MICRO FOCUS

Government Solutions

The Cloud, the Software Factory and Application Security

What goes where and how does this all fit together

Scott Snowden – CISSP, CSSLP, CEH

Director of DoD Software Security Engineering

Key Message

Moving your application to the Cloud may make it more secure and reliable, but there are many controls and requirements that are still your responsibility.

You need to know what is addressed how and where.

MICRO FOCUS

Agenda - Application Security in the Cloud

- USAF Strategic Direction
- The Cloud – a level set
- Modern software development overview
- Application Security
- Putting it all together

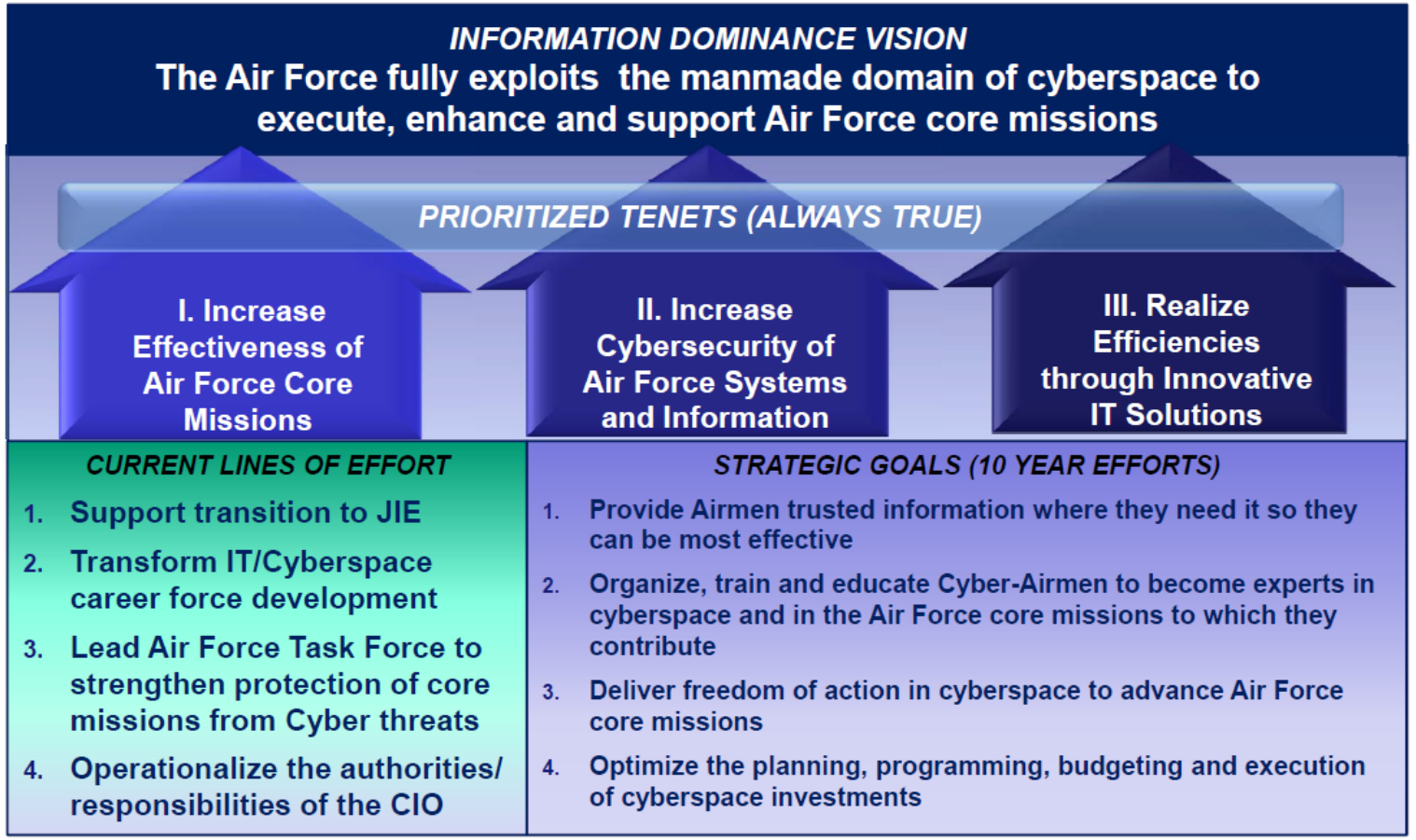
Disclaimer: The views expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

MICRO FOCUS

USAF Strategy and Vision

SAF/CIO A6 Mission Brief

- Increase resiliency, survivability, and cybersecurity of its information and systems
- Overlap with Cloud, Software Factories and Application Security



Reference: https://www.safcioa6.af.mil/

MICRO FOCUS

USAF SAF CIO A6

SAF/CIO A6 Vision: The Air Force fully exploits the man-made domain of cyberspace to execute, enhance and support Air Force core missions.

- **A6 Initiative - Cloud Computing**: In partnership with DISA, the DoD Cloud Broker, the Air Force is exploring the use of Cloud Computing to deliver ubiquitous access to relevant data at the point of need.
- **Air Force Information Dominance Flight Plan (Feb, 2017)**
  - Objective 1.6 – Develop and employ **cyberspace risk methodology**
    - Identify mission-critical cyber assets and assure they operate in a contested env.
  - Objective 1.3 – **Increase cybersecurity** and resiliency of weapon and mission systems
  - Objective 2.1 – Optimize Information and Intelligence Networks
    - **Harness cloud computing** … to increase mission effectiveness and cybersecurity while reducing costs
- **Air Force Policy Directive 17-2 - Cyber Operations**
  - 2.3. AFIN Operations are actions taken to design, build, configure, secure, operate, maintain, and sustain AF IT, to include Platform IT (PIT), cyber enabled systems/weapons systems, and National Security Systems (NSS), in a way that creates and preserves data availability, integrity and confidentiality.

MICRO FOCUS

The Cloud

The Cloud is Just Someone Else's Computer?

NIST Definition

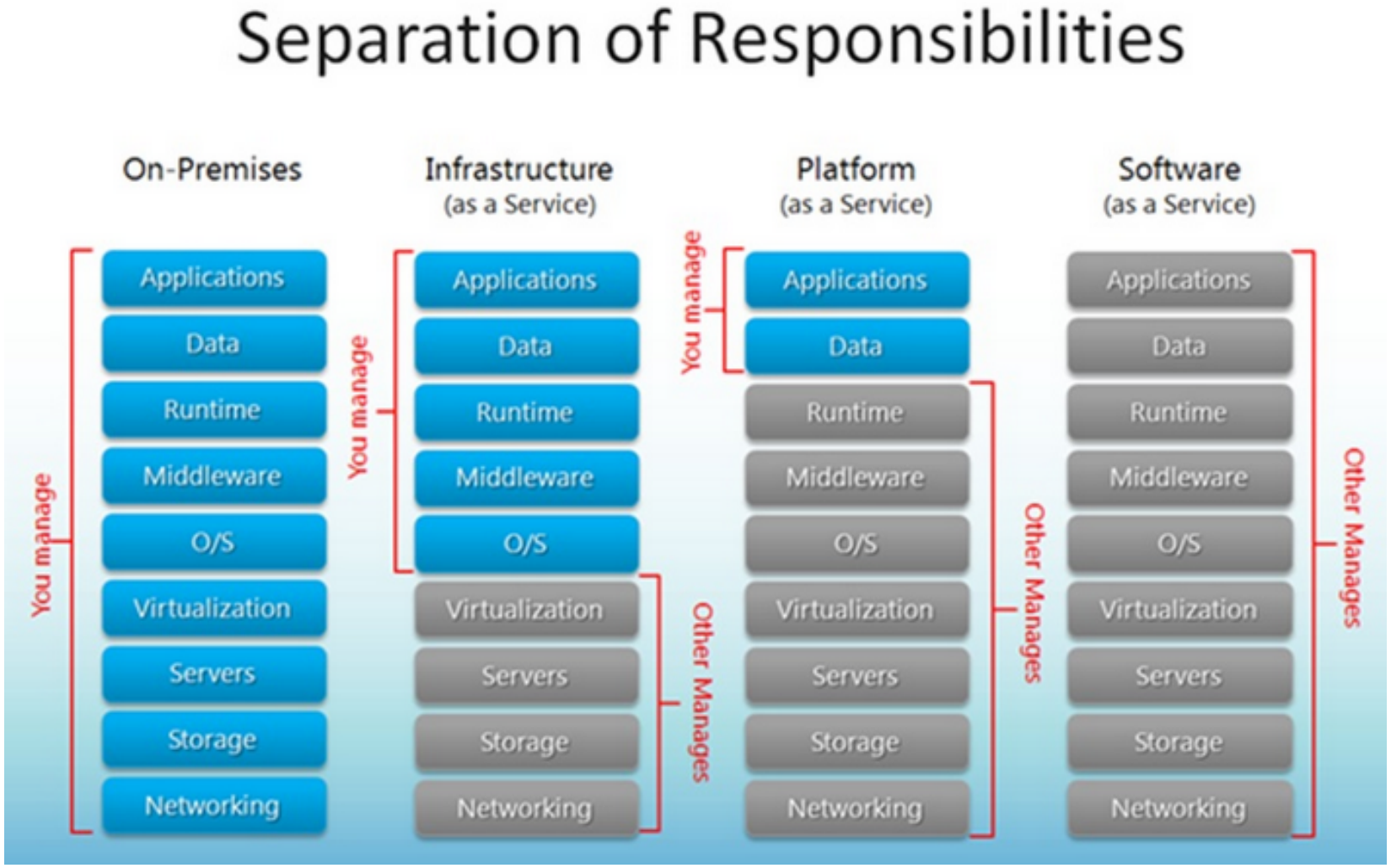
- **On-demand self-service**: The ability for an end user to sign up and receive services without the long delays that have characterized traditional IT.
- **Broad network access:** The ability to access the service via standard platforms (desktop, laptop, mobile, etc.).
- **Resource pooling:** Resources are pooled across multiple customers.
- **Rapid elasticity:** Capability can scale to cope with demand peaks.
- **Measured service:** Billing is metered and delivered as a utility service.

Cloud Service Categories

- **Infrastructure as a Service (IaaS):** A way of delivering cloud computing infrastructure (servers, storage, network, and operating systems) as an on-demand service.
- **Platform as a Service (PaaS):** A computing platform that allows the creation of web applications quickly and easily. *(AWS, Azure, AWS Elastic Beanstalk, Cloud Foundry, OpenShift, Google App Engine, Heroku)*
- **Software as a Service (SaaS):** Software that is deployed over the internet.

MICRO FOCUS

Cloud Service Categories



Source: http://headinthe.cloud/iaas-vs-paas-vs-saas/

Key Cloud Use Cases

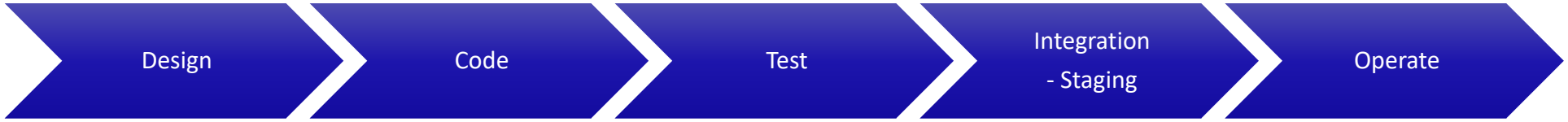
- SaaS: GitHub, Office 365, Slack
  - out of scope – common

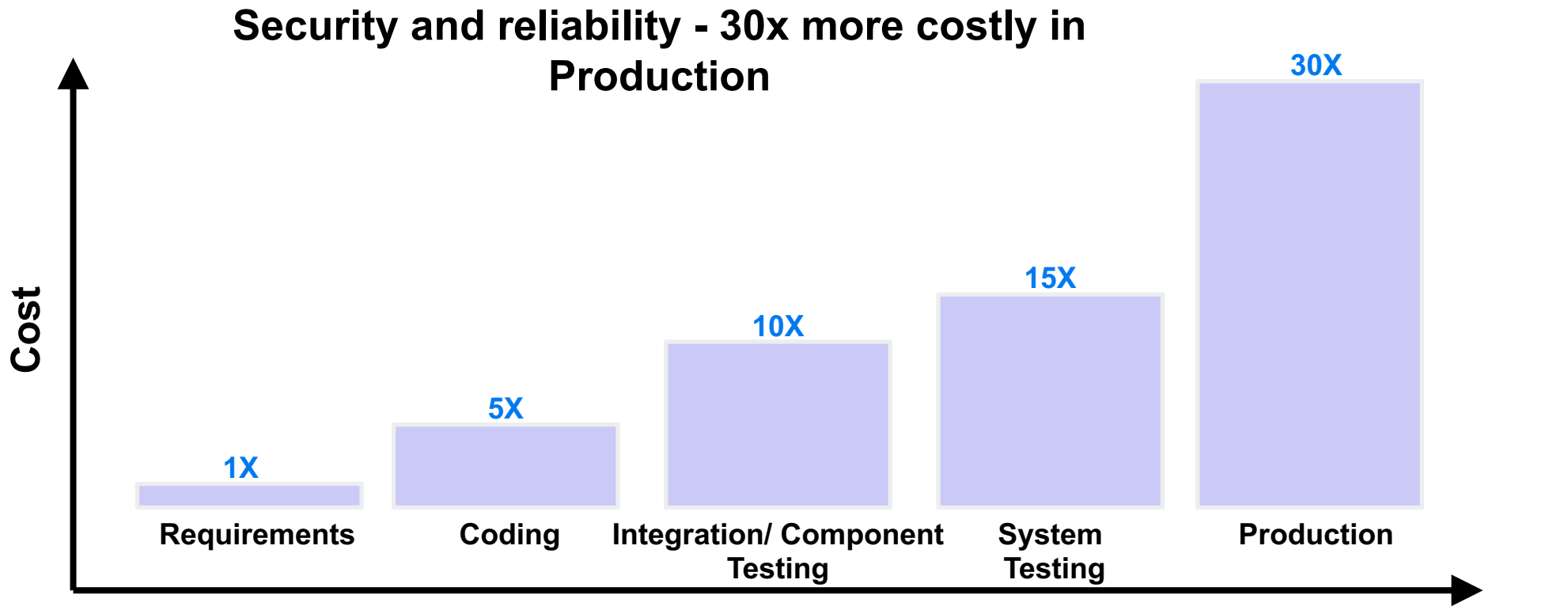
- Application development environment
  - Developers using cloud based resources to write code - somewhat uncommon
- Dev/test environment
  - Compiling, assembling, and testing new code - common
- System integration environment
  - Assembling and packaging multiple components into a system and testing said system - common
- Production hosting
  - Deploying and operating system in a cloud environment - common

MICRO FOCUS

Software Development

Software Development Lifecycle (SDLC)





Source: NIST

MICRO FOCUS

Software Factory

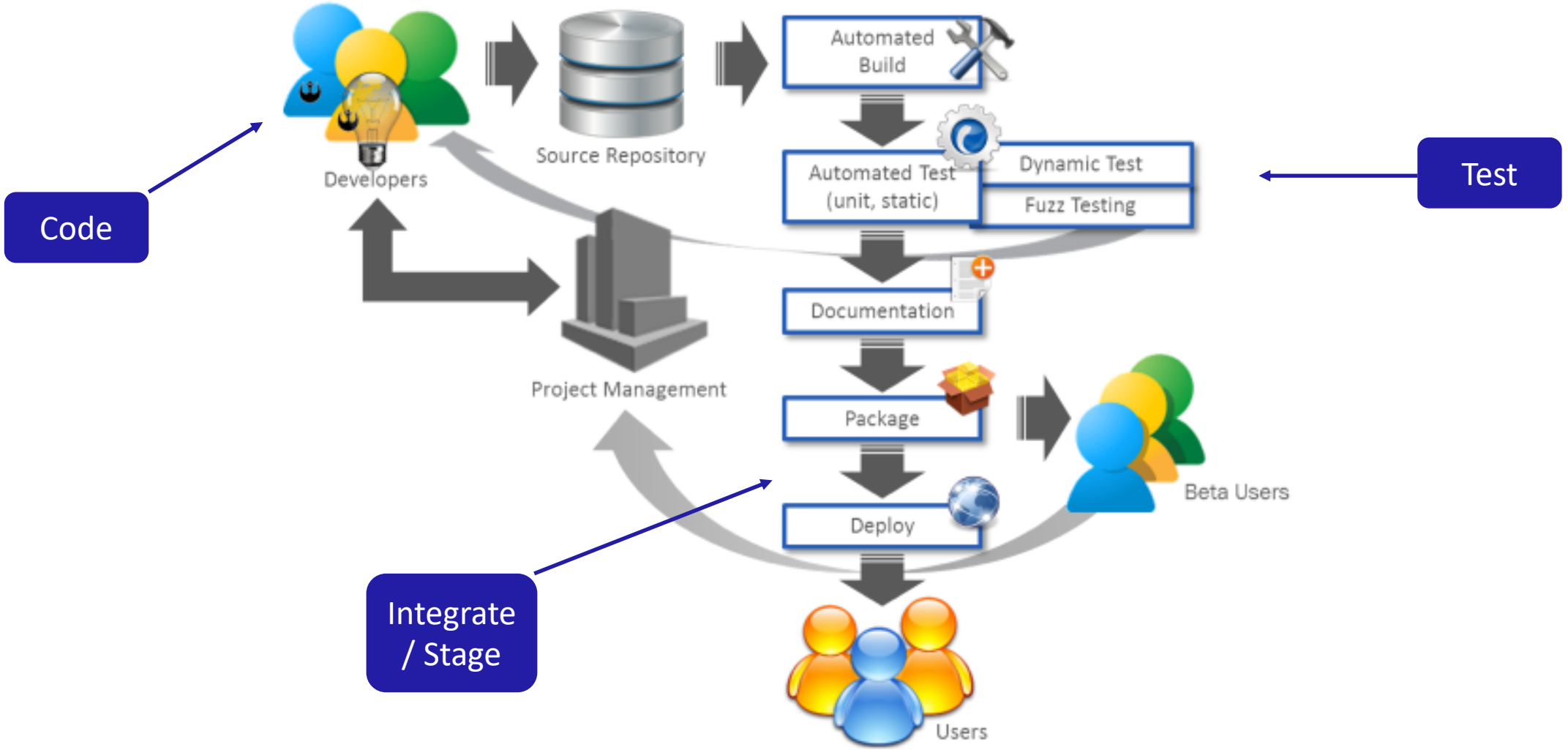
"a set of software tools that programmers use to write their code, confirm it meets style and other requirements, collaborate with other members of the programming team, and automatically build, test, and document their progress."

- Requirements management
- Source Code Repository
- Integrated Development Environment (IDE)
- Testing framework
- Testing tools: performance, functional and security
- Issue tracking
- Configuration management
- Continuous Integration / Continuous Deployment
- **Infrastructure (Cloud – IaaS, PaaS)**
- Log Monitoring software – ArcSight, ELK, Logstash, Splunk, etc

Reference: DSB – Design and Acquisition of Software for Defense Systems (Feb 2018)

MICRO FOCUS

Software Factory



Application Security

Bad Software - CVE vs. CWE

Known vulnerability vs. undisclosed potential vulnerability (Zero Days)

CWE: Common Weakness Enumeration

- Weakness in software that could affect the security of the system and may or may not result in a vulnerability

CVE: Common Vulnerability Enumeration

- Known publically disclosed vulnerabilities in software

CVSS: Common Vulnerability Scoring System

- Requires human input related to a number of metrics to calculate a severity score

OVAL: Open Vulnerability Assessment Language

- Represent and communicate the system characteristics, machine state and results of a vulnerability assessment

Note: cve.mitre.org, cwe.mitre.org, https://danielmiessler.com/blog/mitre-quick-reference/

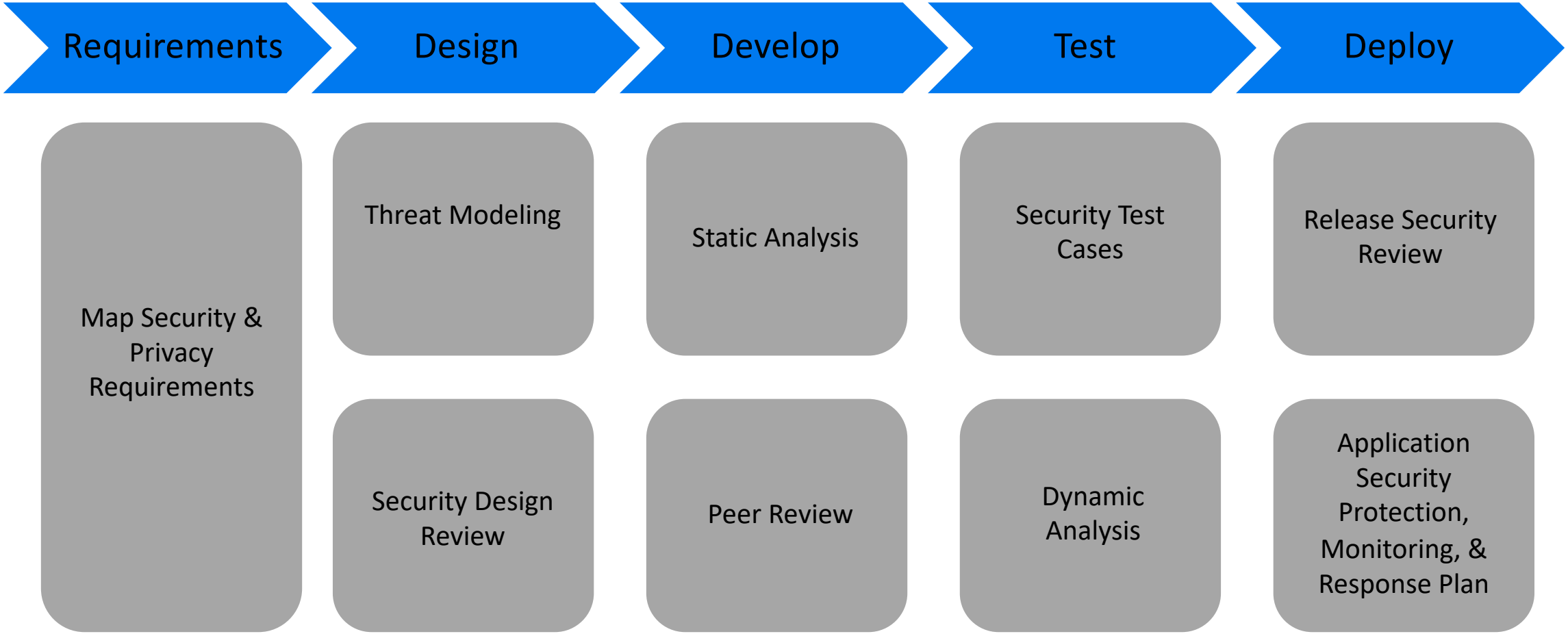
MICRO FOCUS

Traditional Application Security Tasks

- Security Architecture design/review
- Threat modeling
- Source code review (Static Analysis - Fortify)
- Automated fuzzing/penetration testing (Dynamic Analysis - WebInspect)
- Manual Pen testing
- Documentation
- Verification and Validation
- Monitoring and Audit Logs

MICRO FOCUS

Application/Software Security Assurance Life Cycle



MICRO FOCUS

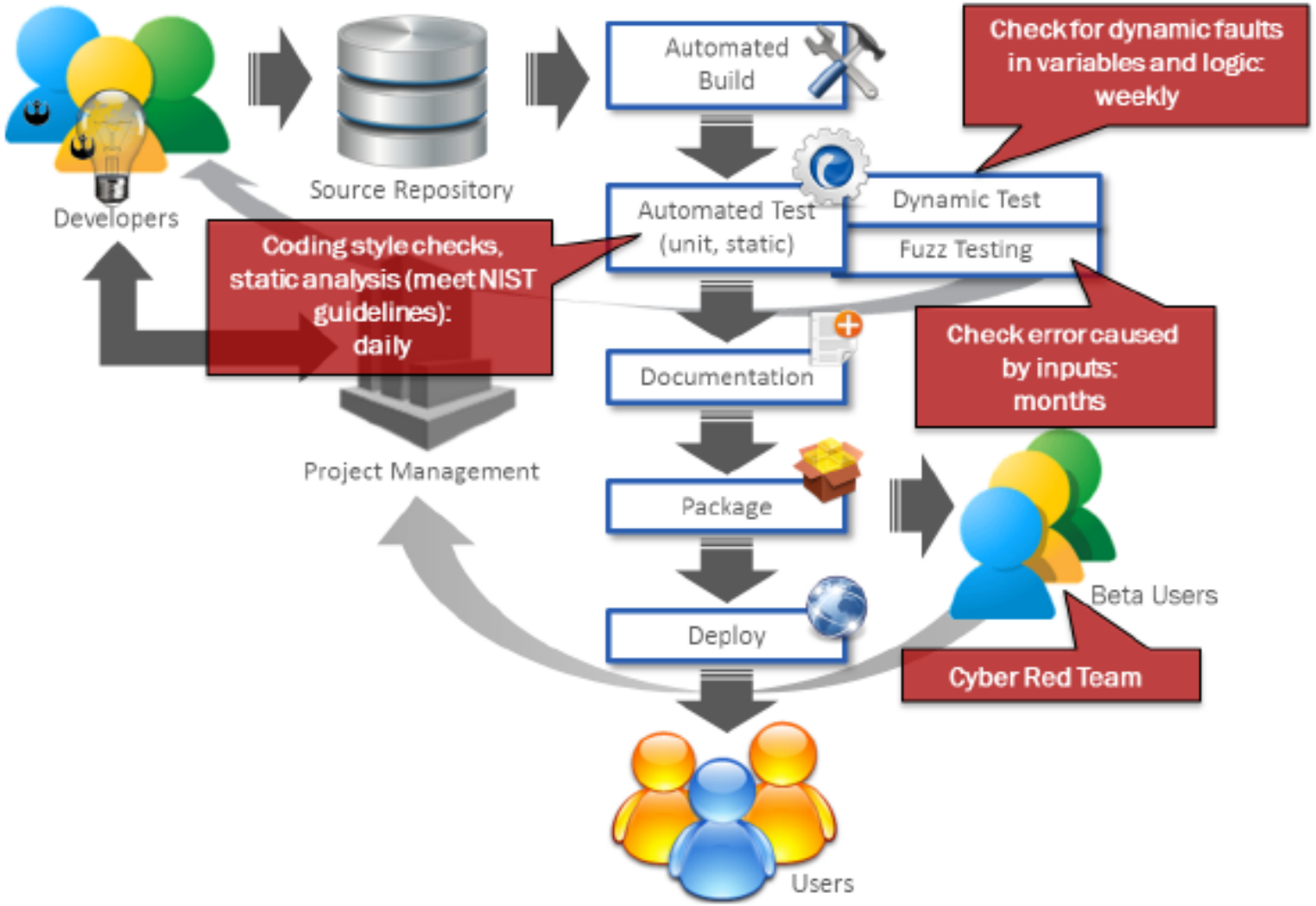
Application Security and Development Stig v4.7

Most controls are implemented by the application not underlying infrastructure

- 290 total controls
- Primary categories
  - Application functionality
  - Policies and process
  - External validation
  - Architecture
  - Documentation
- Many are specific to the application itself: SQLi, XSS, Command Injection, Privacy Violation, etc
- ~150 can be identified statically or dynamically

MICRO FOCUS

Application Dev Processes + Security



Reference: DSB – Design and Acquisition of Software for Defense Systems (Feb 2018)

Putting it all Together

Cloud System Security Responsibility

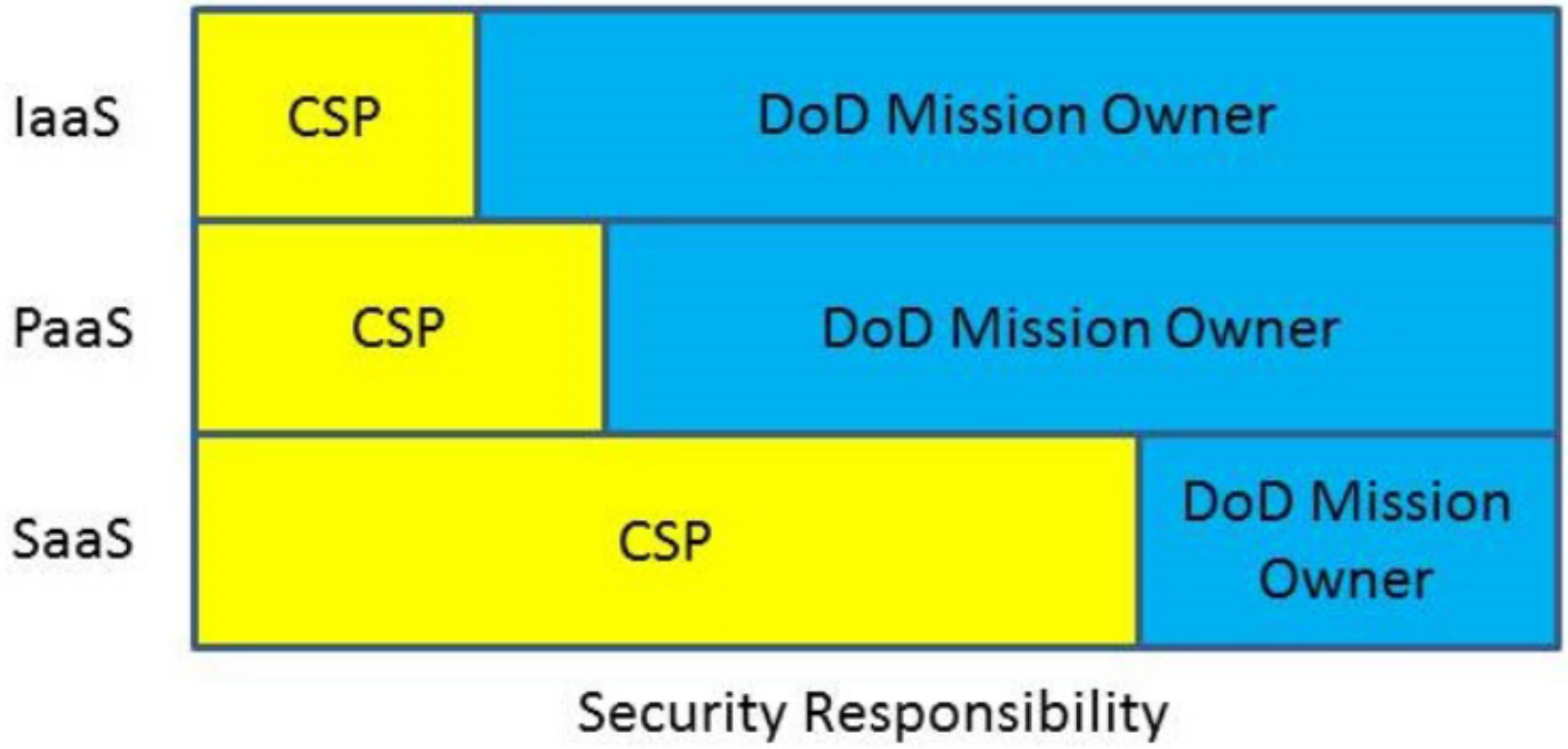


Figure 1 – Notional Division of Security Inheritance and Risk

Reference: DISA – Cloud Computing Security Requirements Guide (SRG)

MICRO FOCUS

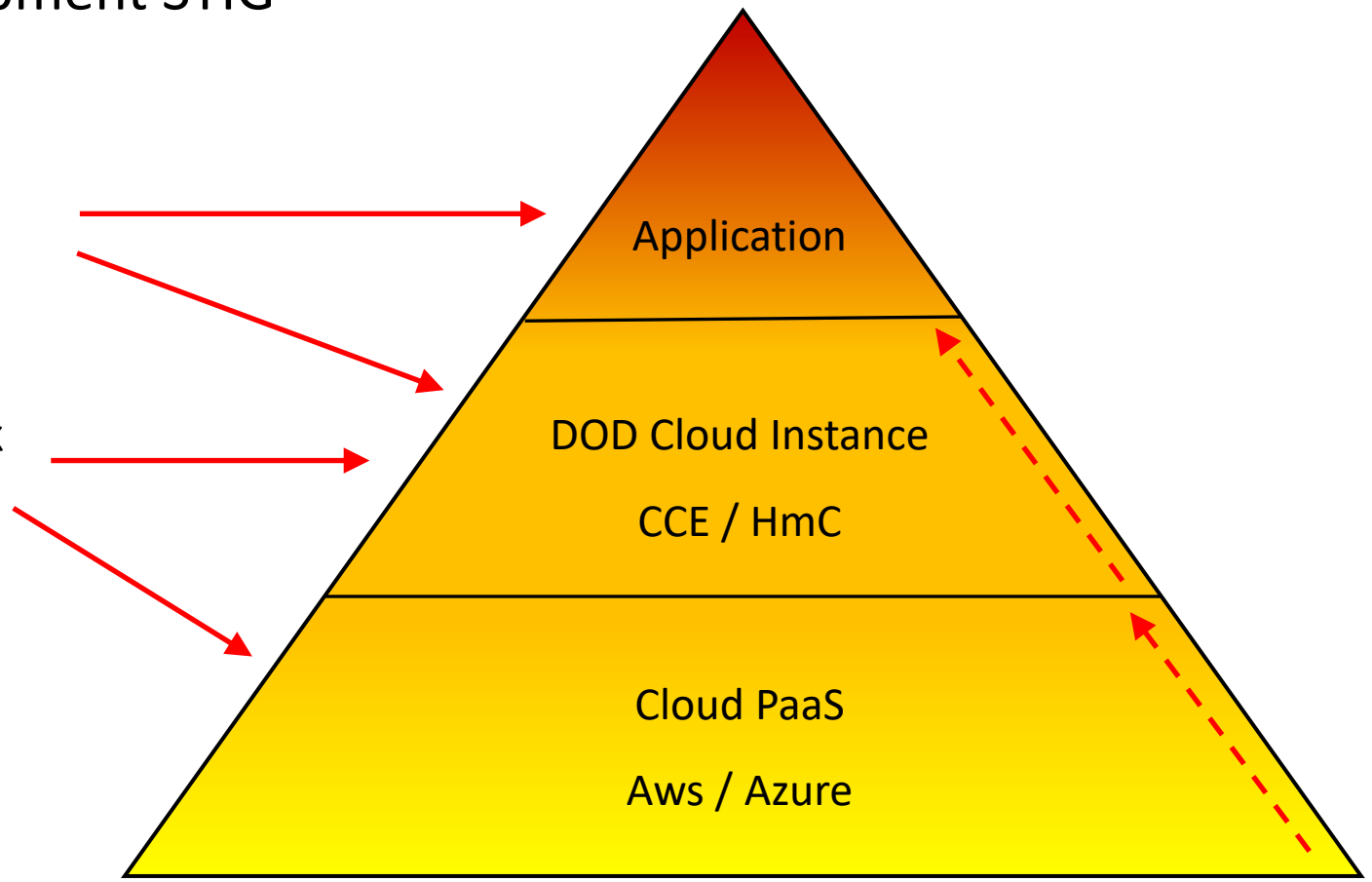
Cloud System Security Responsibility and Inheritance

Application Security and Development STIG

Executive Summary

The **ASD STIG** is published as a tool to improve the security of Department of Defense (DoD) information systems.

This document is meant for use in conjunction with the **Enclave, Network Infrastructure, Application Server, Database, Browser, and appropriate Operating System (OS) STIGs** and relevant technology Security Requirement Guides (SRGs).



What

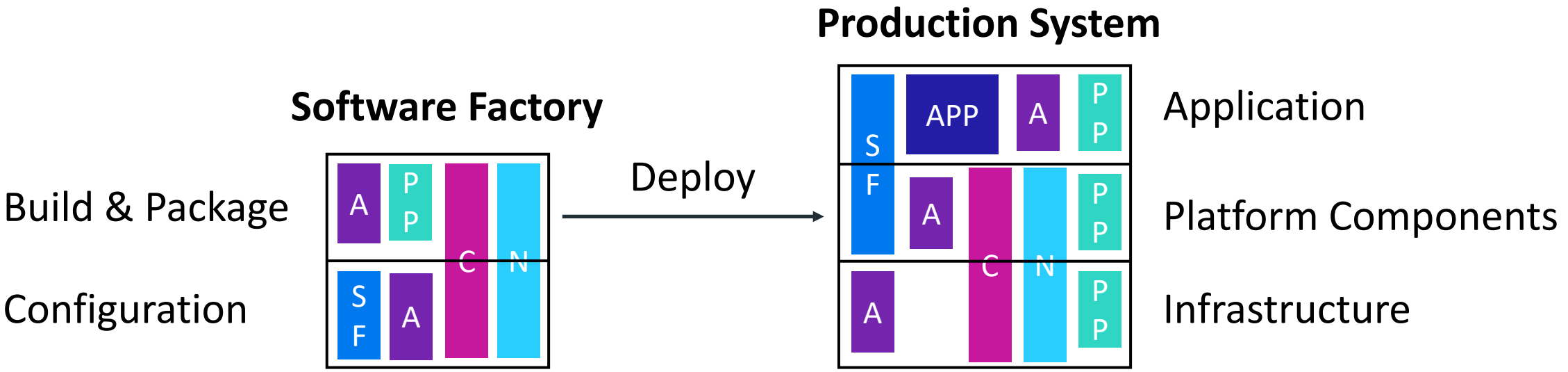
- Software Factory – provides repeatable process with known results. Can provide supply chain assurance
- Application Security Testing – ensures applications produced in the factory do not contain weaknesses and/or security vulnerabilities
- Cloud PaaS – provides hardened operating environment for applications to operate in

MICRO FOCUS

The Control Puzzle

Everything everywhere

- Controls: System Function (SF), Application (App), Audit (A), Component (C), Network (N), Process/Policy (PP)
- Domain: Application, Configuration, Build/Package, Infrastructure, Platform



MICRO FOCUS

Key Takeaways

- Cloud – another operating environment with certain benefits and constraints
- Build security In - it can not be bolted on or inherited from the environment
- Know what goes where – some controls can only be added at certain points, others cross boundaries and domains
- Validate – it’s a complex ecosystem you need to test at each stage to ensure you are meeting security requirements
- Combination of software factory, application security testing and Cloud provide the highest likelihood of repeatedly producing and hosting secure applications

MICRO FOCUS

MICRO FOCUS

Government Solutions