美国国防部DevSecOps最佳实践

ThreatSource

Global Threat Landscape

2.5万亿美元

2019年网络安全将造成经济损失

200%

2019数据泄露量同比增长

85亿条

报告超过 85 亿条泄露记录

2019年海外重要网络安全事件

- Facebook被爆明文存储6亿用户密码，已被查看900万次
- 云存储服务商MEGA泄露87GB数据含7.7亿个邮箱
- 16家网站6.17亿用户信息在暗网被售卖
- 万豪酒店5亿客户数据泄露
- 美国银行第一资本遭黑客入侵，逾1亿用户信息泄露
- 全球7.37亿医疗数据泄露，波及52个国家超过2000万人
- Equifax导致1.43亿美国消费者个人信息被泄露

2019年国内重要网络安全事件

- 超2亿中国求职者简历疑泄露，数据“裸奔”将近一周
- 拼多多现优惠券漏洞，遭黑产团伙盗取数千万元
- 抖音千万级账号遭撞库攻击，牟利百万黑客被捕
- 华硕超百万用户可能感染恶意后门
- 湖北首例入侵物联网系统案告破，十万设备受损

来源：俄罗斯储蓄银行，IBM

导致泄露的最主要原因是漏洞

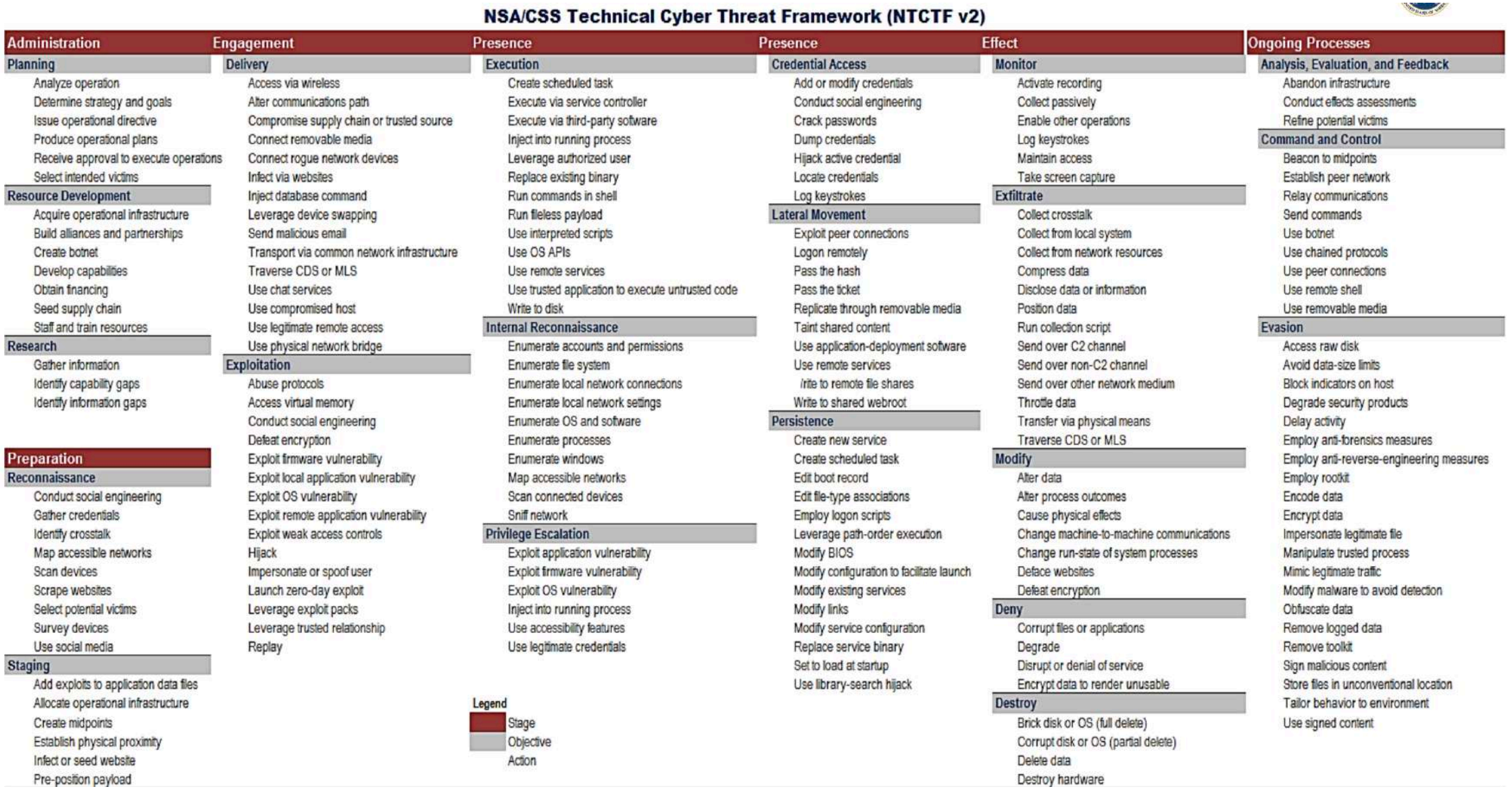
OWASP TOP 10 应用安全漏洞

供应链攻击

Upstream dependencies

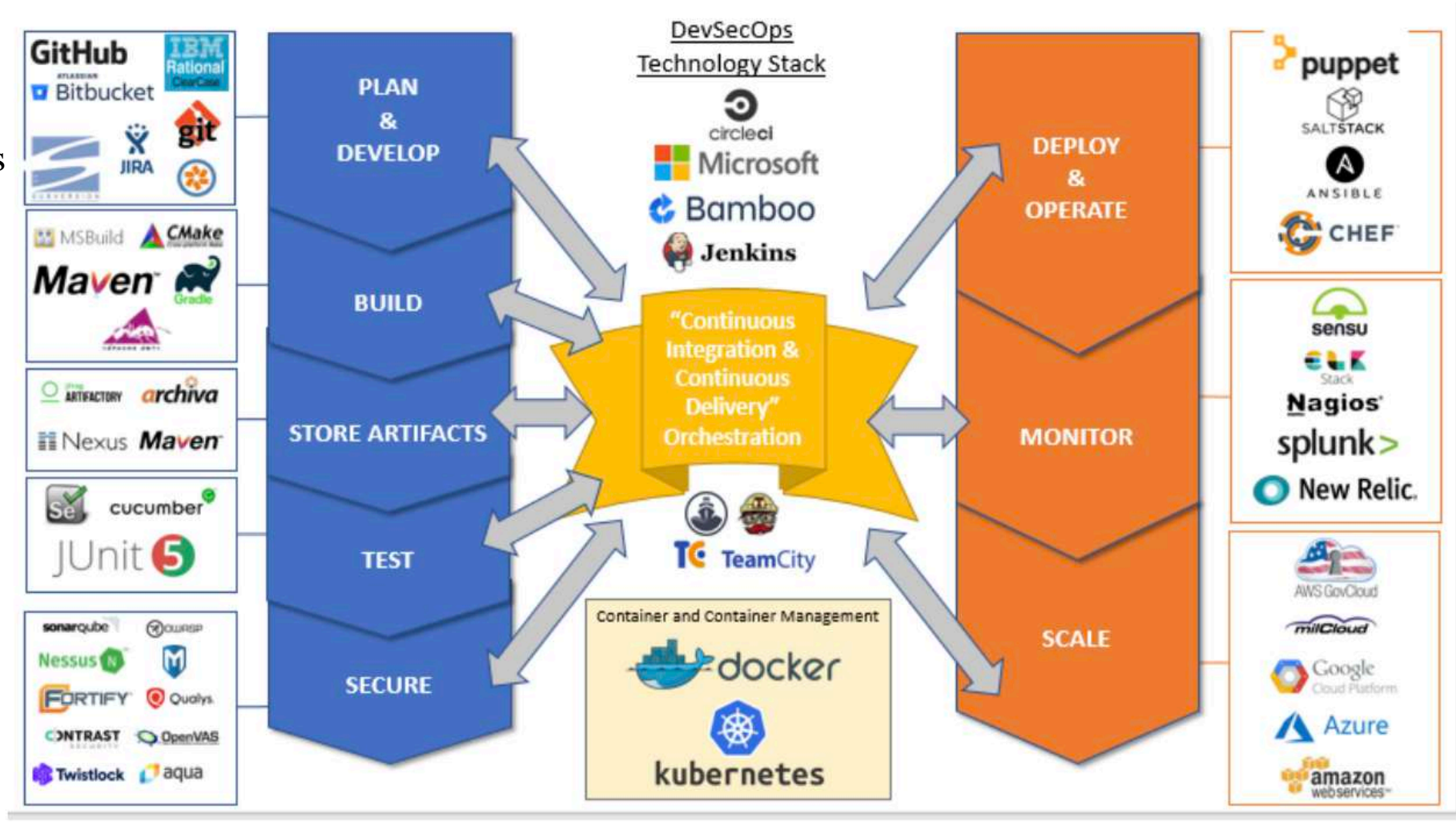
- 1 import != 1 dependency
- Inventory not only direct dependencies, but also 2nd/3rd/Nth level

NSA发布的网空威胁框架



DoD的企业内部开发视角

- Business systems
- Command and Control systems
- Embedded and Weapon systems
- Intelligence analysis systems
- Autonomous systems
- Assisted human operations



DoD的企业内部开发视角

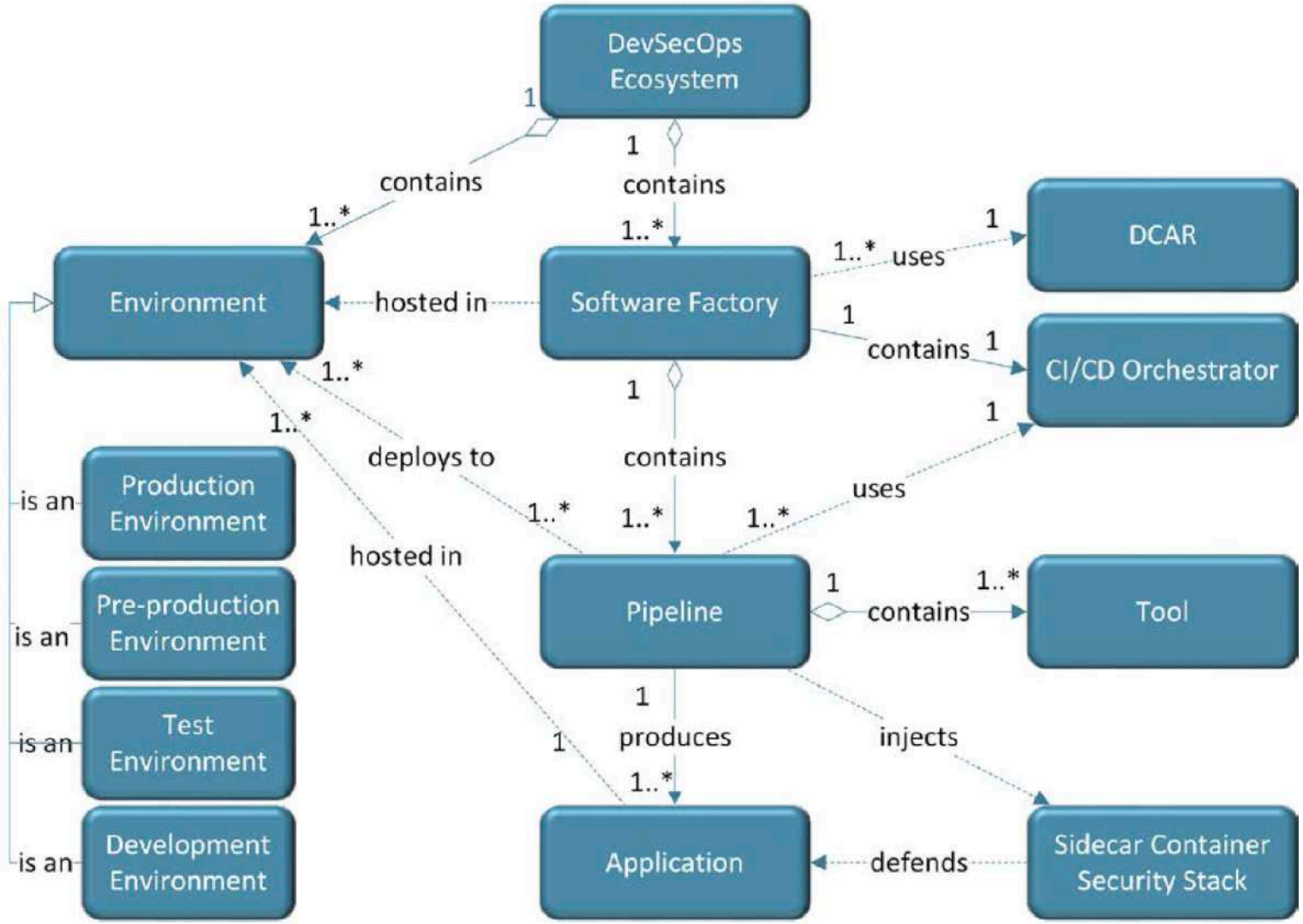


Figure 2: Conceptual Model

U.S. AIR FORCE

What is the DoD Enterprise DevSecOps Initiative?

- Joint Program with OUSD(A&S), DoD CIO, U.S. Air Force, DISA and the Military Services.
- Technology:
  - **Avoid vendor lock-in** at the Infrastructure and Platform Layer by leveraging FOSS with Kubernetes and OCI containers,
  - Creating the DoD Centralized Artifacts Repository (DCAR) of hardened and centrally accredited containers: selecting, certifying, and securing best of breed development tools and software capabilities (over 170+ containers) - https://dccscr.dsop.io/dsop/ and https://dcar.dsop.io
  - **Baked-in Zero Trust Security** with our Sidecar Container Security Stack (SCSS) leveraging behavior detection, zero trust down to the container/function level.
  - Leveraging a Scalable Microservices Architecture with Service Mesh/API Gateway and baked-in security (Istio)
  - Leveraging KNative to avoid lock-in to Cloud provider Serverless stacks
- Bringing **Enterprise IT Capabilities with Cloud One and Platform One** – Cloud and DevSecOps as Managed Services capabilities, on-boarding and support!
- Standardizing metrics and define acceptable thresholds for **DoD-wide continuous Authority to Operate**
- Massive **Scale Training with Self Learning Capabilities** (train over 100K people within a year) and bring state of the art DevSecOps curriculum
- Creating new Agile contracting language to enable and incentivize the use of DevSecOps

Google容器安全的最佳实践

1、BeyondProd认为“服务信任应取决于代码来源和服务身份等特性，而不应取决于在生产网络中的位置，如IP或主机名身份”。

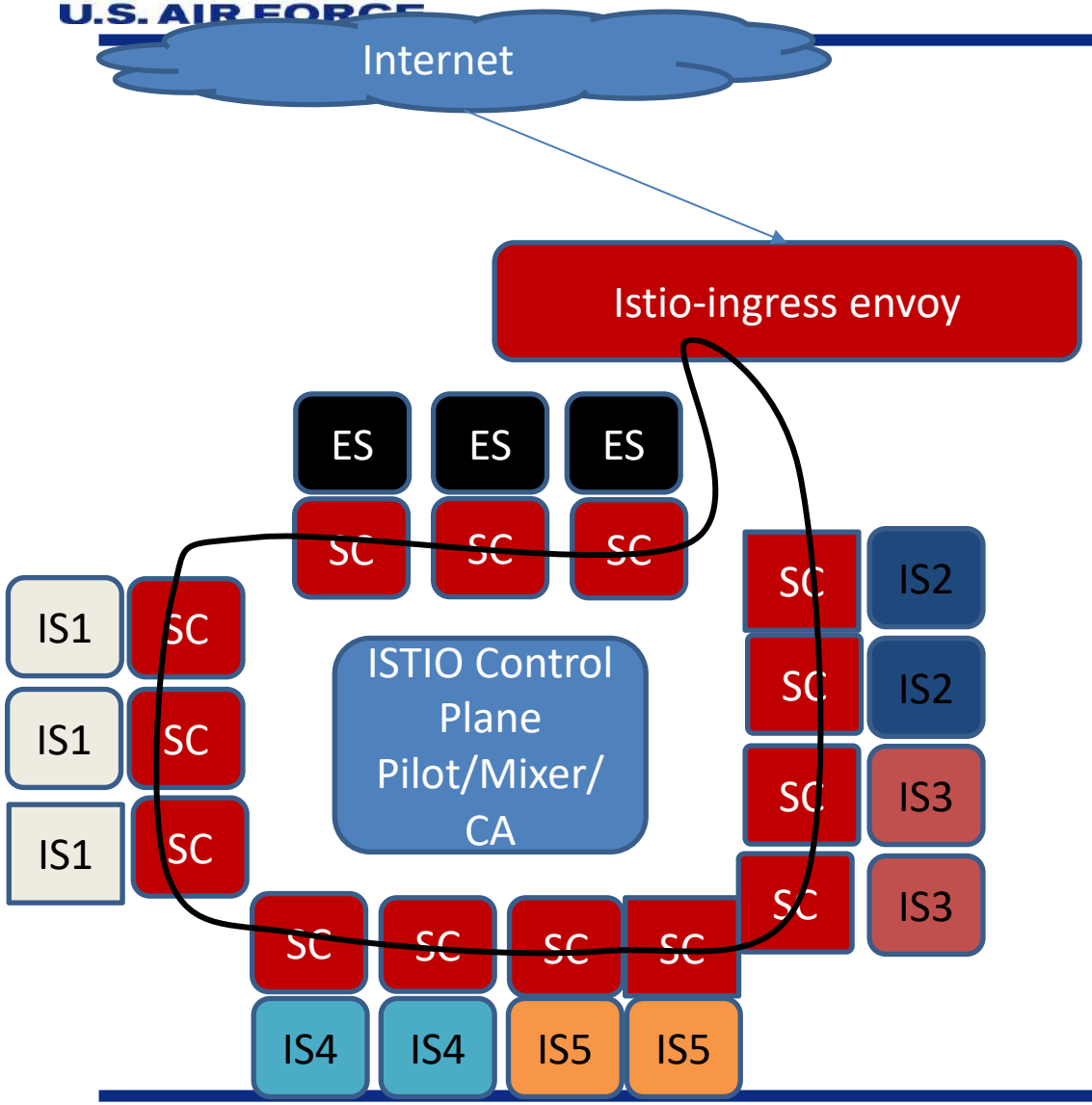
2、在传统安全模型中，防火墙基于IP进行访问控制；

3、容器下产生了新的安全需求，IP地址随时变化，需要新的模型；

安全原则	谷歌的内部安全工具/服务
在边缘保护网络	**谷歌前端（GFE）**，用于管理 TLS 终止和入站流量的策略
服务间默认不互信	**应用层传输安全性（ALTS）**，用于 RPC 身份认证、完整性、加密和服务身份
在可信机器上运行来源已知的代码	**Borg 的二进制授权（BAB）**，代码来源验证 **主机完整性（HINT）**，机器完整性验证
跨服务强制执行一致策略的关卡	**服务访问策略**，用于限制服务间的数据访问方式 **最终用户上下文（EUC）票据**，用于证明原始请求者的身份
简单、自动及标准的更改发布	**Borg 工具**，用于蓝/绿部署
共享操作系统的工作负载间的隔离	**gVisor**，用于工作负载隔离

传统基础架构安全性	云原生安全性	云原生安全性的隐含要求
基于边界的安全（如防火墙），其内部通信默认安全。	零信任安全，对服务之间的通信进行验证，环境中的服务没有隐式信任。	对网络边界的防护依然有效，但服务间没有默认互相信任。
某些应用使用固定 IP 和专用硬件。	包括 IP 和硬件在内的更高资源利用率、复用率、和共享率。	运行已知出处的代码可信机器。
基于 IP 地址的身份。	基于服务的身份。	
服务在已知预期的位置运行。	服务可以在环境中的任何位置运行，包括跨公有云和私有数据中心混合部署。	
每个应用都内置了特定安全要求，且这些要求会单独分别执行。	遵循集中式强制策略，服务栈中集成了共享的安全性要求。	用于跨服务强制执行持续一致策略的关卡。
对如何构建和审核服务的限制有限。	对所有的服务采用持续一致的安全要求。	
对安全组件的监督有限。	集中的安全策略视图及遵守策略的情况。	
专门发布更新，发布频率较低。	标准化构建和发布过程，更改单个微服务更频繁。	发布流程更改实现简单化、自动化及标准化。
工作负载通常作为 VM 部署或部署到物理主机，并使用物理机或 hypervisor 来提供隔离。	封装的工作负载及其进程在共享的操作系统中运行，则需要一种隔离工作负载的机制。	对共享操作系统的工作负载进行隔离。

Micro Service Architecture – Service Mesh technology



SC (Side Car) – One for each Service instance (A container in each POD)

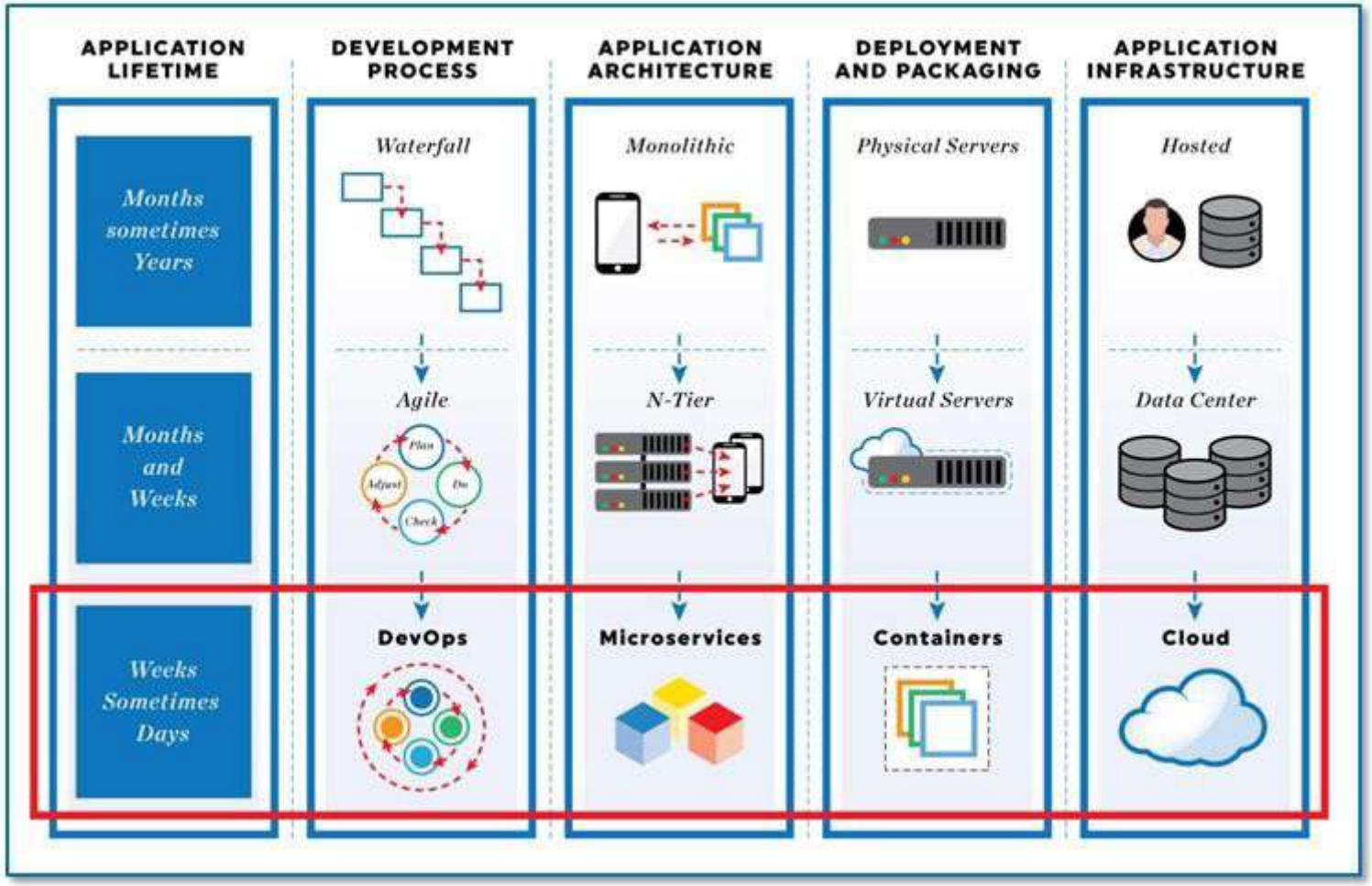
- Envoy proxy
- Service discovery, Load balancing, Failure handling, Circuit breaking (Limits), Fault injection (for troubleshooting), Health checks
- ***Mutual TLS***

ISTIO Control plane:

- Pilot:
  - Service discovery glue between Envoy and K8S
  - Traffic rule configuration
- Security
  - Role based Access control (Pluggable RBAC engine, support for local RBAC, K8S RBAC adapters, but facility to add new adapters – Example AAF RBAC adapter)
  - Certificate Authority

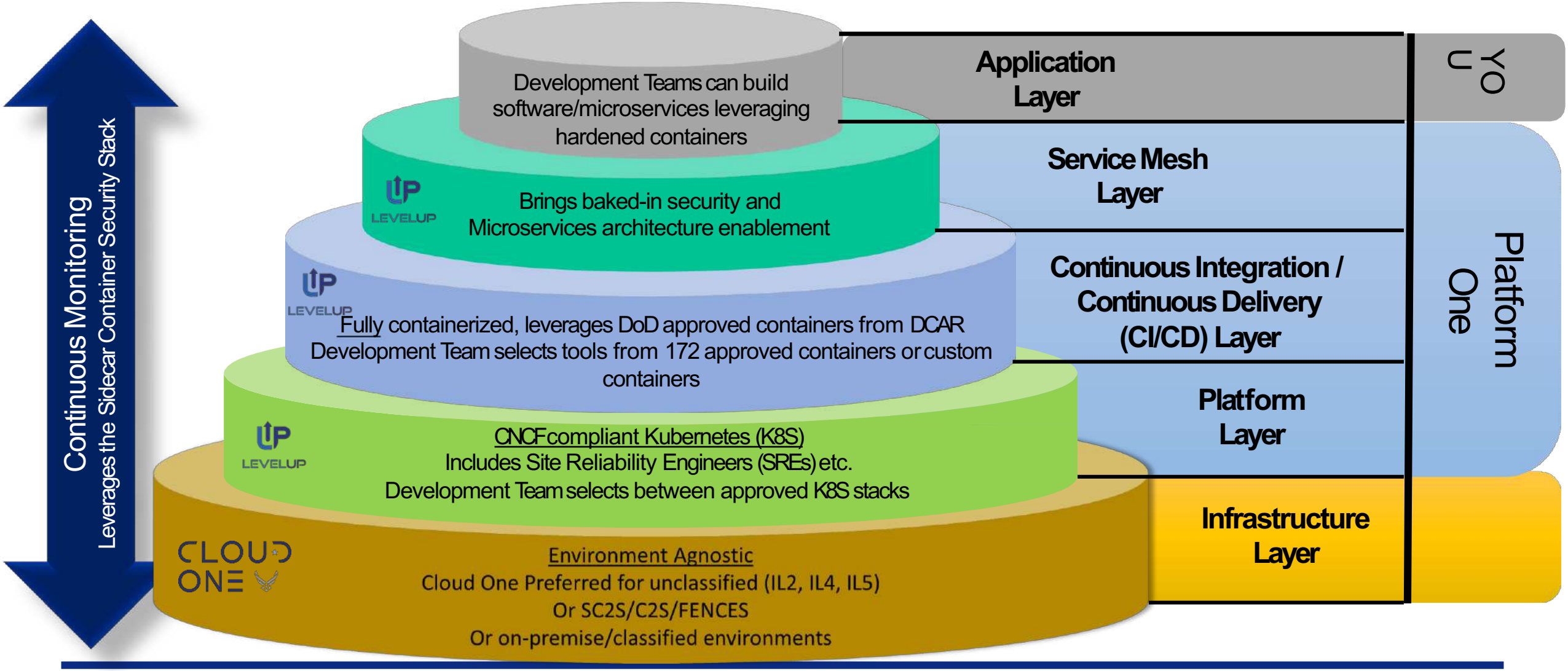
U.S. AIR FORCE

From Waterfall to DevSecOps



U.S. AIR FORCE

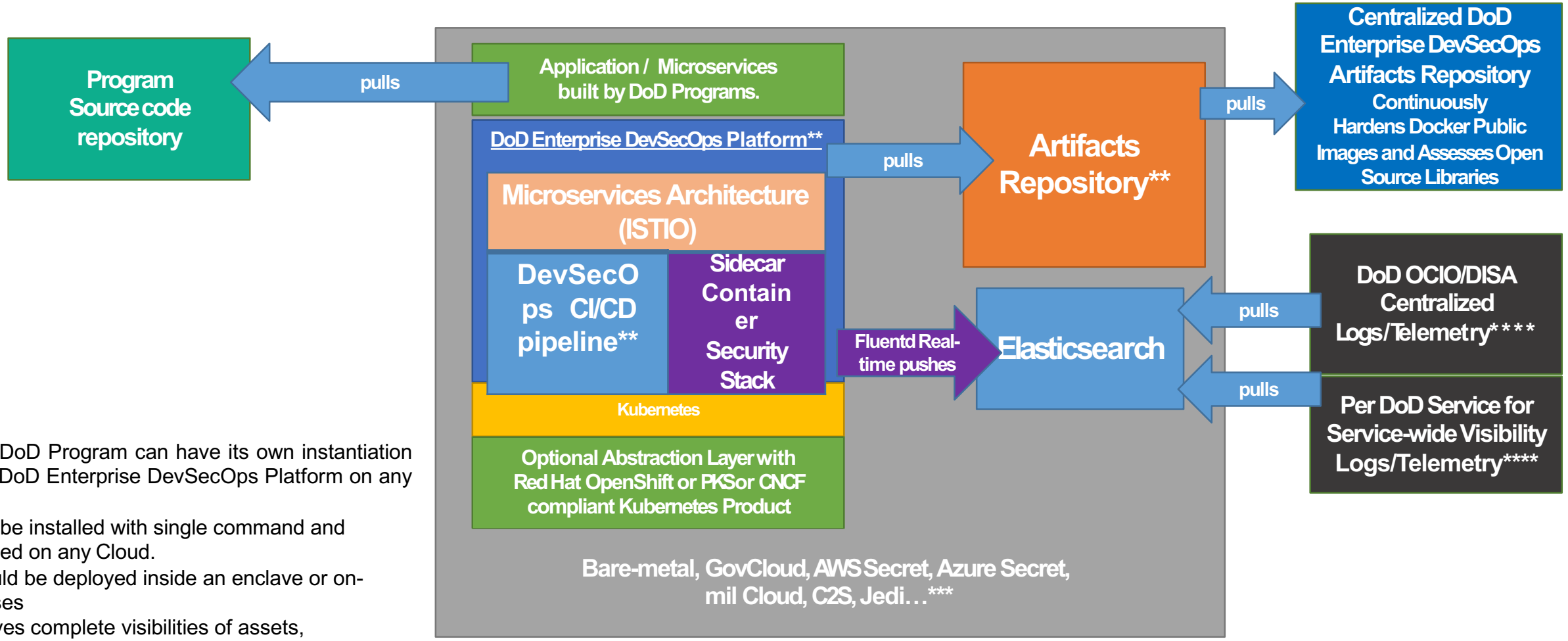
Understanding the DevSecOps Layers



Sidecar Container Security Stack

- Baked-in Zero Trust security down to the Container/Function level with Istio (Envoy) and Knative.
- Centralized logging and telemetry with Elasticsearch, Fluentd, Kibana (EFK).
- Container security: Continuous Scanning, Alerting, CVE scanning, Behavior detection both in development and production (Build, Registry, Runtime) with Twistlock
- Container security and insider threat (custom policies detecting unapproved changes to Dockerfiles) with Anchore
- Automated STIG compliance with OpenSCAP

DoD Enterprise DevSecOps Architecture*



*each DoD Program can have its own instantiation of the DoD Enterprise DevSecOps Platform on any Cloud.
** can be installed with single command and deployed on any Cloud.
*** could be deployed inside an enclave or on-premises
**** gives complete visibilities of assets, security/vulnerability state etc. can be integrated to existing cybersecurity shared services.

U.S. AIR FORCE

DevSecOps Software Lifecycle

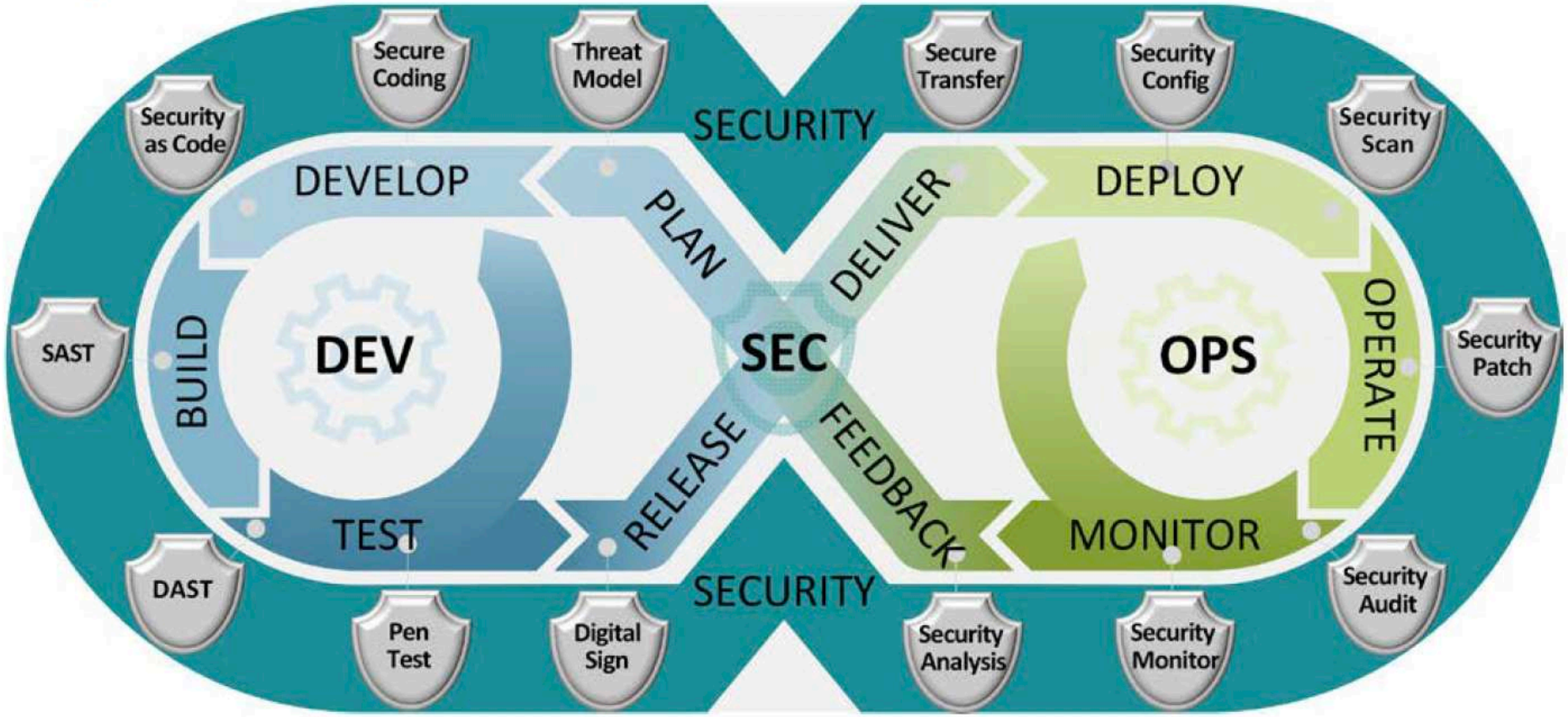


Figure 3: DevSecOps Software Lifecycle

DevSecOps Pillars

组织：
1、利益相关者Buy-in；
2、打破组织隔膜，提升沟通效率；
3、自动化产出QA报告，有Action；
4、漏、误报更新流程；

流程：
1、Test-Driven Development；
2、自动化；
3、安全卡点，逐步减少人工干预；

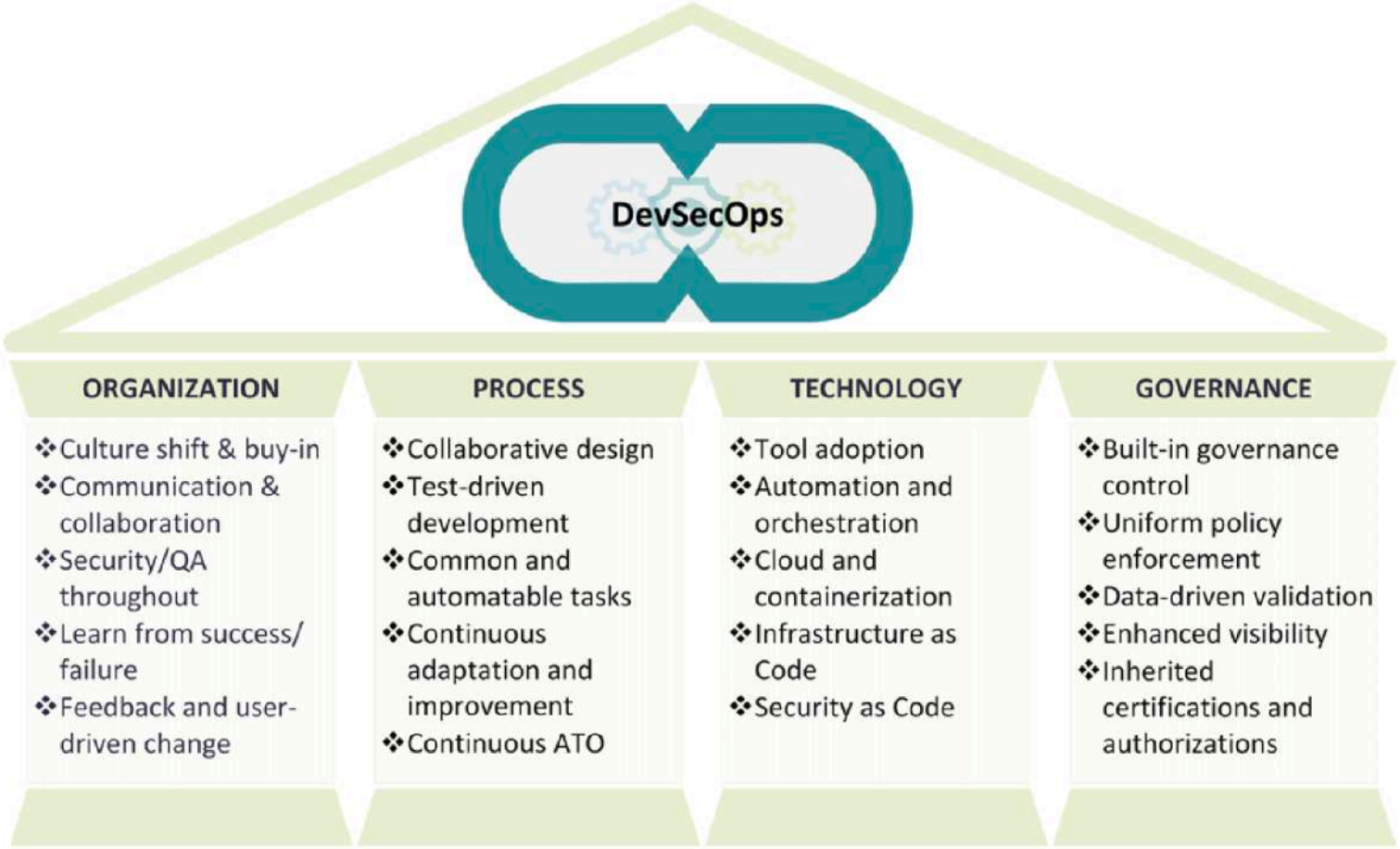


Figure 4: DevSecOps Pillars

U.S. AIR FORCE

DevSecOps Ecosystem

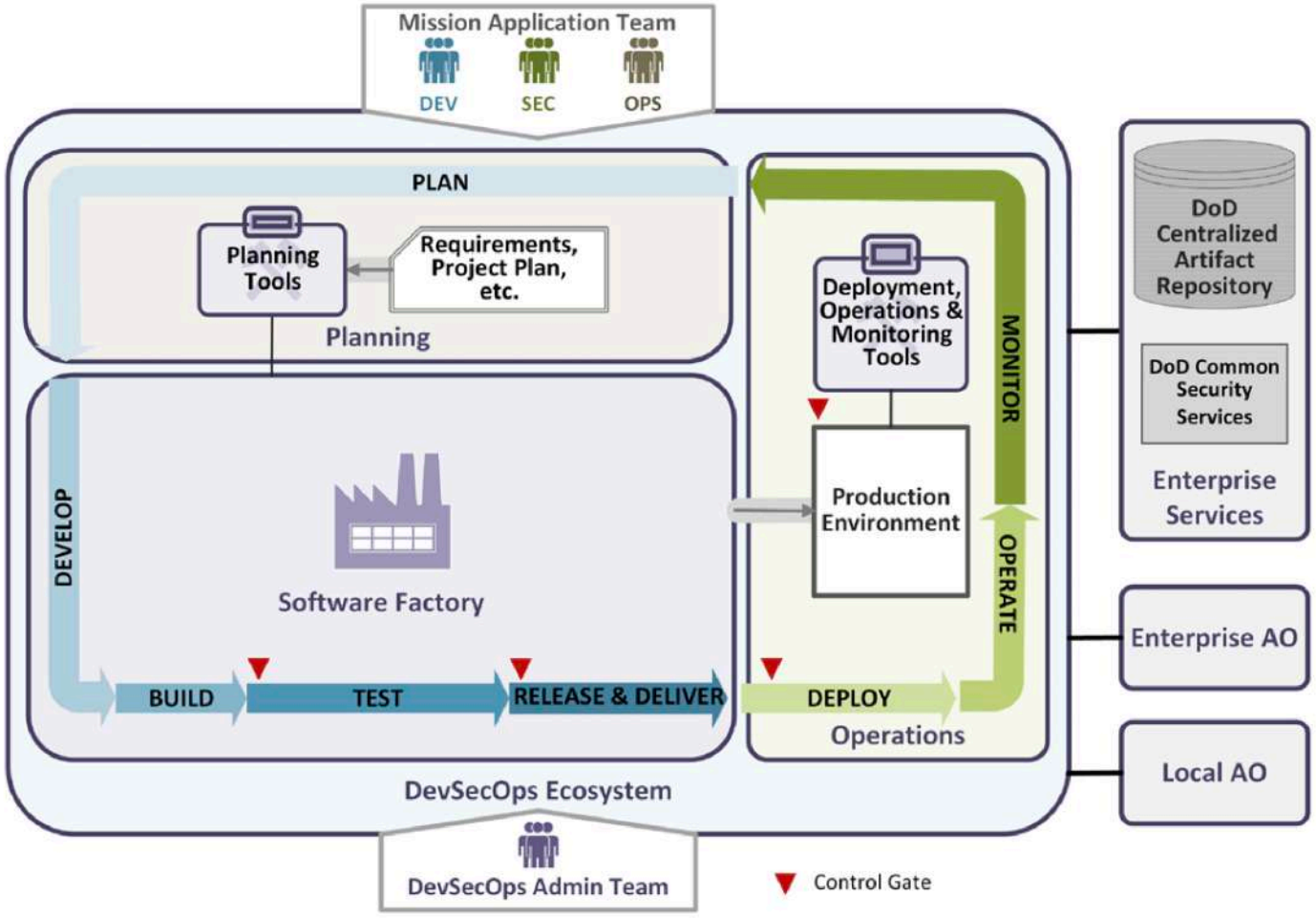


Figure 8: DevSecOps Ecosystem

DevSecOps Software Factory

Test environments：
Unit tests
Static code analysis
Functional tests
Interface tests
Dynamic code analysis

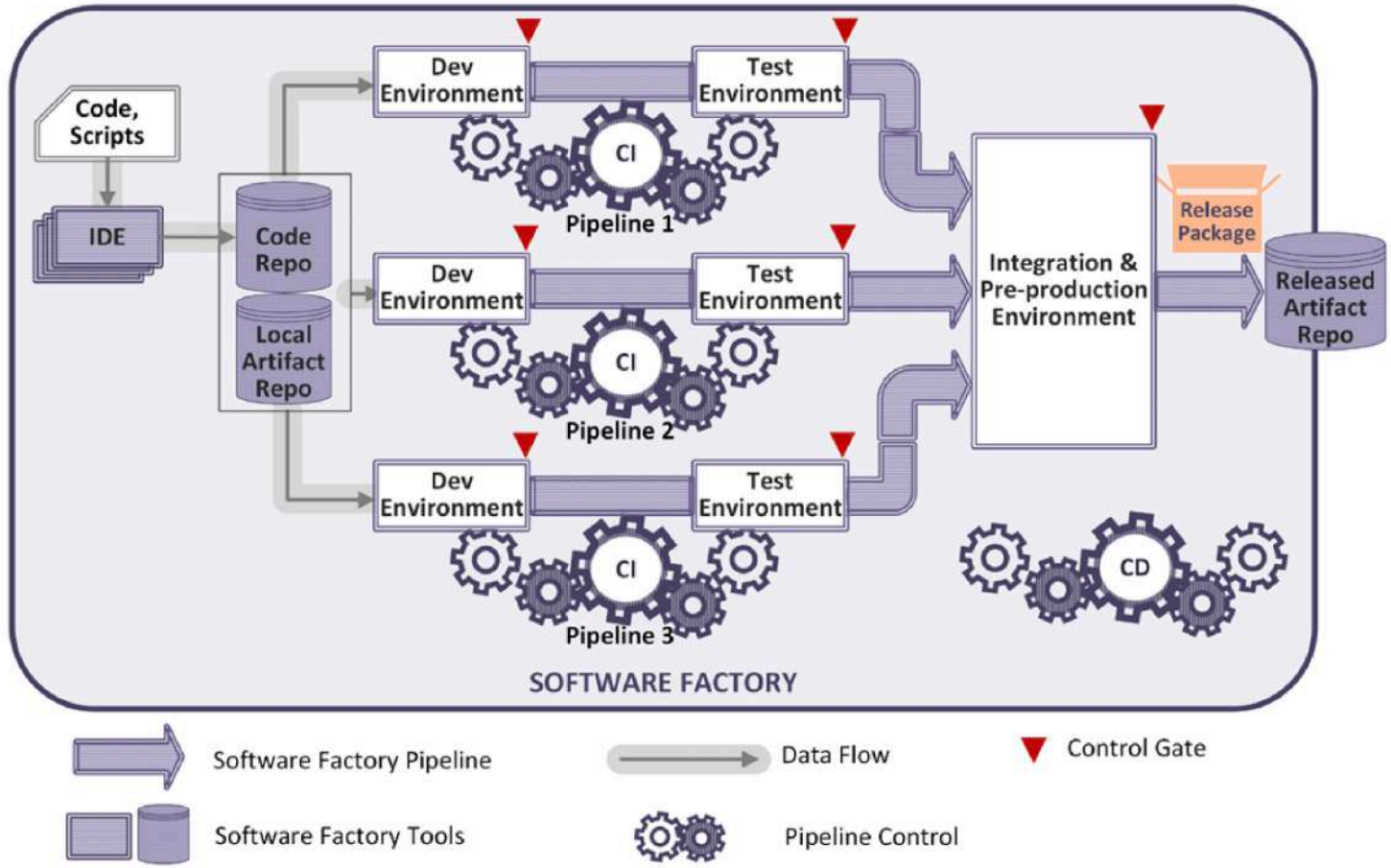


Figure 9: DevSecOps Software Factory

Plan

Activities	Description	Inputs	Outputs	Tool Dependencies
DevSecOps ecosystem design	Design the DevSecOps process workflows that are specific to this project	- Change management process; - System design; - Release plan & schedule.	DevSecOps process flow chart; DevSecOps ecosystem tool selection; Deployment platform selection	Team collaboration system
Project team onboarding planning	Plan the project team onboarding process, interface, access control policy	Organization policy	Onboarding plan	Team collaboration system
Change management planning	Plan the change control process	- Organizational policy; - Software development best practice.	Change control procedures; Review procedures; Control review board; change management plan	Team collaboration system; Issue tracking system
Configuration management (CM) planning	Plan the configuration control process; Identify configuration items	- Software development, security and operations best practice; - IT infrastructure asset; - Software system components.	CM processes and plan; CM tool selection; Responsible configuration items; Tagging strategy	Team collaboration system; Issue tracking system
Software requirement analysis	Gather the requirements from all stakeholders	- Stakeholder inputs or feedback; - Operation monitoring feedback; - Test feedback.	-Feature requirements -Performance requirements -Privacy requirements -Security requirements	Team collaboration system; Issue tracking system
System design	Design the system based the requirements	Requirements documents	Documents: -System architecture -Functional design -Data flow diagrams -Test plan -Infrastructure configuration plan -Tool selections -Development tool -Test tool -Deployment platform	Team collaboration system; Issue tracking system Software system design tools

Plan

Activities	Description	Inputs	Outputs	Tool Dependencies
Project planning	Project task management Release planning		Task plan & schedule; Release plan & schedule.	Team collaboration system; Project management system
Risk management	Risk assessment	- System architecture; - Supply chain information; - Security risks.	Risk management plan	Team collaboration system;
Configuration identification	Discover or manual input configuration items into CMDB; Establish system baselines	-IT infrastructure asset; - Software system components (include DevSecOps tools); -code baselines -document baselines.	Configuration items	CMDB; Source code repository; Artifact repository; Team collaboration system
Threat modeling	Identify potential threats, weaknesses and vulnerabilities. Define the mitigation plan	System design	Potential threats and mitigation plan	Threat modeling tool
Database design	Data modeling; database selection; Database deployment topology	System requirement; System design	Database design document	Data modeling tool; Team collaboration system
Design review	Review and approve plans and documents	Plans and design documents;	Review comments; Action items	Team collaboration system
Documentation version control	Track design changes	Plans and design documents;	Version controlled documents	Team collaboration system

Dev

Activities	Description	Inputs	Outputs	Tool Dependencies
Application code development	Application coding	Developer coding input	Source code	IDE
Infrastructure code development	-System components and infrastructure orchestration coding -Individual component configuration script coding	Developer coding input	Source code	IDE
Security code development	Security policy enforcement script coding	Developer coding input	Source code	IDE
Test development	Develop detailed test procedures, test data, test scripts, test scenario configuration on the specific test tool	Test plan	Test procedure document; Test data file; Test scripts	IDE; Specific test tool
Database development	Implement the data model using data definition language or data structure supported by the database; Implement triggers, views or applicable scripts; Implement test scripts, test data generation scripts.	Data model	Database artifacts (including data definition, triggers, view definitions, test data, test data generation scripts, test scripts, etc.)	IDE or tools come with the database software
Code commit	Commit source code into version control system	Source code	Version controlled source code	Source code repository
Code commit scan	Check the changes for sensitive information before pushing the changes to the main repository. If it finds suspicious content, it notifies the developer and blocks the commit.	Locally committed source code	Security findings and warnings	Source code repository security plugin
Code review	Perform code review to all source code. Note that pair programming counts.	Source code	Review comments	Code quality review tool
Documentation	Detailed implementation documentation	User input; Source code	Documentation; Auto generated Application Programming Interface (API) documentation	IDE or document editor or build tool
Static code scan before commit	Scan and analyze the code as the developer writes it. Notify developers of potential code weakness and suggest remediation.	Source code; known weaknesses	source code weakness findings	IDE security plugins
Container or VM hardening	Harden the deliverable for production deployment	Running VM or container	Vulnerability report and recommended mitigation	Container security tool Security compliance tool

Build

Activities	Description	Inputs	Outputs	Tool Dependencies
Build	Compile and link	Source code; dependencies	Binary artifacts	Build tool; Lint tool; Artifact repository
Static application security test and scan	Perform SAST to the software system	Source code; known vulnerabilities and weaknesses	Static code scan report and recommended mitigation.	SAST tool
Dependency vulnerability checking	Identify vulnerabilities in the open source dependent components	Dependency list or BOM list	Vulnerability report	Dependency checking / BOM checking tool
Containerize	Packages all required components OS, developed code, libraries, etc.) into a hardened container	Container base image; Container build file	Container image	Container builder
Release packaging	Package binary artifacts, container or VM images, infrastructure configuration scripts, proper test scripts, documentation, checksum, digital signatures, and release notes as a package.	Binary artifacts; Scripts; Documentation; Release notes	Released package with checksum and digital signature	Release packaging tool
Store artifacts	Store artifacts to the artifact repository	Binary artifacts; Database artifacts; Scripts; Documentation; Container images	Versioned controlled artifacts	Artifact Repository
Build configuration control and audit	Track build results, SAST and dependency checking report; Generate action items; Make go/no-go decision to the next phase	Build results; SAST report; Dependency checking report	Version controlled build report; Action items; Go/no-go decision	Team collaboration system; Issue tracking system; CI/CD orchestrator

Testing

Activities	Description	Inputs	Outputs	Tool Dependencies
Unit test	Assist unit test script development and unit test execution. It is typically language specific.	Unit test script, individual software unit under test (a function, method or an interface), test input data, and expected output data	Test report to determine whether the individual software unit performs as designed.	Test tool suite, Test coverage tool
Dynamic application security test and scan	Perform DAST or IAST testing to the software system	Running application and underlying OS; fuzz inputs	Vulnerability, static code weakness and/or dynamic code weakness report and recommended mitigation	DAST tool or IAST tool
Integration test	Develops the integration test scripts and execute the scripts to test several software units as a group with the interaction between the units as the focus.	Integration test scripts, the software units under test, test input data, and expected output data	Test report about whether the integrated units performed as designed.	Test tool suite
System test	System test uses a set of tools to test the complete software system and its interaction with users or other external systems.	System test scripts, the software system and external dependencies, test input data and expected output data	Test result about if the system performs as designed.	Test tool suite
Manual security test	Such as penetration test, which uses a set of tools and procedures to evaluate the security of the system by injecting authorized simulated cyber-attacks to the system. CI/CD orchestrator does not automate the test, but the test results can be a control point in the pipeline.	Running application, underlying OS, and hosting environment	Vulnerability report and recommended mitigation	Varies tools and scripts (may include network security test tool)
Performance test	Ensure applications will perform well under the expected workload. The test focus is on application response time, reliability, resource usage and scalability.	Test case, test data, and the software system	Performance metrics	Test tool suite, Test data generator
Regression test	A type of software testing to confirm that a recent program or code change has not adversely affected existing features.	Functional and non- functional regression test cases; the software system	Test report	Test tool suite

Testing

Activities	Description	Inputs	Outputs	Tool Dependencies
Acceptance test	Conduct operational readiness test of the system. It generally includes: Accessibility and usability test failover and recovery test performance, stress and volume test security and penetration test interoperability test compatibility test supportability and maintainability	The tested system Supporting system Test data	Test report	Test tool suite, Non-security compliance scan
Container policy enforcement	Check developed containers to be sure they meet container policies	Container, Policies in SCAP form	Container compliance report	Container policy enforcement
Compliance scan	Compliance audit	Artifacts; Software instances; System components	Compliance reports	Non-security compliance scan; Software license compliance checker; Security compliance tool
Test audit	Test audit keeps who performs what test at what time and test results in records	Test activity and test results	Test audit log	Test management tool
Test deployment	Deploy application and set up testing environment using Infrastructure as Code	Artifacts (application artifacts, test code) Infrastructure as Code	The environment ready to run tests	Configuration automation tool; IaC
Database functional test	Perform unit test and functional test to database to verify the data definition, triggers, constrains are implemented as expected	Test data	Test results	Database test tools
Database non- functional test	Conduct performance test, load test, and stress test; Conduct failover test	Test data; Test scenarios	Test results	Database test tools
Database security test	Perform security scan; Security test	Test data; Test scenarios	Test results	Vulnerability findings; Recommended mitigation actions
Test configuration control and audit	Track test and security scan results; Generate action items; Make go/no-go decision to the next phase.	Test results; Security scan and compliance scan report	Version controlled test results; Action items; Go/no-go decision	Team collaboration system; Issue tracking system; CI/CD orchestrator

Release

Activities	Description	Inputs	Outputs	Tool Dependency
Release go / no- go decision	This is part of configuration audit; Decision on whether to release artifacts to the artifact repository for the production environment.	Design documentation; Test reports; Security test and scan reports; Artifacts	go / no-go decision; Artifacts are tagged with release tag if go decision is made	CI/CD Orchestrator
Deliver released artifacts	Push released artifacts to the artifact repository	The release package	New release in the artifact repository	Artifacts repository
Artifacts replication	Replicate newly release artifacts to all regional artifact repositories	Artifacts	Artifacts in all regional artifact repositories	Artifacts repositories (release, regional)

Deploy

Activities	Description	Inputs	Outputs	Tool Dependency
Artifact download	Download newly release artifacts from the artifact repository	Artifact download request	Requested artifacts	Artifact repository
Infrastructure provisioning automation	Infrastructure systems auto provisioning (such as software defined networking, firewalls, DNS, auditing and logging system, user/group permissions, etc.)	Infrastructure configuration scripts / recipes / manifests / playbooks	Provisioned and configured infrastructure	Configuration automation tools; IaC
Create linked clone of VM master image	Instantiate VM by creating a link clone of parent VM with master image	VM parent New VM instance parameters	New VM instance	Virtualization Manager
Deliver container to container registry	Upload the hardened container and associated artifacts to the container registry	Hardened container	New container instance	CNCF-certified Kubernetes; Artifact repository container registry
Post-deployment security scan	System and infrastructure security scan	Access to system components and infrastructure components	Security vulnerability findings	Security compliance tool
Post-deployment checkout	Run automated test to make sure the important functions of system are working	Smoke test scenarios and test scripts	Test results	Test scripts
Database installation and database artifact deployment	Database software installation; Cluster or high availability setup; Database artifacts deployment and data loading	Artifacts in the repository; data	Running database system	Artifact repository; Database automation tool; Data masking or encryption tool if needed

U.S. AIR FORCE

Plan Operation

Activities	Description	Inputs	Outputs	Tool Dependency
Backup	Data backup; System backup	Access to backup system	Backup data or image	Backup management; Database automation tool
Scale	Scale manages VMs/containers as a group. The number of VMs/containers in the group can be dynamically changed based on the demand and policy.	Real-time demand and VM/container performance measures Scale policy (demand or Key Performance Indicator (KPI)threshold; minimum, desired, and maximum number of VMs/containers)	Optimized resource allocation	VM management capability on the hosting environment; Container management on the hosting environment
Load balancing	Load balancing equalizes the resource utilization	Load balance policy Real time traffic load and VM/container performance measures	Balanced resource utilization	VM management capability on the hosting environment; Container management on the hosting environment

Monitor

Activities	Description	Inputs	Outputs	Tool Dependencies
Logging	Log system events	All user, network, application, and data activities	Logs	Logging
Log analysis & auditing	Filter or aggregate logs; Analyze and correlate logs	Logs	Alerts and remediation report	Log aggregator Log analysis & auditing
System performance monitoring	Monitor system hardware, software, database, and network performance; Baselining system performance; Detect anomalies	Running system	Performance KPI measures; Recommended actions; Warnings or alerts	Operation monitoring Issue tracking system; Alerting and notification;
System Security monitoring	Monitor security of all system components Security vulnerability assessment System security compliance scan	Running system	Vulnerabilities; Incompliance Findings; assessments and recommendations; Warnings and alerts.	ISCM; Issue tracking system; Alerting and notification; Operations dashboard
Asset Inventory	Inventory system IT assets	IT assets	Asset inventory	Inventory Management;
System configuration monitoring	System configuration (infrastructure components and software) compliance checking, analysis, and reporting	Running system configuration; Configuration baseline	Compliance report; Recommended actions; Warnings and alerts	ISCM; Issue tracking system; Alerting and notification; Operations dashboard
Database monitoring and security auditing	Database performance and activities monitoring and auditing	Database traffic, event, and activities	Logs; Warnings and alerts	Database monitoring tool; Database security audit tool; Issue tracking system; Alerting and notification; Operations dashboard

Security in DevSecOps

Activities	Phase	Activities Table Reference	Tool Dependencies	Tool Table Reference
Threat modeling	Plan	Table 4	Threat modeling tool	Table 3
Security code development	Develop	Table 7	IDE	Table 6
Static code scan before commit	Develop	Table 7	IDE security plugins	Table 6
Code commit scan	Develop	Table 7	Source code repository security plugin	Table 6
Container or virtual machine hardening	Develop	Table 7	Container security tool Security compliance tool	Table 10
Static application security test and scan	Build	Table 9	SAST tool	Table 8
Dependency vulnerability checking	Build	Table 9	Dependency checking / BOM checking tool	Table 8
Dynamic application security test and scan	Test	Table 11	DAST tool or IAST tool	Table 10
Manual security testing (such as penetration test)	Test	Table 11	Varies tools and scripts (may include network security test tool)	Table 10
Container policy enforcement	Test	Table 11	Container policy enforcement	Table 10
Post-deployment security scan	Deploy	Table 15	Security compliance tool	Table 10
System Security monitoring	Monitor	Table 19	Information Security Continuous Monitoring (ISCM)	Table 18

U.S. AIR FORCE

DevSecOps Product Stack (1)

Source Repository
GitHub Government
GitLab

Container Management technologies:
Kubernetes
Openshift
VMWare Tanzu
PKS
OKD
Rancher (K8S only)
D2IQ (K8S only)
Docker EE (K8S only)

Container Packagers:
Helm
Kubernetes Operators

API Gateways
Kong
Azure API
AWS API
Axway
3Scale
Apigee
ISTIO (service mesh)

Artifacts
Artifactory
Nexus
Maven
Archiva
S3 bucket

Programming Languages
C/C++
C#/.NET
.NET Core
Java
PHP
Python
Groovy
Ruby
R
Rust
Scala
Perl
Go
Node.JS
Swift

Databases
SQL Server
MySQL
PostgreSQL
MongoDB
SQLite
Redis
Elasticsearch
Oracle
etcd
Hadoop/HDInsight
Cloudera
Oracle Big Data
Solr
Neo4J
Memcached
Cassandra
MariaDB
CouchDB
InfluxDB (time)

U.S. AIR FORCE

DevSecOps Product Stack (2)

Message bus/Streams
Kafka
Flink
Nats
RabbitMQ
ActiveMQ

Proxy
Oauth2 proxy
nginx ldap auth proxy
openldap
HA Proxy

Visualization
Tableau
Kibana

Logs
Logstash
Splunk Forwarder
Fluentd
Syslogd
Filebeat
rsyslog

Webservers
Apache2
Nginx
IIS
Lighttpd
Tomcat

Docker base images OS:
~~Alpine~~
~~Busybox~~
~~Ubuntu~~
~~Centos~~
~~Debian~~
~~Fedora~~
Universal Base Image

Serverless
Knative

U.S. AIR FORCE

DevSecOps Product Stack (3)

Build
MSBuild
CMake
Maven
Gradle
Apache Ant

Tests suite
Cucumber
J-Unit
Selenium
TestingWhiz
Watir
Sahi
Zephyr
Vagrant
AppVerify
nosetests
SoapUI
LeanFT

Test coverage
JaCoCo
Emma
Cobertura
codecov

CI/CD Orchestration
Jenkins (open source)
CloudBees Jenkins
GitLab

Jenkins plugins
Dozens (Need to verify security).

Configuration Management / Delivery
Puppet
Chef
Ansible
Saltstack

Security
Tenable / Nessus Agents
Fortify
Twistlock
Aqua
SonarQBE
Qualys
StackRox
Aporeto
Snort
OWASP ZAP
Contrast Security
OpenVAS
Metasploit
ThreadFix
pylint
JFrog Xray
OpenSCAP (can check against DISA STIG)
OpenControl for compliance documentation

Security (2)
Snyk
Code Climate
AJAX Spider
Tanaguru (508 compliance)
InSpec
OWASP Dependency-Check
Burp
HBSS
Anchore
Checkmarx
SD Elements
Clair
Docker Bench Security
Notary
Sysdig
Layered Insight
BlackDuck
Nexus IQ/Lifecycle/Firewall

U.S. AIR FORCE

DevSecOps Product Stack (4)

Monitoring
Sensu
EFK (Elasticsearch, Fluentd, Kibana)
Splunk
Nagios
New Relic
Sentry
Promotheus
Grafana
Kiali

Collaboration
Rocket.Chat
Matter.Most
PagerDuty

Plan
Jira
Confluence
Rally
Redmine
Pivotal Tracker

Secrets
Kubernetes Secrets
Vault
Credentials (Jenkins)
CryptoMove

SSO
Keycloak

Documentation
Javadoc
RDoc
Sphinx
Doxygen
Cucumber
phpDocumentator
Pydoc

Performance
Apache AB
Jmeter
LoadRunner

DoD Security Defense

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS); malware detection; data loss prevention; host-based security; log/telemetry aggregation and analysis; and Identity, Credential, and Access Management (ICAM). A Cybersecurity Service Provider (CSSP) will provide additional services, including Attack Sensing and Warning (ASW), Forensic Media Analysis (FMA), Assurance Vulnerability Management (AVM), Incident Reporting (IR), Incident Handling Response (IHR), Information Operations Condition (INFOCON), Cyber Protection Condition (CPCON), Malware Notification Protection (MNP), and Network Security Monitoring (NSM).

INFOCON 5描述了没有针对计算机网络的明显敌对活动的情况。监视所有信息系统的运行性能，并将密码系统用作保护层。
INFOCON 4描述了增加的攻击风险。必须加强对所有网络活动的监视，所有国防部最终用户必须确保其系统安全。互联网使用可能仅限于政府站点，将文件备份到可移动媒体是理想的选择。
INFOCON 3描述了何时识别风险。重要系统的安全审查是当务之急，计算机网络防御系统的警觉性得到了提高。所有未分类的拨号连接已断开连接。
INFOCON 2描述何时发生攻击，但计算机网络防御系统未处于最高警报状态。非必需网络可以脱机，并且可以实现替代的通信方法。
INFOCON 1描述何时发生攻击以及计算机网络防御系统处于最大警报状态。任何受损的系统都与网络的其余部分隔离。

U.S. AIR FORCE

Self-Learning (1)

- Recommended Videos (Part 1)
  - Watch our playlists, available at different expertise levels and continuously augmented!
  - Kafka / KSQL (message bus, pub/sub, event driven):
    - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLIzz0zt03Ludtid7icrXBesg
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIxxXX0oCzt7laO6mD61UIQw
    - Advanced: N/A
  - Kubernetes
    - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLIydFzQzkYYDdQK7k5cEKubQ
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIx8dSFH_jFLK40Tt7KUXTN_
    - Advanced: https://www.youtube.com/playlist?list=PLSIv_F9TtLIytdAJiVqbHucWOvn5LrTNW

U.S. AIR FORCE

Self-Learning (2)

- Recommended Videos (Part 2)
  - Watch our playlists, available at different expertise levels and continuously augmented!
  - Service Mesh
    - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLIxtC4rDIMQ8QiG5UBCjz7VH
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIwWK_Y_Cas8Nyw-DsdbH6vl
    - Advanced: https://www.youtube.com/playlist?list=PLSIv_F9TtLIx8VW2MFONMRwS_-2rSJwdn
  - Microservices
    - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLIz_U2_RaONTGYLkz0lh-A_L
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIxqjuAXxoRMjvspaEE8L2cB
    - Advanced: https://www.youtube.com/playlist?list=PLSIv_F9TtLIw4CF4F4t3gVV3j0512CMsu

U.S. AIR FORCE

Self-Learning (3)

- Recommended Books
  - A Seat at the Table – by Mark Schwartz (former CIO of USCIS, leader in Agile)

    This book is highly recommended for ALL leadership as it is not technical but focused on the challenges around business, procurement and how leadership can enable DevOps across the organization and remove impediments.
  - The Phoenix Project – by the founders of DevOps
  - The DevOps Handbook – by Gene Kim, Patrick Debois.

For those who drive to work like me (for hours), please note that these books are available as Audiobooks.

Thank you!

ThreatSource