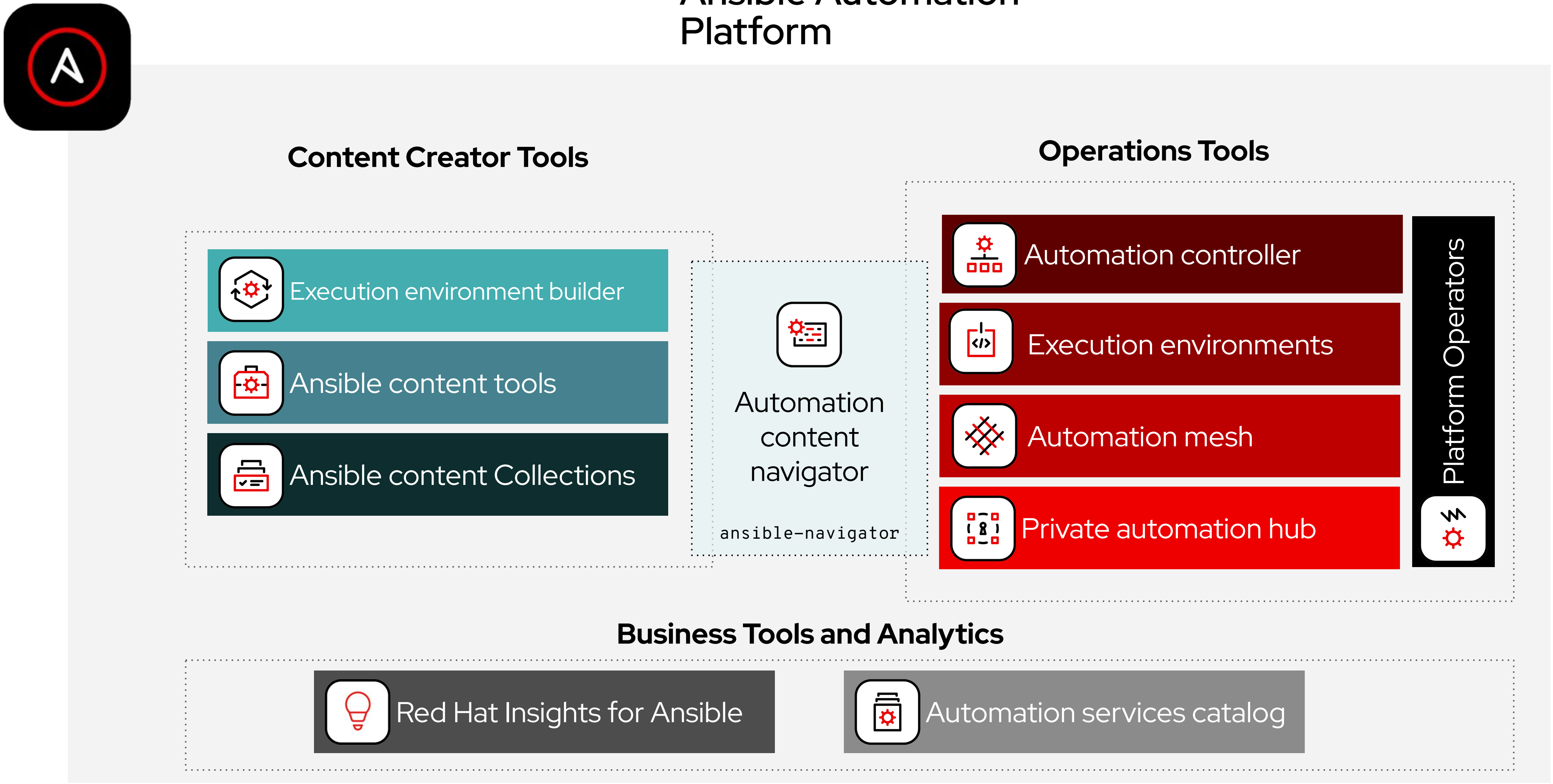
Ansible Automation Platform: Private Automation Hub

Securing the Automation Supply Chain

Presented by:

Jay Ryan

Red Hat
Ansible Automation Platform



Content Creator Tools

- Execution environment builder
- Ansible content tools
- Ansible content Collections

Automation content navigator

```
ansible-navigator
```

Operations Tools

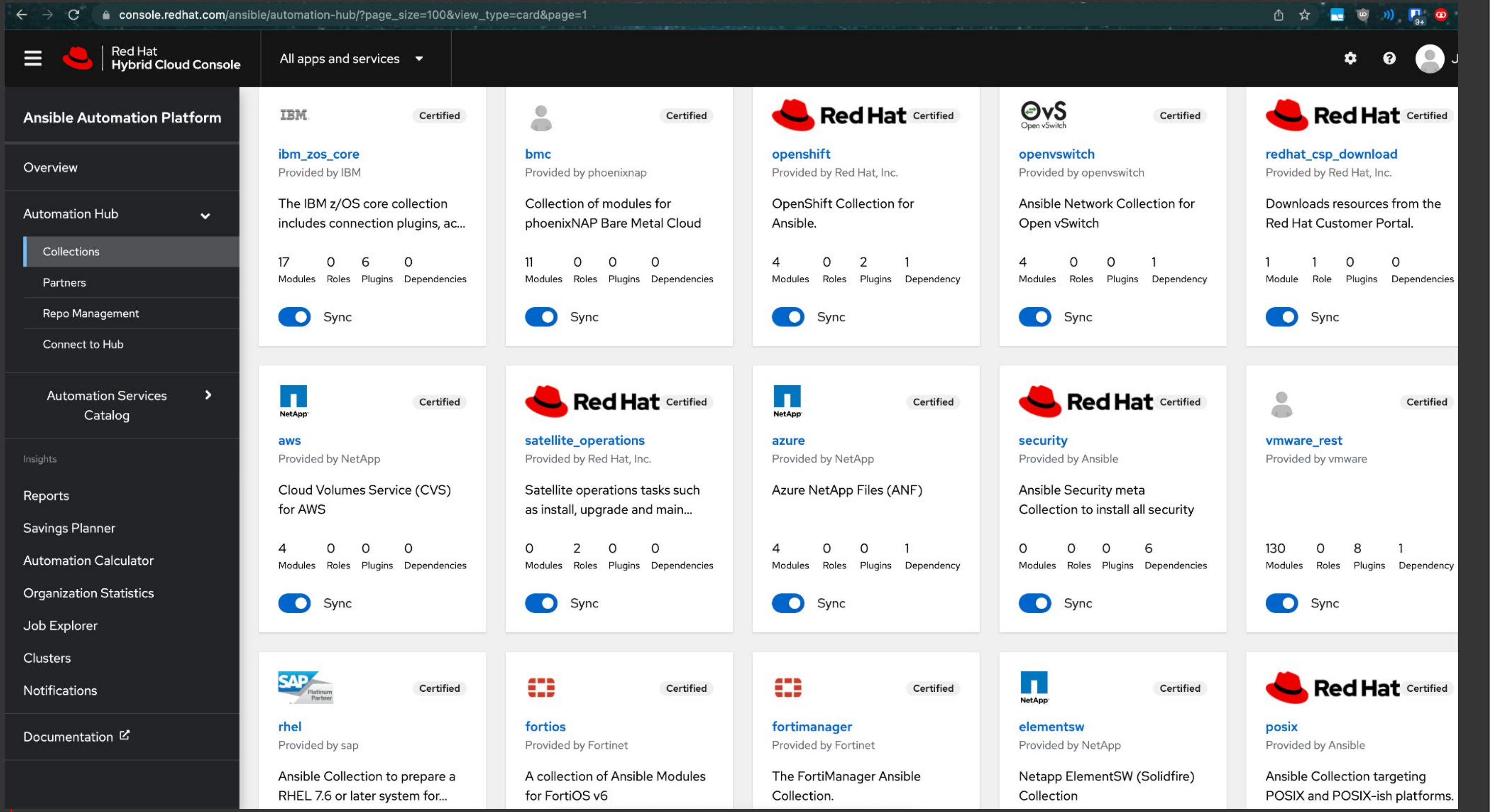
- Automation controller
- Execution environments
- Automation mesh
- Private automation hub

Platform Operators

Business Tools and Analytics

- Red Hat Insights for Ansible
- Automation services catalog

Ansible Automation Hub



console.redhat.com/ansible/automation-hub/?page_size=100&view_type=card&page=1

ibm_zos_core (Certified)
Provided by IBM
The IBM z/OS core collection includes connection plugins, ac...
17 Modules 0 Roles 6 Plugins 0 Dependencies
Sync

bmc (Certified)
Provided by phoenixnap
Collection of modules for phoenixNAP Bare Metal Cloud
11 Modules 0 Roles 0 Plugins 0 Dependencies
Sync

openshift (Certified)
Provided by Red Hat, Inc.
OpenShift Collection for Ansible.
4 Modules 0 Roles 2 Plugins 1 Dependency
Sync

openvswitch (Certified)
Provided by openvswitch
Ansible Network Collection for Open vSwitch
4 Modules 0 Roles 0 Plugins 1 Dependency
Sync

redhat_csp_download (Certified)
Provided by Red Hat, Inc.
Downloads resources from the Red Hat Customer Portal.
1 Module 1 Role 0 Plugins 0 Dependencies
Sync

aws (Certified)
Provided by NetApp
Cloud Volumes Service (CVS) for AWS
4 Modules 0 Roles 0 Plugins 0 Dependencies
Sync

satellite_operations (Certified)
Provided by Red Hat, Inc.
Satellite operations tasks such as install, upgrade and main...
0 Modules 2 Roles 0 Plugins 0 Dependencies
Sync

azure (Certified)
Provided by NetApp
Azure NetApp Files (ANF)
4 Modules 0 Roles 0 Plugins 1 Dependency
Sync

security (Certified)
Provided by Ansible
Ansible Security meta Collection to install all security
0 Modules 0 Roles 0 Plugins 6 Dependencies
Sync

vmware_rest (Certified)
Provided by vmware
130 Modules 0 Roles 8 Plugins 1 Dependency
Sync

rhel (Certified)
Provided by sap
Ansible Collection to prepare a RHEL 7.6 or later system for...

fortios (Certified)
Provided by Fortinet
A collection of Ansible Modules for FortiOS v6

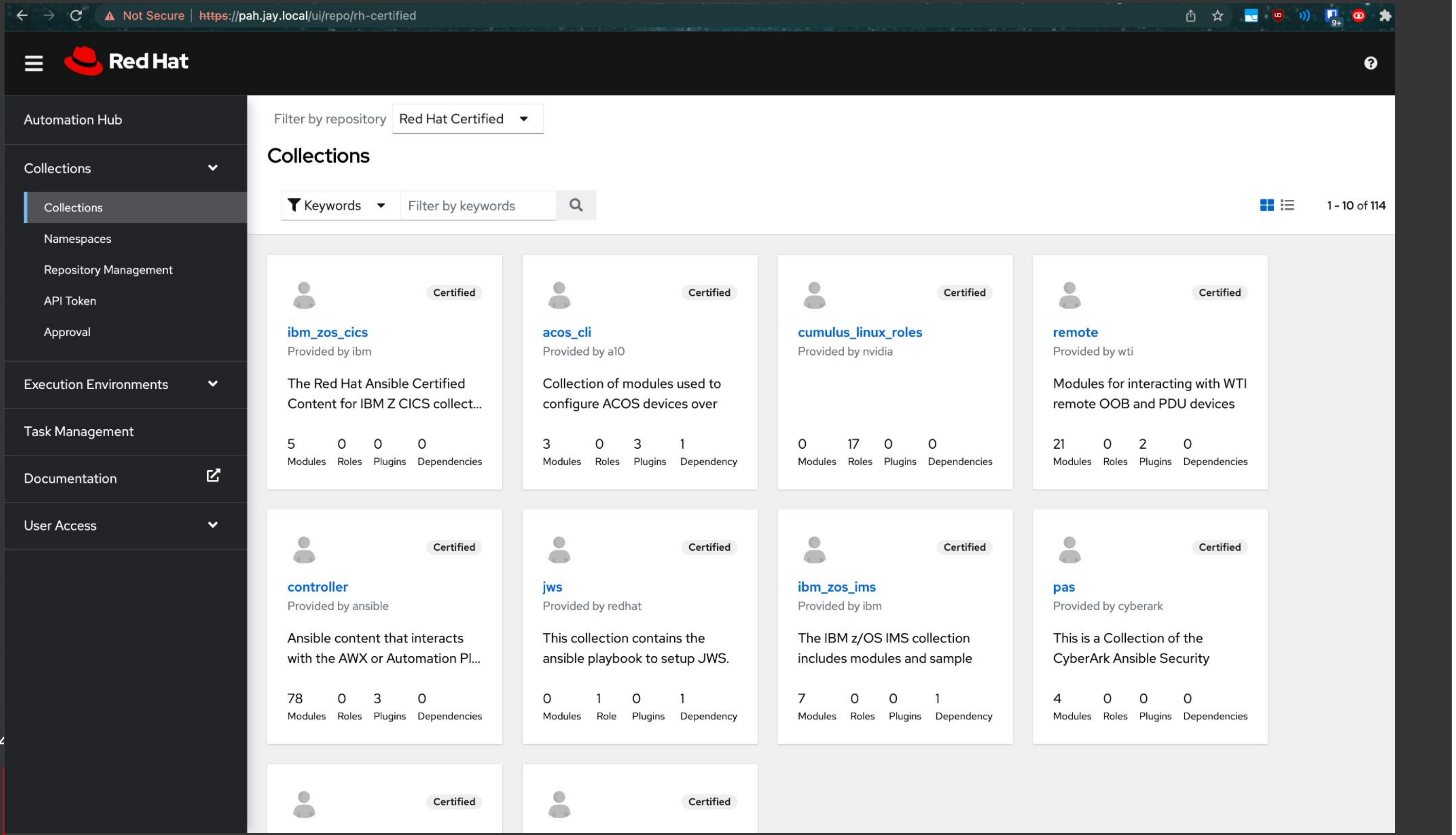
fortimanager (Certified)
Provided by Fortinet
The FortiManager Ansible Collection.

elementsw (Certified)
Provided by NetApp
Netapp ElementSW (Solidfire) Collection

posix (Certified)
Provided by Ansible
Ansible Collection targeting POSIX and POSIX-ish platforms.

- Certified Content (118 collections)
- Jointly supported by Red Hat and Partners
- “Stable and supported”

Private Automation Hub



Automation Hub

Collections
- Collections
- Namespaces
- Repository Management
- API Token
- Approval

Execution Environments

Task Management

Documentation

User Access

Filter by repository: Red Hat Certified

Collections

Keywords | Filter by keywords | 1 - 10 of 114

ibm_zos_cics (Certified)
Provided by ibm
The Red Hat Ansible Certified Content for IBM Z CICS collect...
5 Modules, 0 Roles, 0 Plugins, 0 Dependencies

acos_cli (Certified)
Provided by a10
Collection of modules used to configure ACOS devices over
3 Modules, 0 Roles, 3 Plugins, 1 Dependency

cumulus_linux_roles (Certified)
Provided by nvidia
0 Modules, 17 Roles, 0 Plugins, 0 Dependencies

remote (Certified)
Provided by wti
Modules for interacting with WTI remote OOB and PDU devices
21 Modules, 0 Roles, 2 Plugins, 0 Dependencies

controller (Certified)
Provided by ansible
Ansible content that interacts with the AWX or Automation Pl...
78 Modules, 0 Roles, 3 Plugins, 0 Dependencies

jws (Certified)
Provided by redhat
This collection contains the ansible playbook to setup JWS.
0 Modules, 1 Role, 0 Plugins, 1 Dependency

ibm_zos_ims (Certified)
Provided by ibm
The IBM z/OS IMS collection includes modules and sample
7 Modules, 0 Roles, 0 Plugins, 1 Dependency

pas (Certified)
Provided by cyberark
This is a Collection of the CyberArk Ansible Security
4 Modules, 0 Roles, 0 Plugins, 0 Dependencies

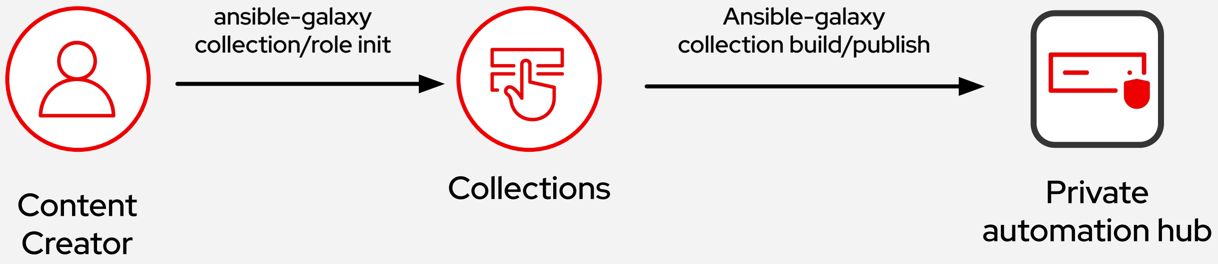
Certified

Certified

- On-Prem Automation Hub
- Sync content from multiple sources
- Gate / Approval process
- Manage who can use which collections/EEs in your organization
- Air-gapped installations
- Multi-hub / high-availability capable
- Easy to install

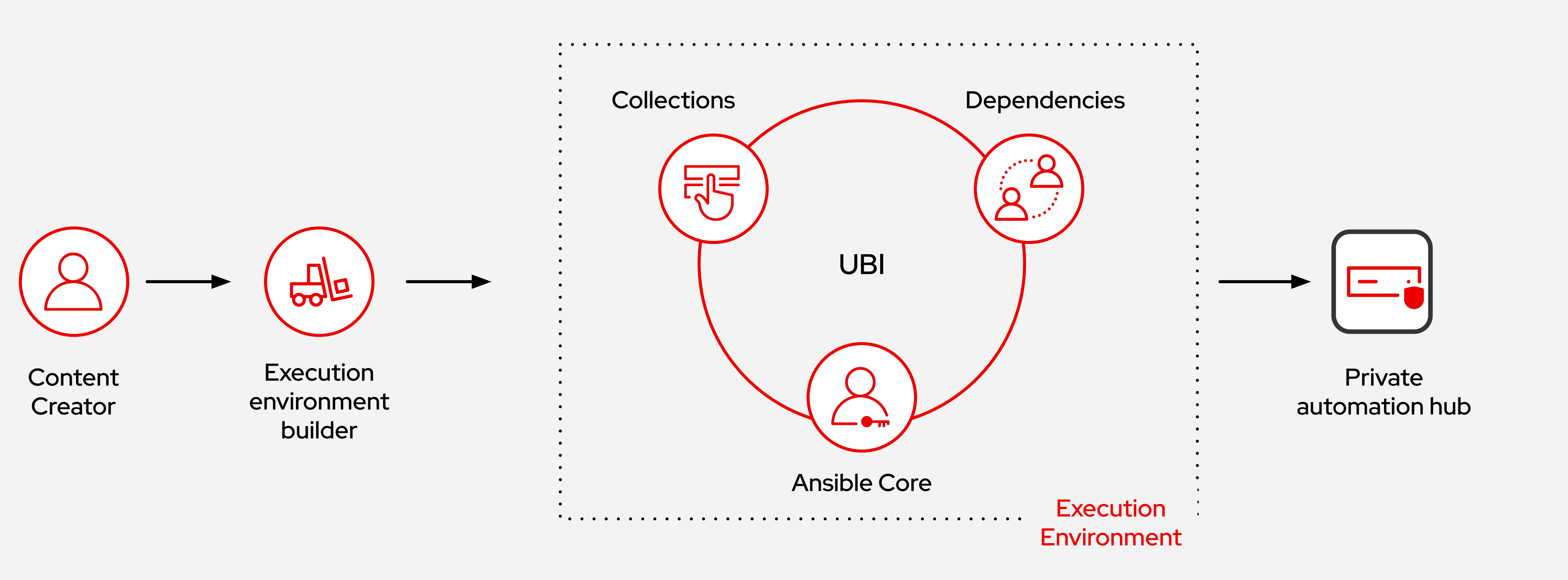
Build, create, publish

Development cycle of an automation execution environment

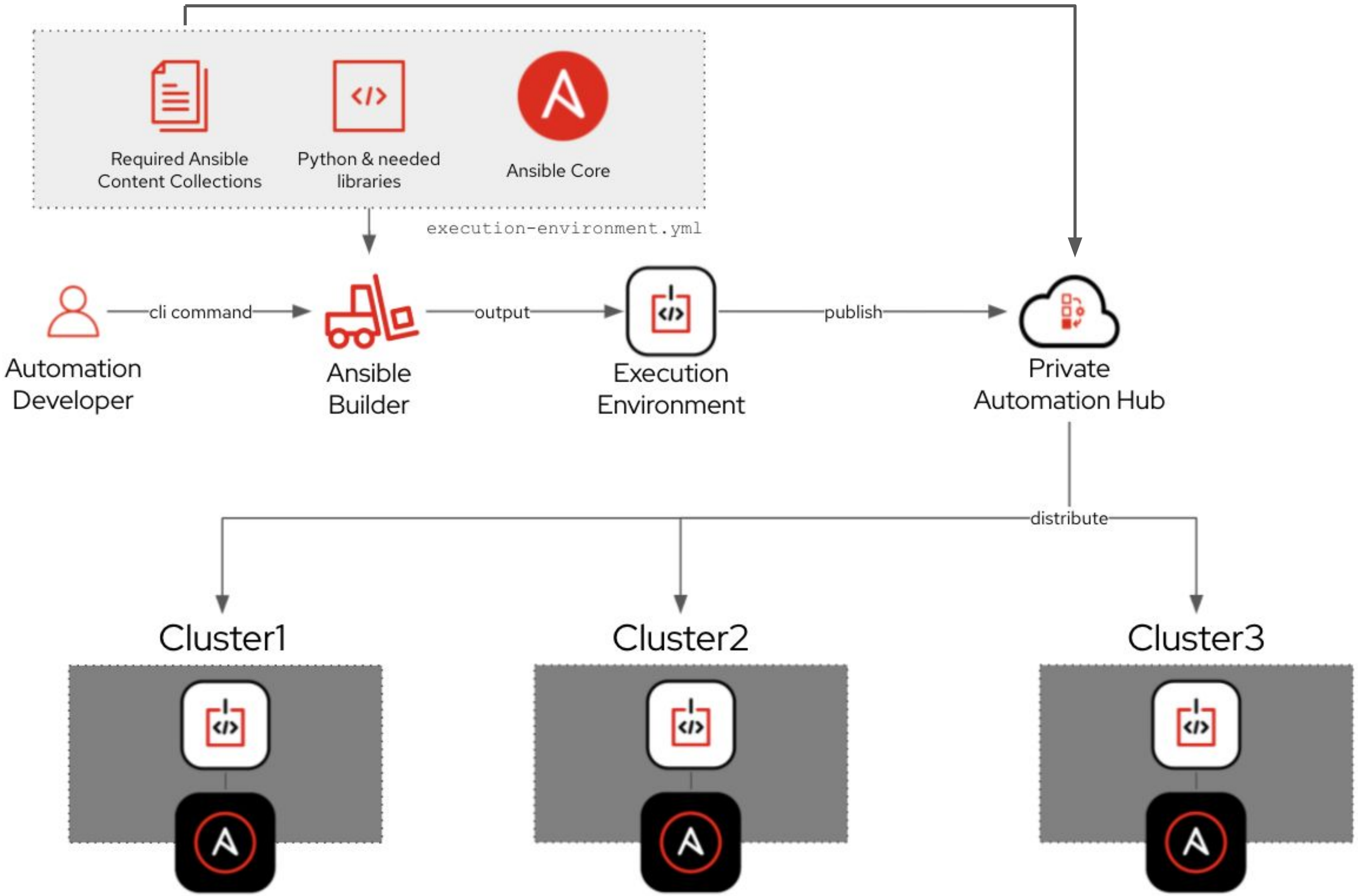


Build, create, publish

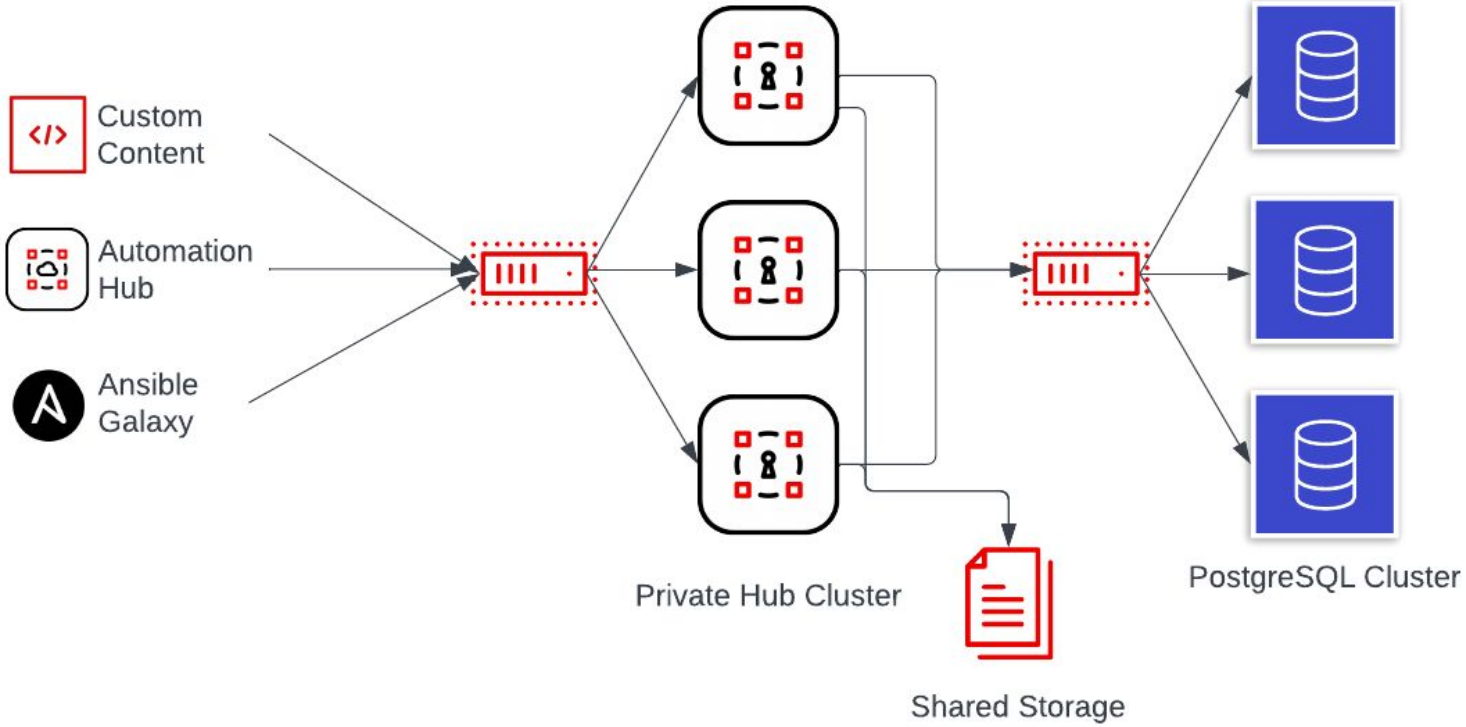
Development cycle of an automation execution environment



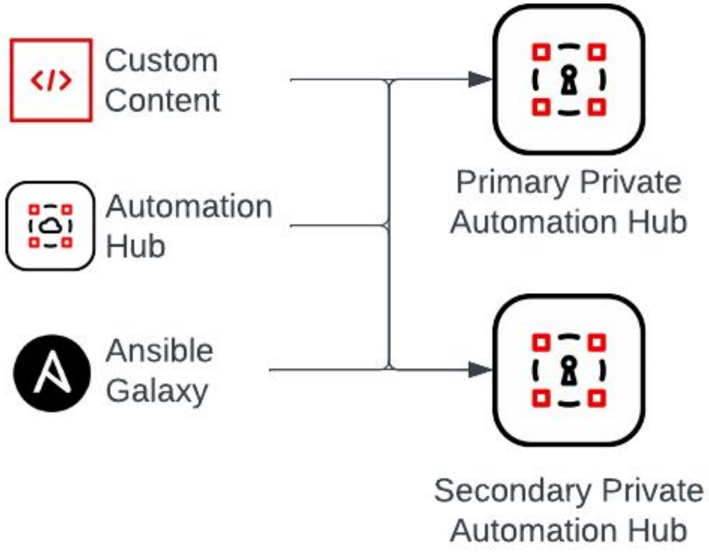
Workflow Diagram



Enterprise Deployment (Clustering)



Enterprise Deployment (MultiHub)


Custom Content
Automation Hub
Ansible Galaxy
Primary Private Automation Hub
Secondary Private Automation Hub

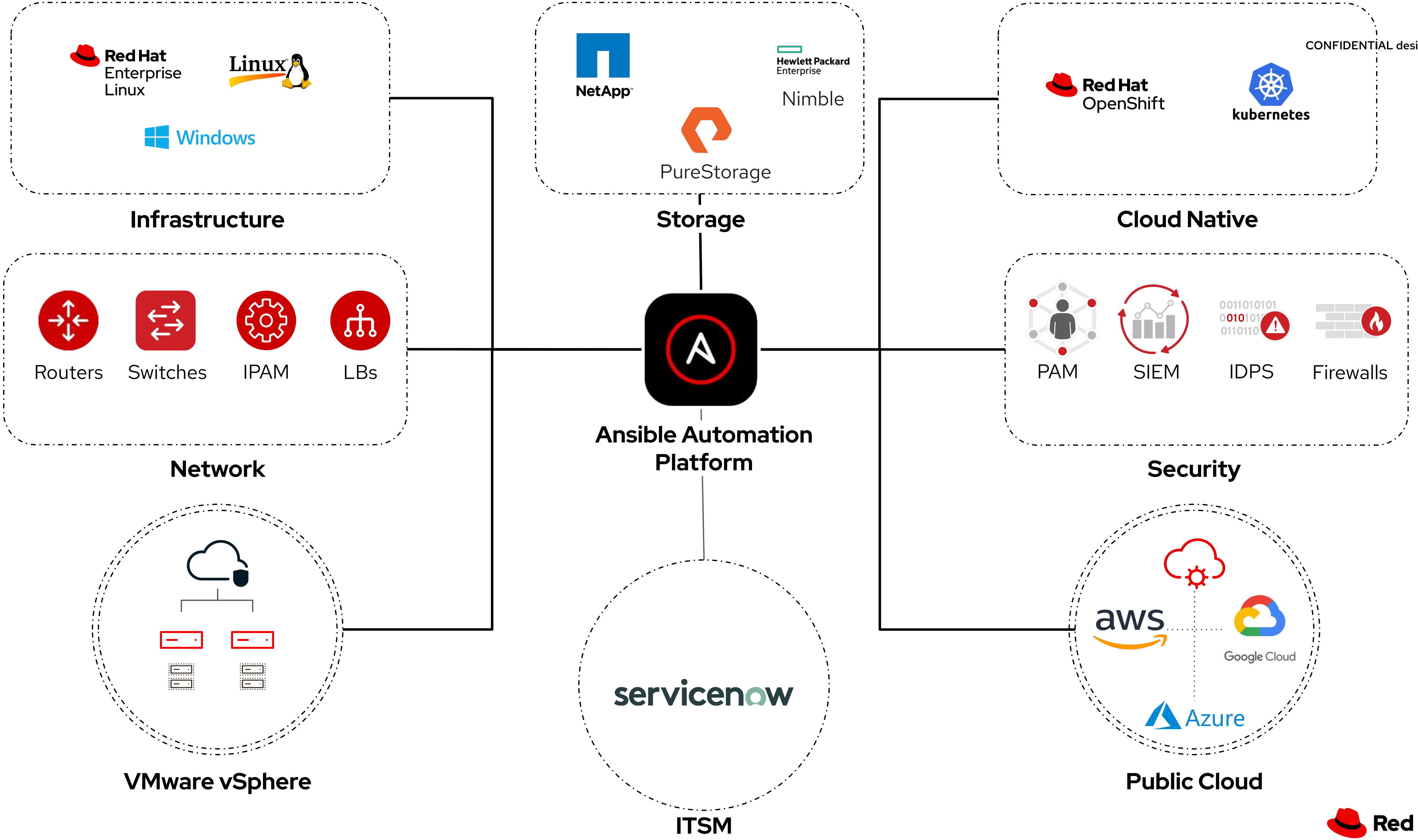
Why do I need this?

We already….

I don’t need….

No issues today…

CONFIDENTIAL designator



Infrastructure

Red Hat Enterprise Linux

Linux

Windows

Storage

NetApp

Hewlett Packard Enterprise

Nimble

PureStorage

Cloud Native

Red Hat OpenShift

kubernetes

Network

Routers

Switches

IPAM

LBs

Ansible Automation Platform

Security

PAM

SIEM

IDPS

Firewalls

VMware vSphere

ITSM

servicenow

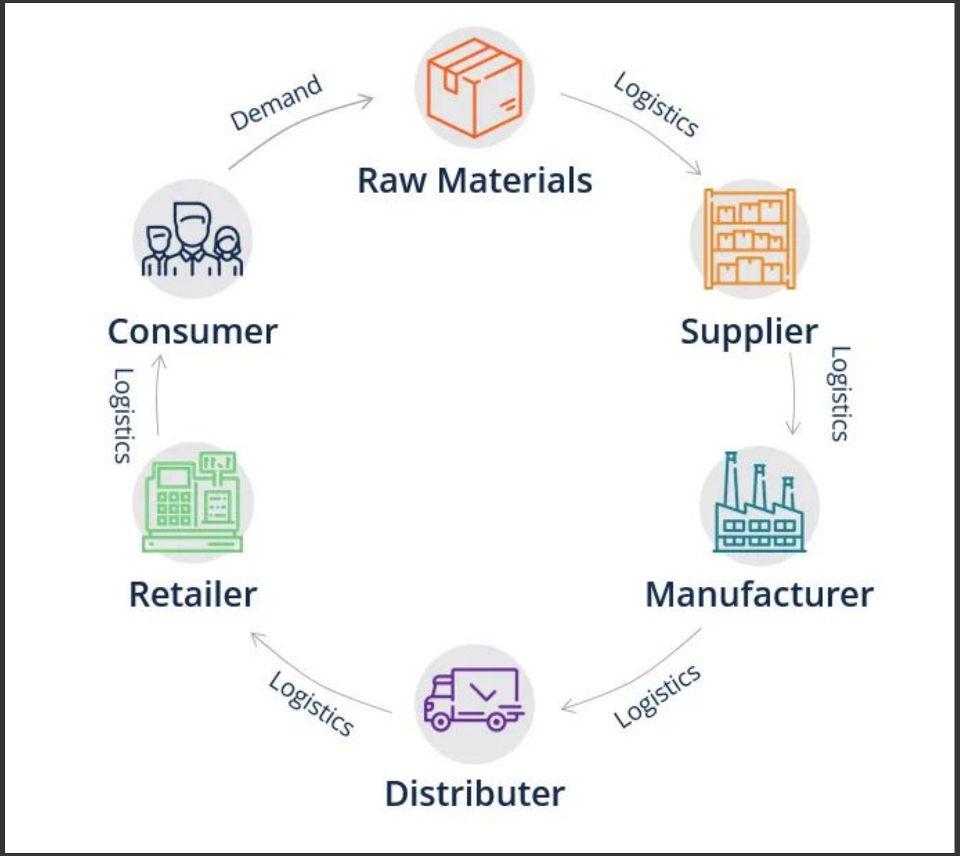
Public Cloud

aws

Google Cloud

Azure

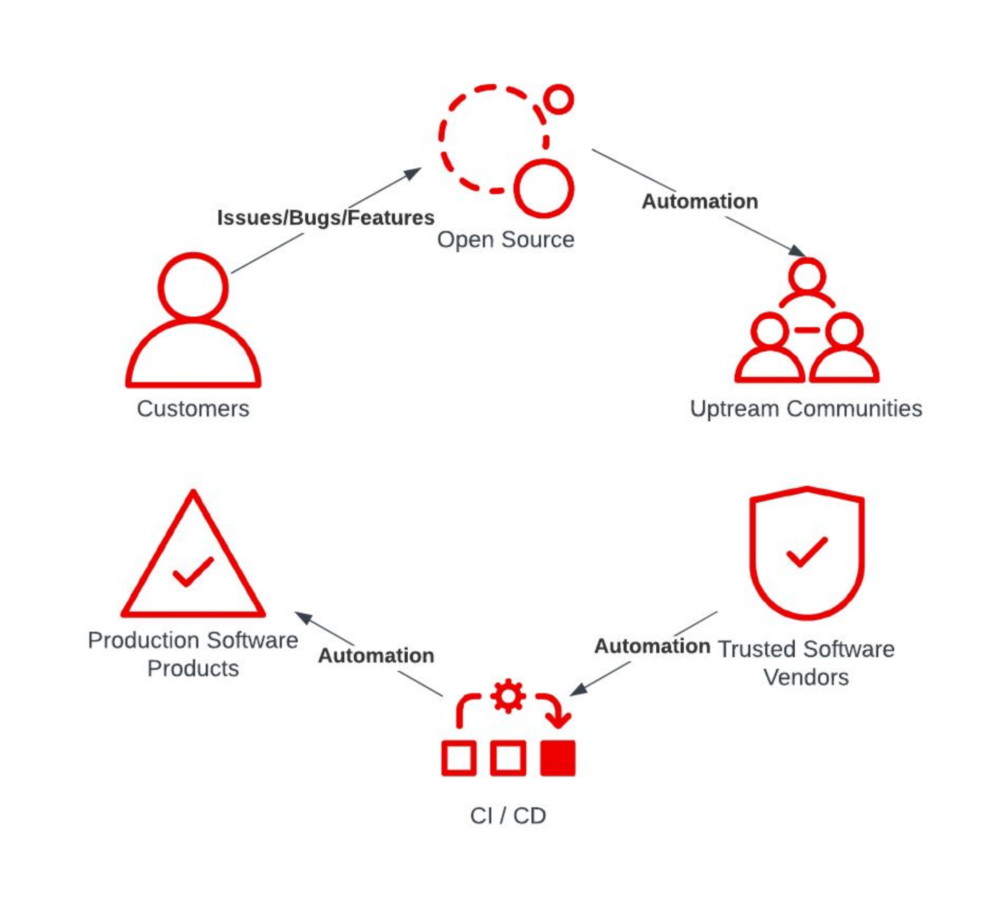
Supply Chain



https://corporatefinanceinstitute.com/resources/knowledge/strategy/supply-chain/

A supply chain is an entire system of producing and delivering a product or service, from the very beginning stage of sourcing the raw materials to the final delivery of the product or service to end-users.

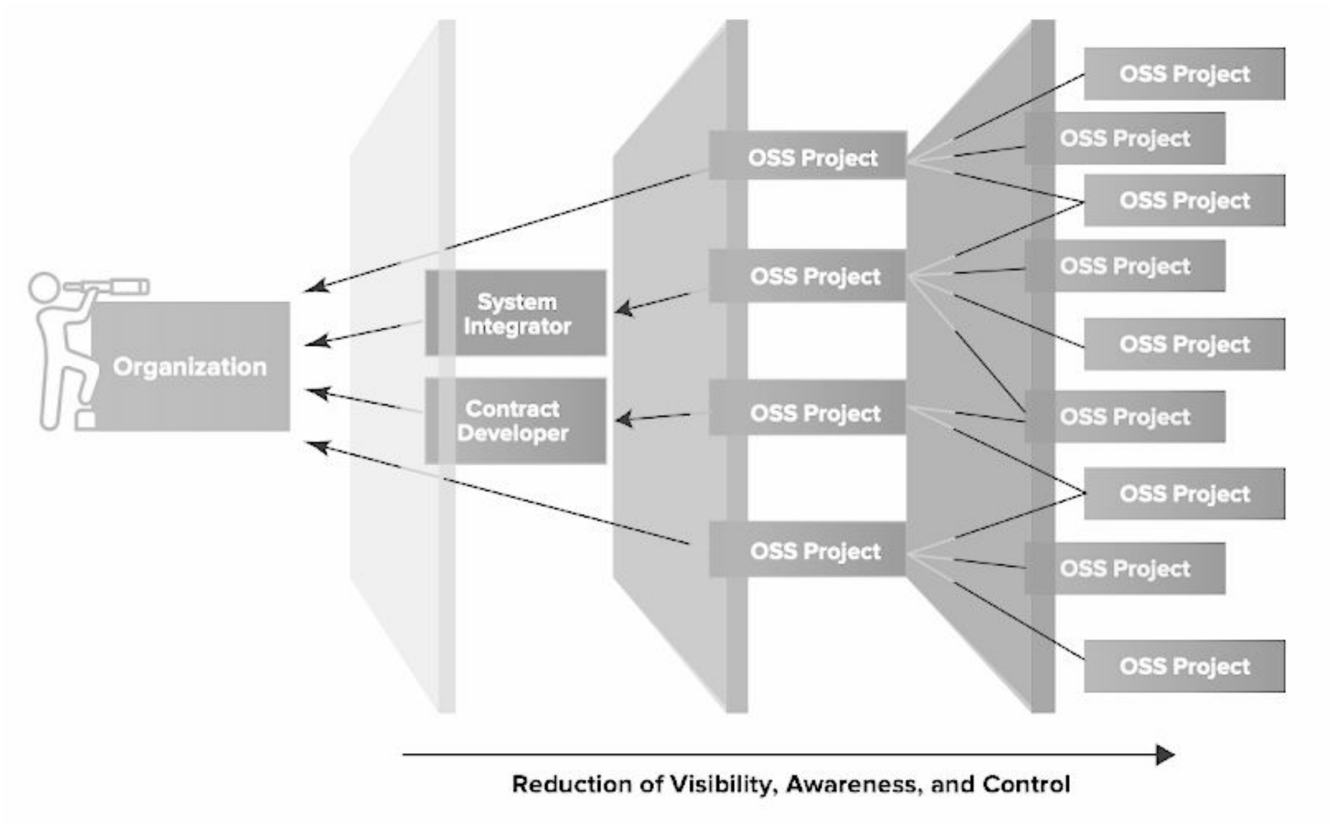
Software Supply Chain



A **software** supply chain is an entire system of producing and delivering a product or service, from the very beginning stage of **source code** ~~sourcing the raw materials~~ to the final delivery of the product or service to end-users.

How to Manage a Software Supply Chain?

Create Trust = Visibility Where There Isn't Any



Source: 2020 State of Software Supply Chain Report

Infrastructure Software Supply Chain

This applies to Automation!

Raw Materials

Open Source projects, community and internal development (collections, modules, roles, plugins, filters, other projects)

Warehouse

Component registries such as github, galaxy, dockerhub, quay.io, artifactory, chocolatey, brew, rpm, deb, pyPI, helm repos

Supplier / Manufacturing

Software Vendors, Consultants, SMEs

Playbooks, Scripts, Makefiles, ContainerFiles, Execution Environments, Job Templates

Finished Goods

Repeatable Build/Deploy

Consistent/compliant/immutable infrastructure

Supply Chain considerations when Automating

How are new vulnerabilities in your automations discovered?

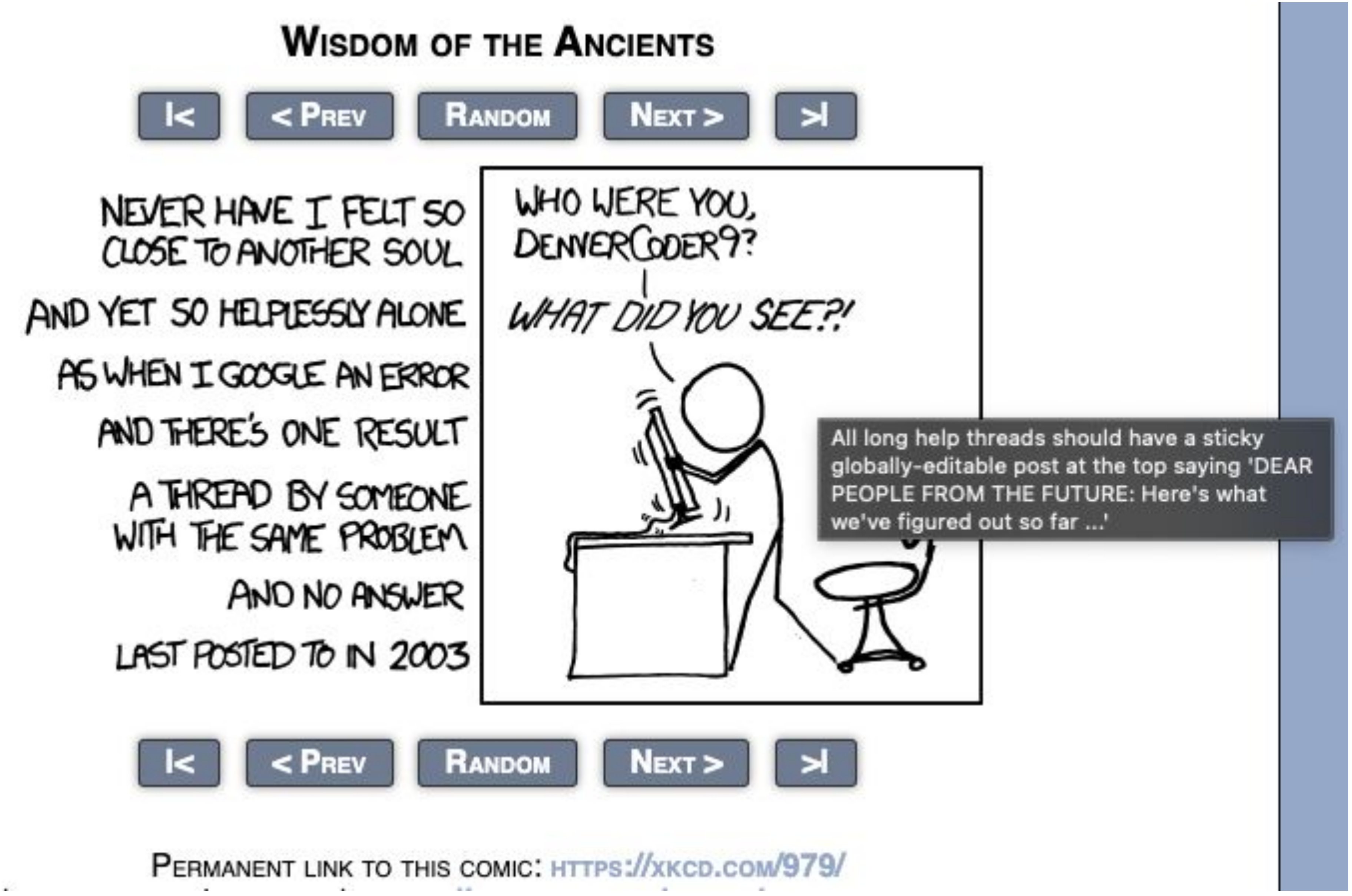
What level of awareness exists around the automation in use today?

What is the security impact to the automation if compromised?

How are fixes to automation code addressed?

Is the appropriate expertise available to assess and remediate security issues in-house?

What about critical and immediate support?



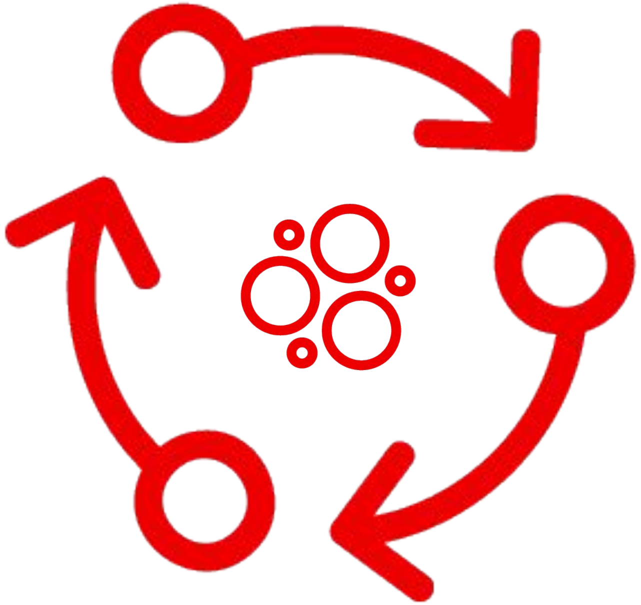
Wisdom of the Ancients

|<
< Prev
Random
Next >
>|
NEVER HAVE I FELT SO CLOSE TO ANOTHER SOUL
AND YET SO HELPLESSLY ALONE
AS WHEN I GOOGLE AN ERROR
AND THERE'S ONE RESULT
A THREAD BY SOMEONE WITH THE SAME PROBLEM
AND NO ANSWER
LAST POSTED TO IN 2003
WHO WERE YOU, DENVERCODER9?
WHAT DID YOU SEE?!
|<
< Prev
Random
Next >
>|

All long help threads should have a sticky globally-editable post at the top saying 'DEAR PEOPLE FROM THE FUTURE: Here's what we've figured out so far ...'

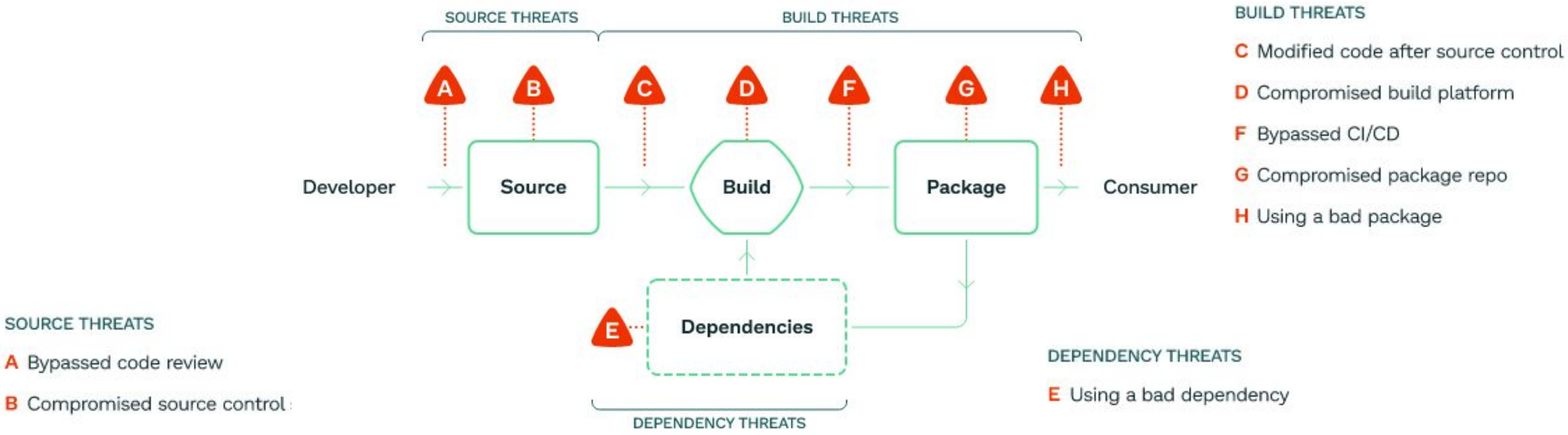
Permanent link to this comic: https://xkcd.com/979/

Current state of the Infrastructure supply chain?



- Repositories and dependencies can be anywhere
- Distribution tends to be unsigned and in community repositories, what version was working last?
- Some safeguards may exist, but to what standard, are they followed, and audited?
- Upstream repositories are prime targets for supply chain attacks (solarwinds, PHP, webmin, browserify)
- “Release early, release often” can lead to significant changes

SLSA, an End-to-End Framework for Supply Chain Integrity



BUILD THREATS

- C Modified code after source control
- D Compromised build platform
- F Bypassed CI/CD
- G Compromised package repo
- H Using a bad package

SOURCE THREATS

- A Bypassed code review
- B Compromised source control

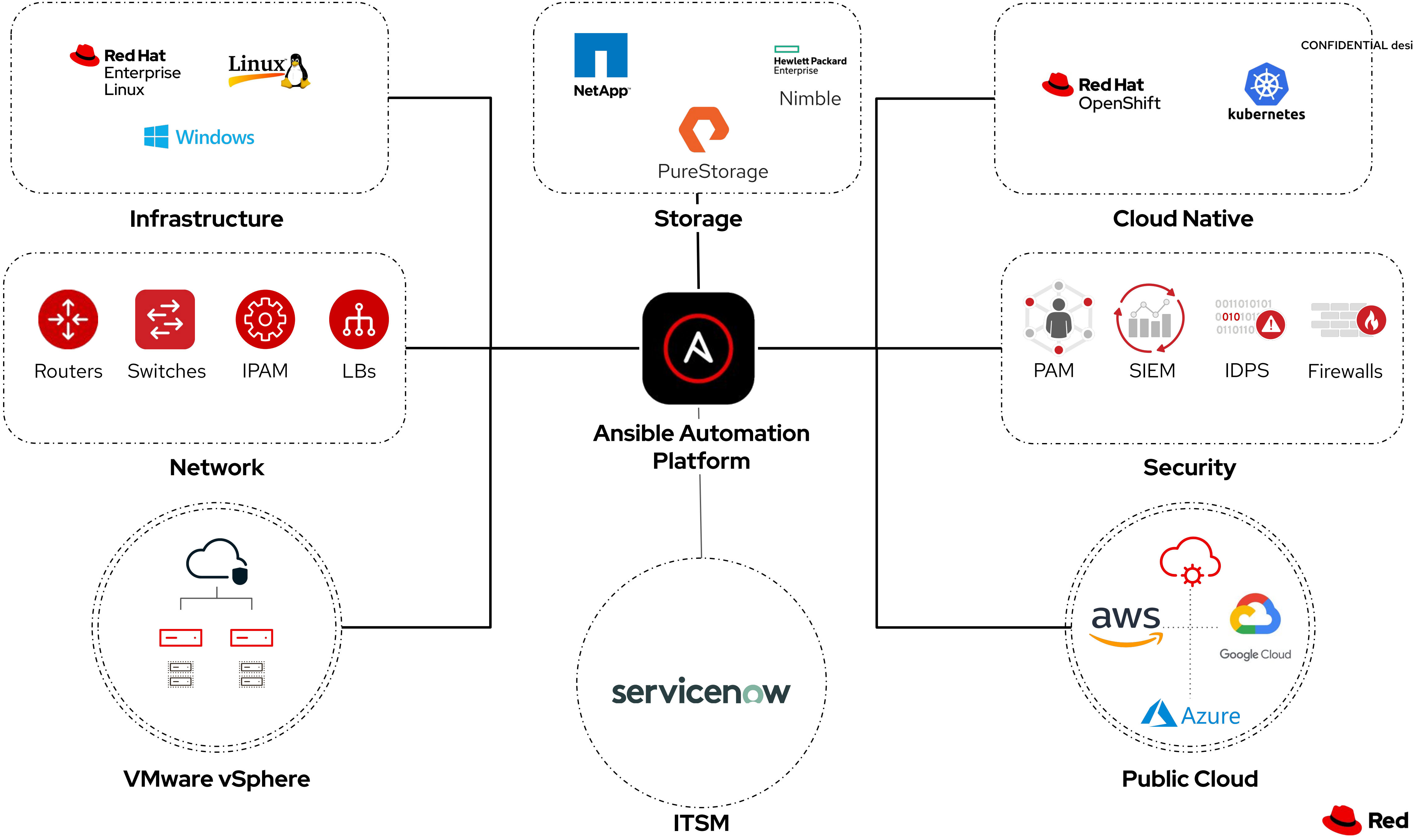
DEPENDENCY THREATS

- E Using a bad dependency

https://slsa.dev/

Demo Time!

CONFIDENTIAL designator



Red Hat Enterprise Linux

Linux

Windows

Infrastructure

NetApp

Hewlett Packard Enterprise

Nimble

PureStorage

Storage

Red Hat OpenShift

kubernetes

Cloud Native

Routers

Switches

IPAM

LBs

Network

Ansible Automation Platform

PAM

SIEM

IDPS

Firewalls

Security

VMware vSphere

servicenow

ITSM

aws

Google Cloud

Azure

Public Cloud

Red Hat

Undermanaged open source can have costly impacts

6 million new versions

of OSS introduced in the past year; 37 million component versions now available[1]

650% increase

in open source software supply chain attacks[1]

$25 million

the predicted cost of a recent supply chain attack[2]

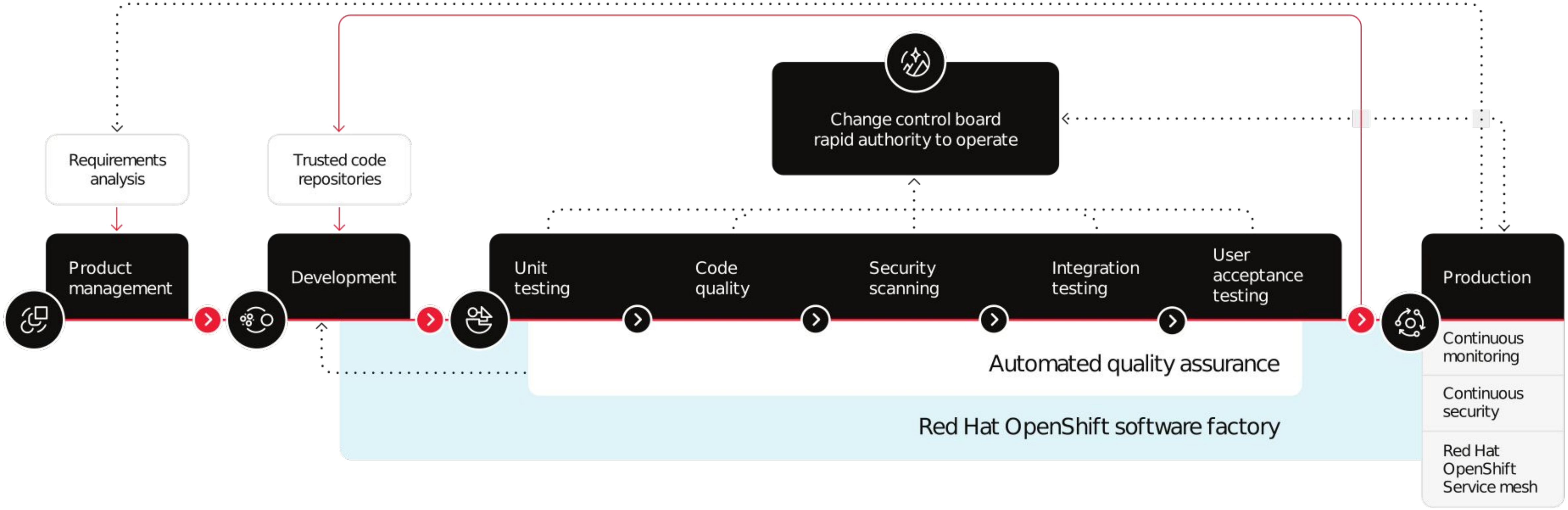
$2 billion

the cost of a data breach that resulted from an unpatched bug[3]

Source:
[1] Sonatype 2021 State of the software supply chain
[2] SolarWinds Expects Cyber Incident Costs Up To $25 Million In 2021
[3] Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement

Red Hat OpenShift

Trusted software supply chain



Requirements analysis

Trusted code repositories

Change control board rapid authority to operate

Product management

Development

Unit testing

Code quality

Security scanning

Integration testing

User acceptance testing

Production

Continuous monitoring

Continuous security

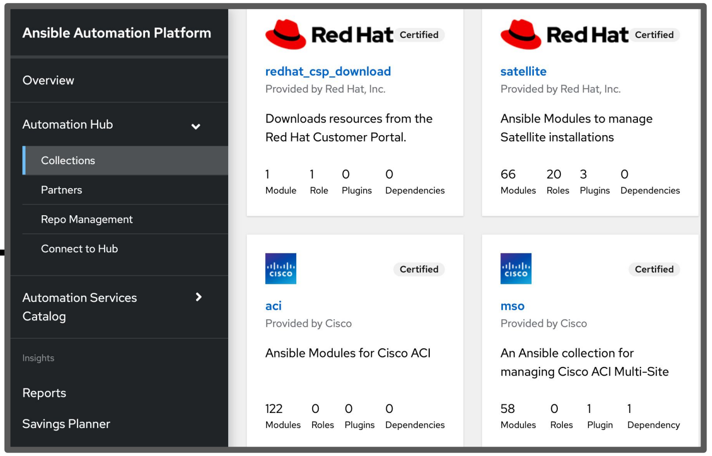
Red Hat OpenShift Service mesh

Automated quality assurance

Red Hat OpenShift software factory

—— Capability

····· Feedback



Red Hat Certified

redhat_csp_download

Provided by Red Hat, Inc.

Downloads resources from the Red Hat Customer Portal.

1 Module 1 Role 0 Plugins 0 Dependencies

Red Hat Certified

satellite

Provided by Red Hat, Inc.

Ansible Modules to manage Satellite installations

66 Modules 20 Roles 3 Plugins 0 Dependencies

Certified

aci

Provided by Cisco

Ansible Modules for Cisco ACI

122 Modules 0 Roles 0 Plugins 0 Dependencies

Certified

mso

Provided by Cisco

An Ansible collection for managing Cisco ACI Multi-Site

58 Modules 0 Roles 1 Plugin 1 Dependency

Modules / Plugins / Roles / Dependencies -> Roles/Playbooks -> Workflows -> Job Templates

Secure Supply Chain of Quality Parts

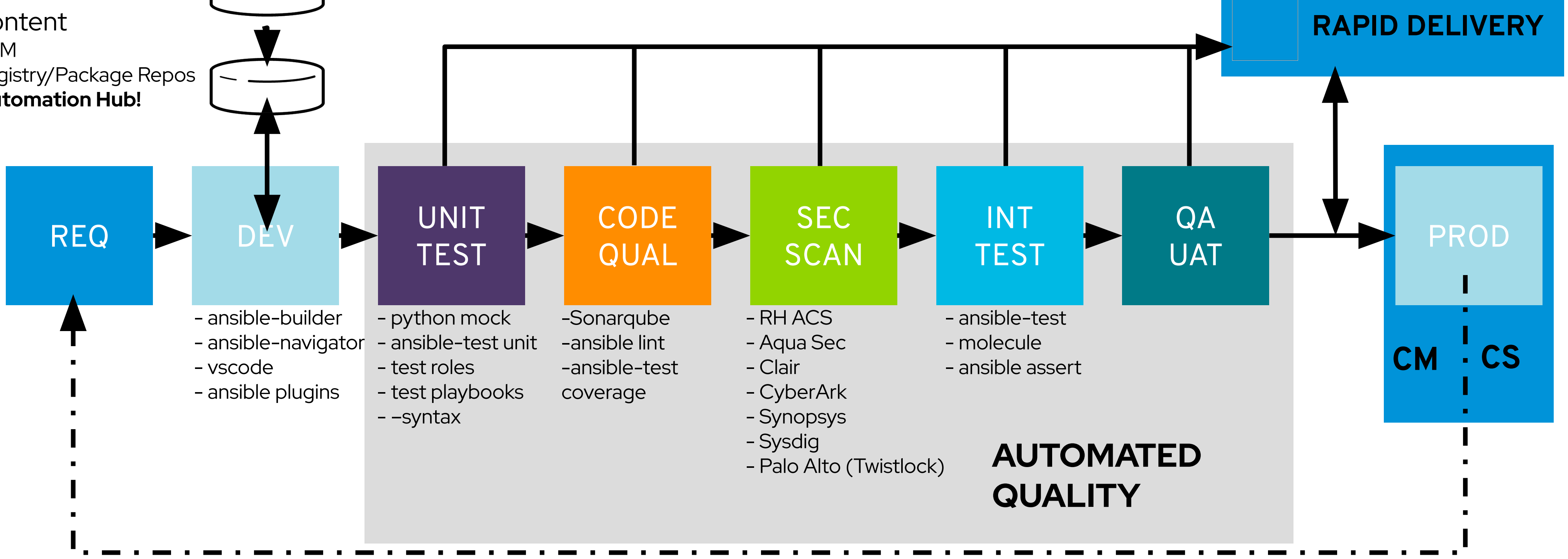
- Quality Assurance
- Certifications
- Signing & Secure
- Distribution

Trusted content

- Red Hat Automation Hub

Private content

- Internal SCM
- Internal Registry/Package Repos
- **Private Automation Hub!**



- ansible-builder
- ansible-navigator
- vscode
- ansible plugins

- python mock
- ansible-test unit
- test roles
- test playbooks
- –syntax

-Sonarqube
-ansible lint
-ansible-test coverage

- RH ACS
- Aqua Sec
- Clair
- CyberArk
- Synopsys
- Sysdig
- Palo Alto (Twistlock)

- ansible-test
- molecule
- ansible assert

- E2E signing
- RH ACS
- Aqua Sec
- CyberArk
- Sysdig
- Palo Alto (Twistlock)

Ansible Automation Factory

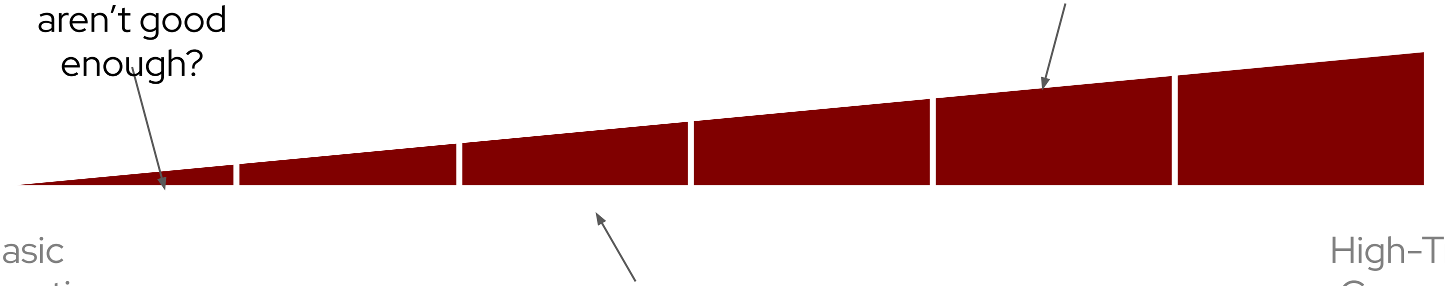
Orig Source:

Red Hat Container Catalog: Java Applications

More about the Container Health Index

TSSC is a journey

Where are you at?



New to this, where do we start? Upstream bits aren’t good enough?

We are using Private Automation Hub, were good right?

Basic Automation, scripts

We use AAP from Red Hat, what else do we have to do?

High-Trust, Governed and enforced

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat

Resources

- Getting Started with Automation Hub
- Private Automation Hub System Requirements
- Managing user access in Private Automation Hub
- Deploying a high availability automation hub
- Curating collections using namespaces in Automation Hub
- Publishing proprietary content collections in Automation Hub
- Managing Containers in Private Automation Hub
- Managing Red Hat Certified and Ansible Galaxy collections in Automation Hub

Resources

- Uploading content to Red Hat Automation Hub
- Pulp REST API Documentation
- 2022: The year of software supply chain security
- In Community We Trust: Open source software and supply chain security
- Defending Against Software Supply Chain Attacks
- AAP 2.1 Reference Architecture
- Kubernetes SLSA Work

Private Automation Hub Roadmap

The content set forth herein is Red Hat confidential information and does not constitute in any way a binding or legal agreement or impose any legal obligation or duty on Red Hat.

This information is provided for discussion purposes only and is subject to change for any or no reason.

Automation Hub

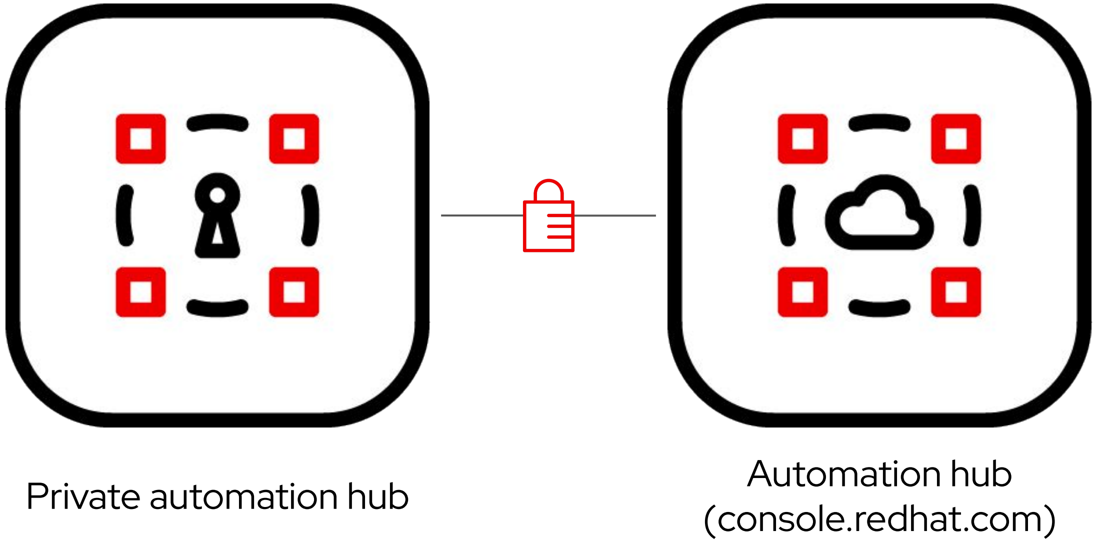
Discover, publish, and manage your Ansible Content

Major changes for AAP 2.2

- **Secure Supply Chain**
  Sign Certified and Private content
- **Repo Management**
  Private Automation Hub as a service. Create, delete and sync private repos.
- **Role Based Access**
  Support user defined roles for console.redhat.com

Solution & Business Value

- Provides content creators ability to collaborate and publish their own automation content and streamline Ansible code within their own organizations.
- Organizations can now manage and control the lifecycle of their Ansible content as their needs scale across the hybrid cloud.



Automation content signing

Major changes for AAP 2.2

Major changes for AAP 2.2

- **Automation Hub**
  Certified content from Red Hat and partners is signed on console.redhat.com ensuring end-to-end security
- **Content signing**
  Sign private content when you publish to Private automation hub. Both execution environments and Ansible content collections can be signed.
- **Certified Content with signatures**
  Certified content from Red Hat will come with accompanying signatures

Solution & Business Value

- End-to-end secure content signing from creator to production to ensure what is being executed in your enterprise