compliance ready
- Transparency in origin : SBOM
- Enforced Ownership
- Assured Resilience

- Applies to everyone who has an interest in EU
- All content is in boundary
- Standards are required
- Build to intended use is now required

Red Hat

EU Digital Services Act

- Transparency : Process, Code, Content, Adverts
- Risk Assessment and Regulator Control
- 6% of the global revenue : Penalty



EU Network and Information Systems Directive 2

- Focused on cyber security for core infra
- Process focused : incident handling, network security etc
- Procedures for cryptography and encryption
- Enforces people centric context: eg Auth

Red Hat

EU Cyber Solidarity Act

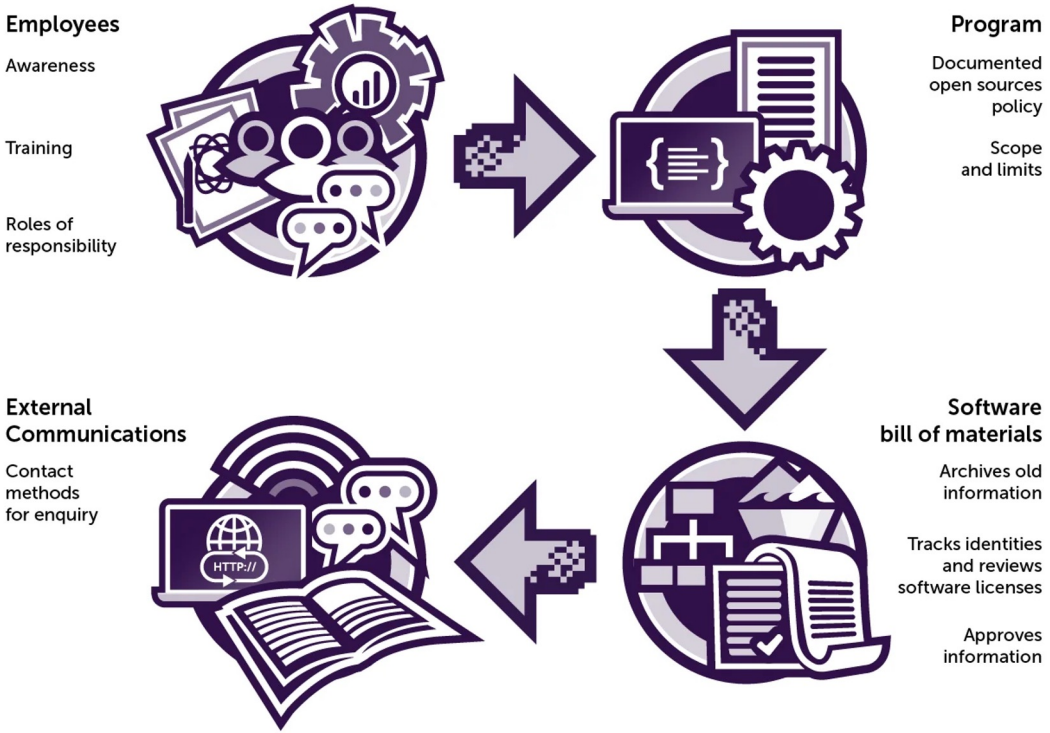
Q1 / 2025

Red Hat

In Germany, the Product Liability Act (ProdHaftG) is being updated to explicitly include software as a product

Red Hat

License Compliance is not a regulation context

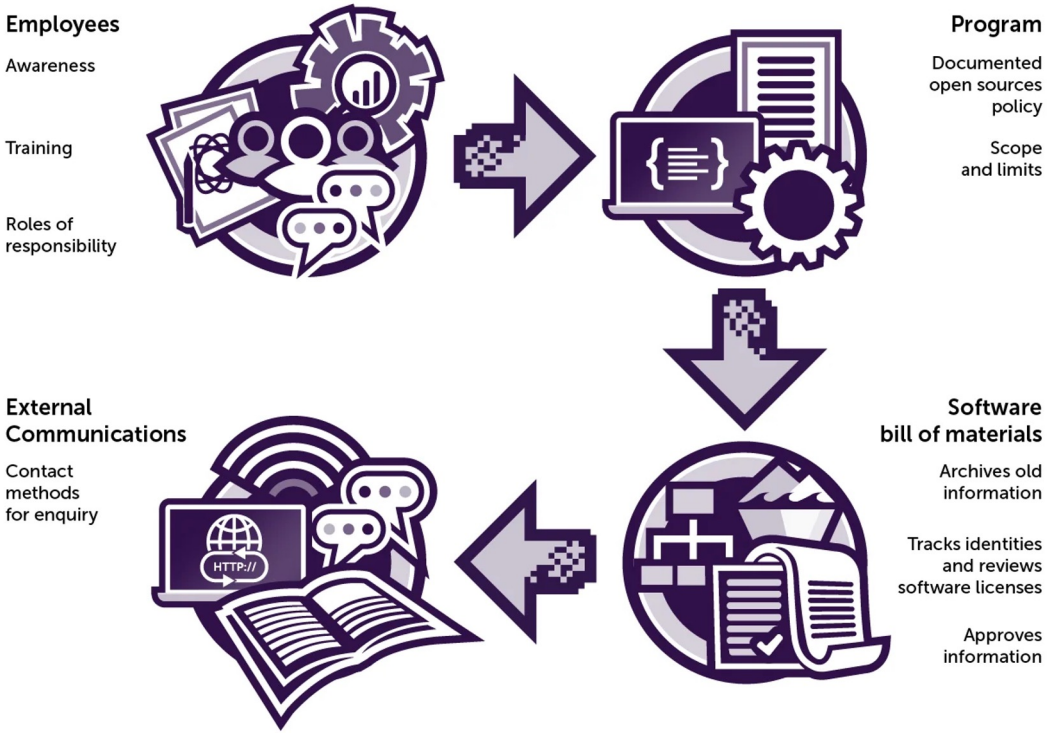


The OpenChain project aims to formalise and deliver compliance program and tools for License focused Compliance posture

Red Hat

License Compliance is

regulation context



The OpenChain project aims to formalise and deliver compliance program and tools for License focused Compliance posture

Red Hat

As an Open Source developer

- Safety is everyone's concern
- Security is everyone's concern
- Maintainability is a concern
- Evidence generation is key
- Provenance should be assured

- Data privacy is a challenge
- Vulnerability can have severe consequences
- Open can imply lower barrier for APT
- Transactions need confidence

Key Takeaways & Considerations

- Open source has a vital role in regulated environments.
- Safety and security start at inception
- Understanding regulations is crucial for developers.
- Evidence generation and provenance are key.
- Standards enable a rapidly maturing open source compliance tools .

Karanbir Singh, Senior Distinguished Engineer, Red Hat (UK) Ltd, https://uk.linkedin.com/in/karanbirsingh