E X E T E R

Agile, SecDevOps, and Hybrid-Cloud

"Below the clouds, the practical elevation for rapid delivery of capability."

September 2019

Who we are

EXETER GOVERNMENT SERVICES

- Founded in 2002, VOSB
- Systems Engineering Institute (SEI) Capability Maturity Model Integrated Development (CMMI-DEV) Maturity L3
- ISO 9001:2015 (Quality) certification.
- Supporting both Army & USAF Personnel Systems as Prime Contractor
- CONUS / OCONUS
- Currently support 18 classified contracts up to the TS/SCI level.
- Same Leadership Team since inception

Headquarters Gaithersburg, MD

Overall Performance Rating Score of 96 out of 100 via Dun & Bradstreet, Inc. Open Ratings

Discussion Points

IT Continues to Change

How we move forward

Agile & DevOps

Cloud Computing in 2020

So, We're Going to the Cloud

About that Cloud, Security Thing…

IT Continues to Change

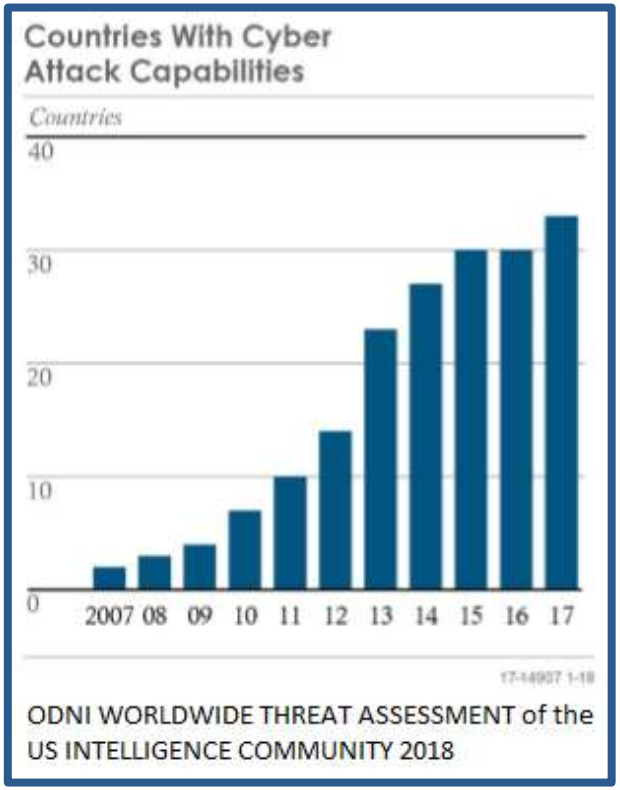
IT continues to change, aggressively!

Hardware, Software, Workforce

(Quantum, Blockchain, AI/ML, Decentralization, True Collaborative Dev)

Threats (Cyber Attacks)

- Standard vectors (viruses/trojans)
- Financial/Blackmail/Extortion
- Identity Theft (OPM, Equifax, CapitalOne)
- Infrastructure (Power/nuclear)
- Standard vectors (viruses/trojans)
- Financial/Blackmail/Extortion/Ransomware
- Autonomous Systems
- Social Media
- IT Degradation



How we move forward

Continuous Delivery of Capability

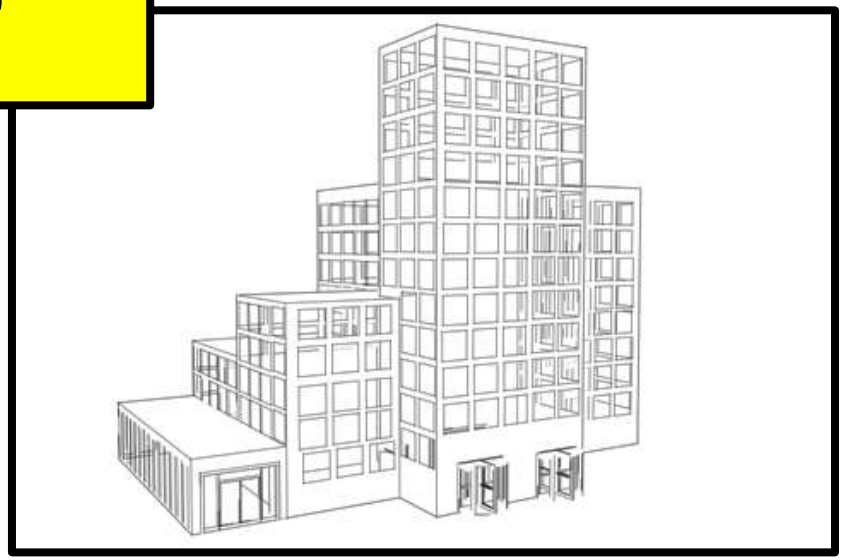
Our new priority must be,

“Get capability to the user faster!”

How we move forward

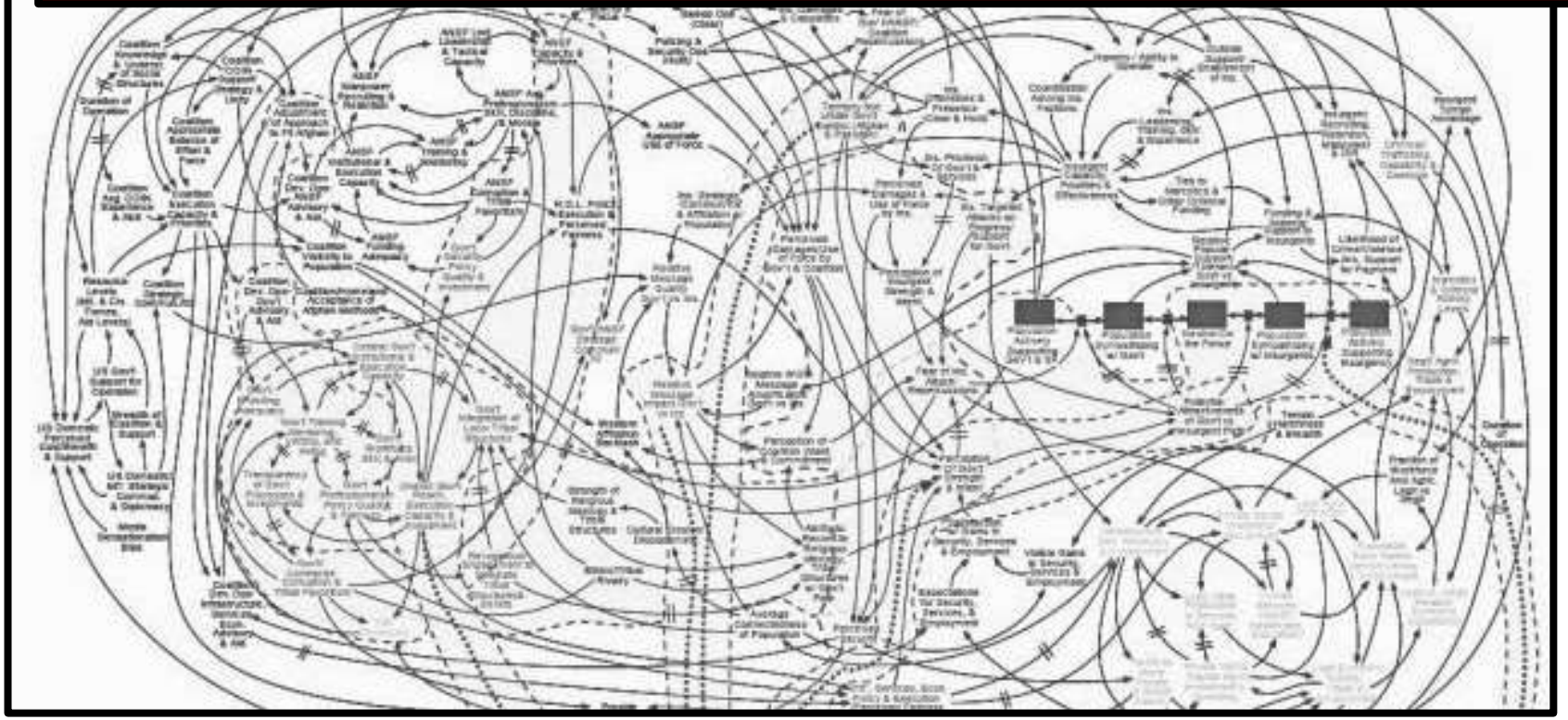
But Wait!

"Software engineering is totally different than standard engineering."



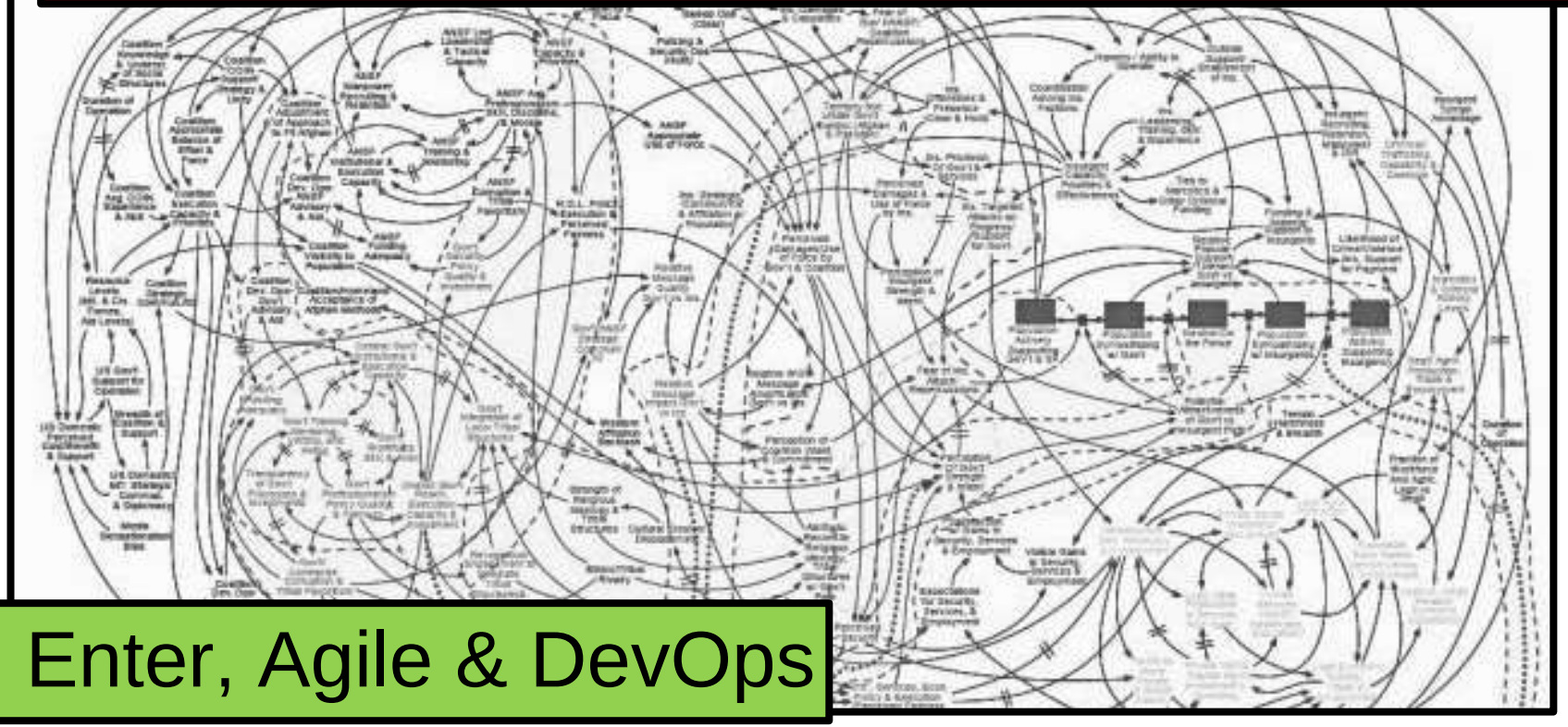
How we move forward

Here's the Reality of Software Engineering!



How we move forward

Here's the Reality of Software Engineering!



Enter, Agile & DevOps

Agile Development

Agile Development

Manifesto for Agile Software Development

We are uncovering better ways of developing
software by doing it and helping others do it.
Through this work we have come to value:

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

That is, while there is value in the items on
the right, we value the items on the left more.

https://agilemanifesto.org/

Agile Development

Agile Development

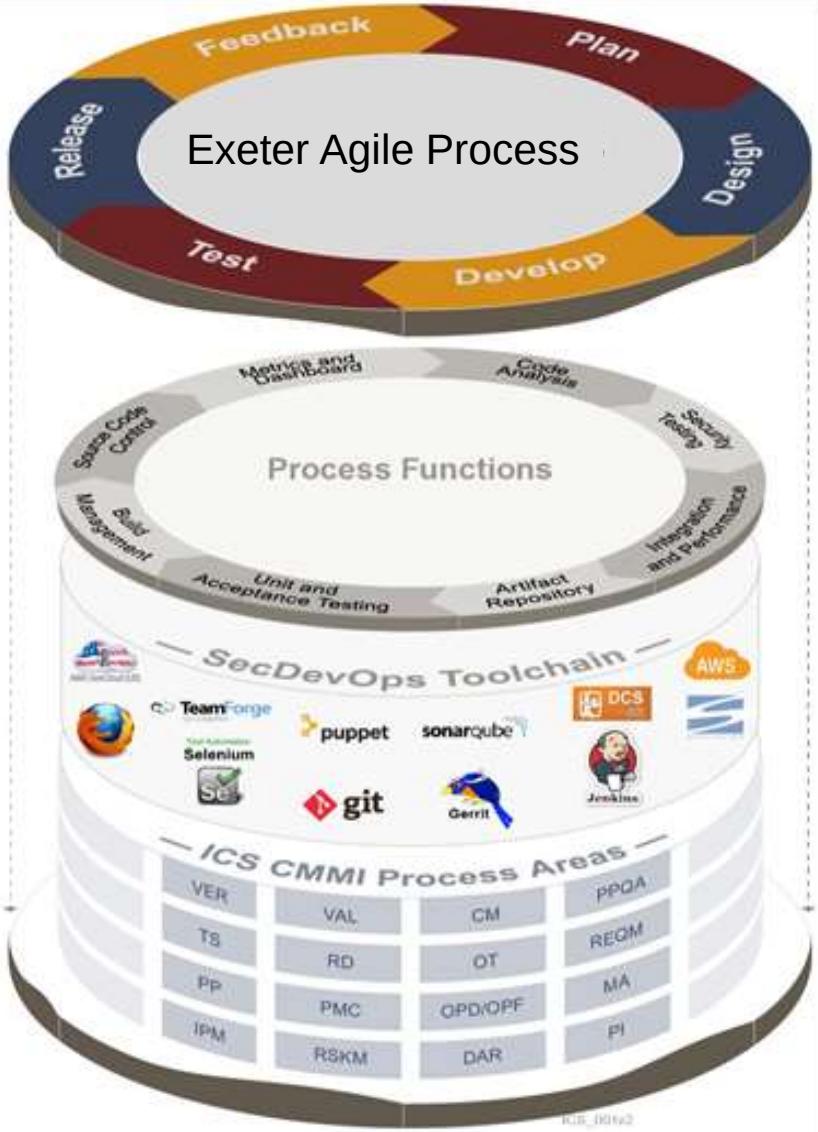
TDD
Product Owner
SCRUM
CI/CD
PAIR PROGRAMMING
DEVOPS
BACKLOG

Agile & DevOps

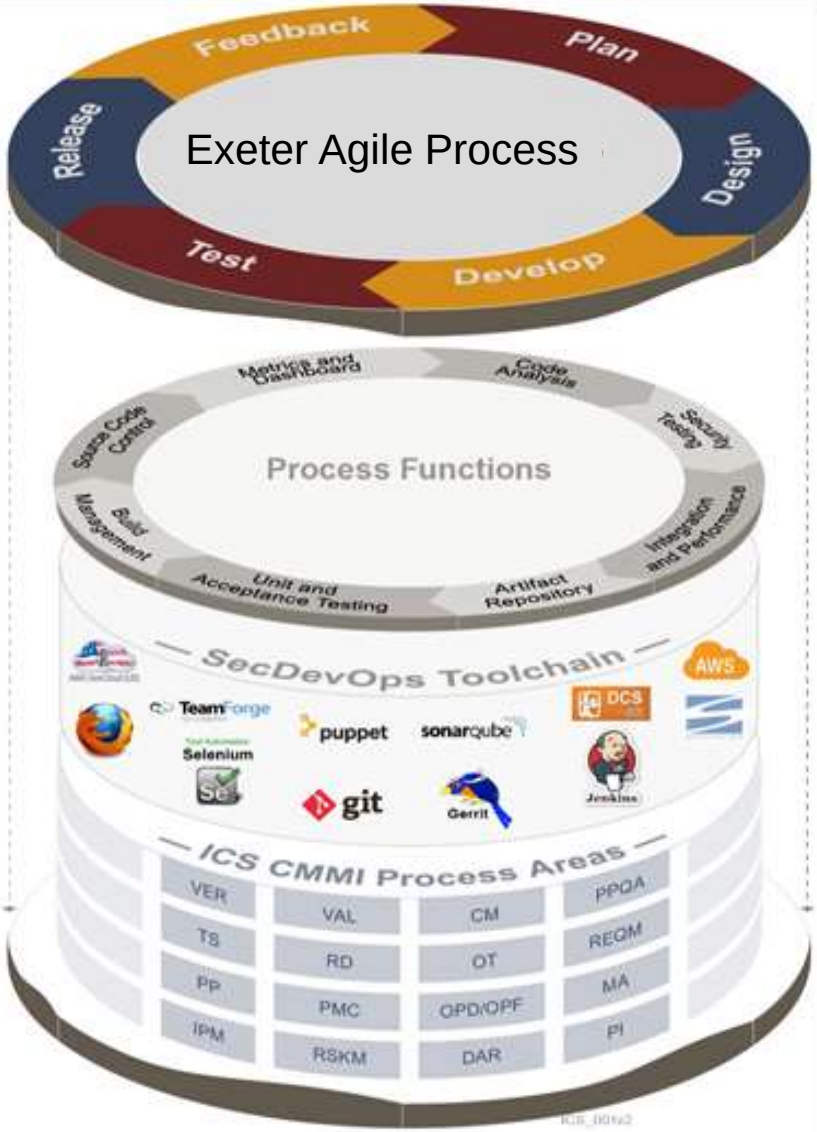
EXETER

How Exeter does Agile:

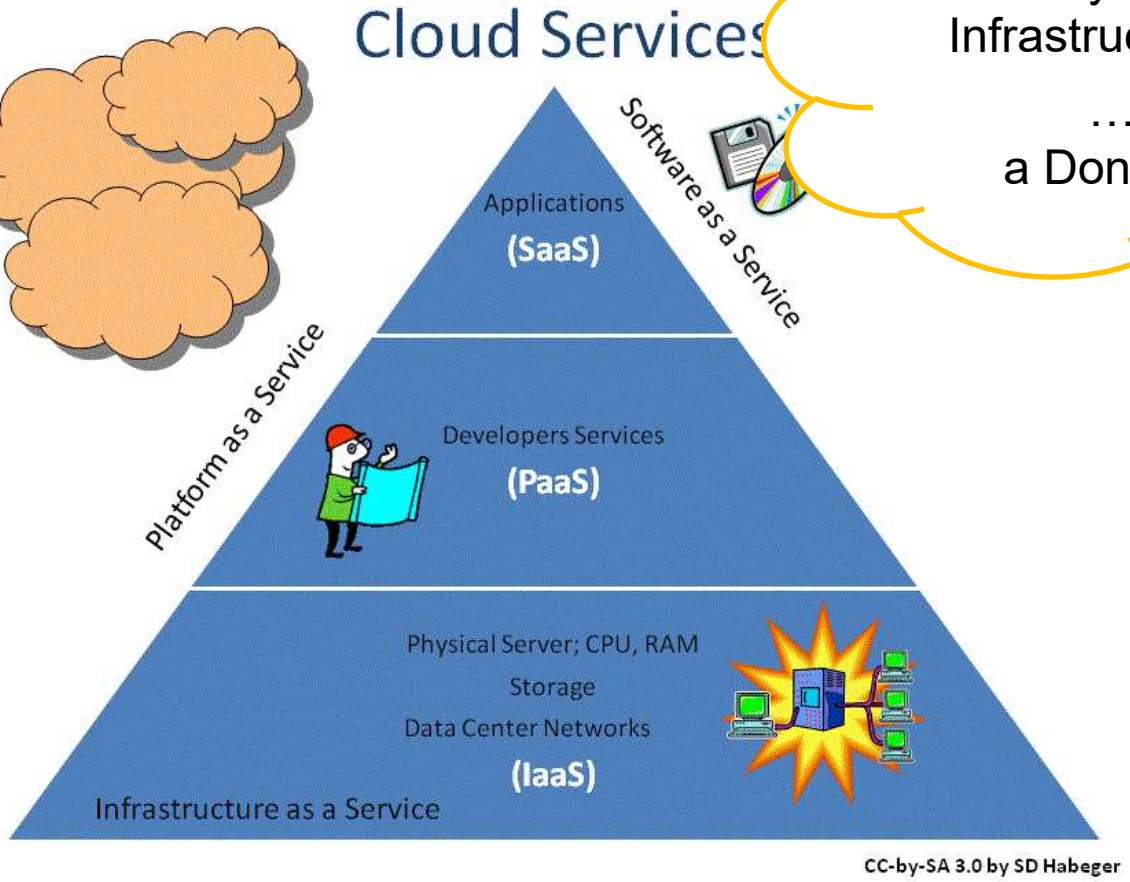
- 2-week Sprints (Iterations)
- Daily SCRUM Meetings
- Kickoff/Iteration Planning/UAT
- Govt = Product Owner
- Dev in AWS-East
- Preprod in AWS GovCloud
- Prod in Govt Cloud
- Rigorous CM processes
- RMF ATOs for all environments



Agile & DevOps



Cloud Computing in 2020

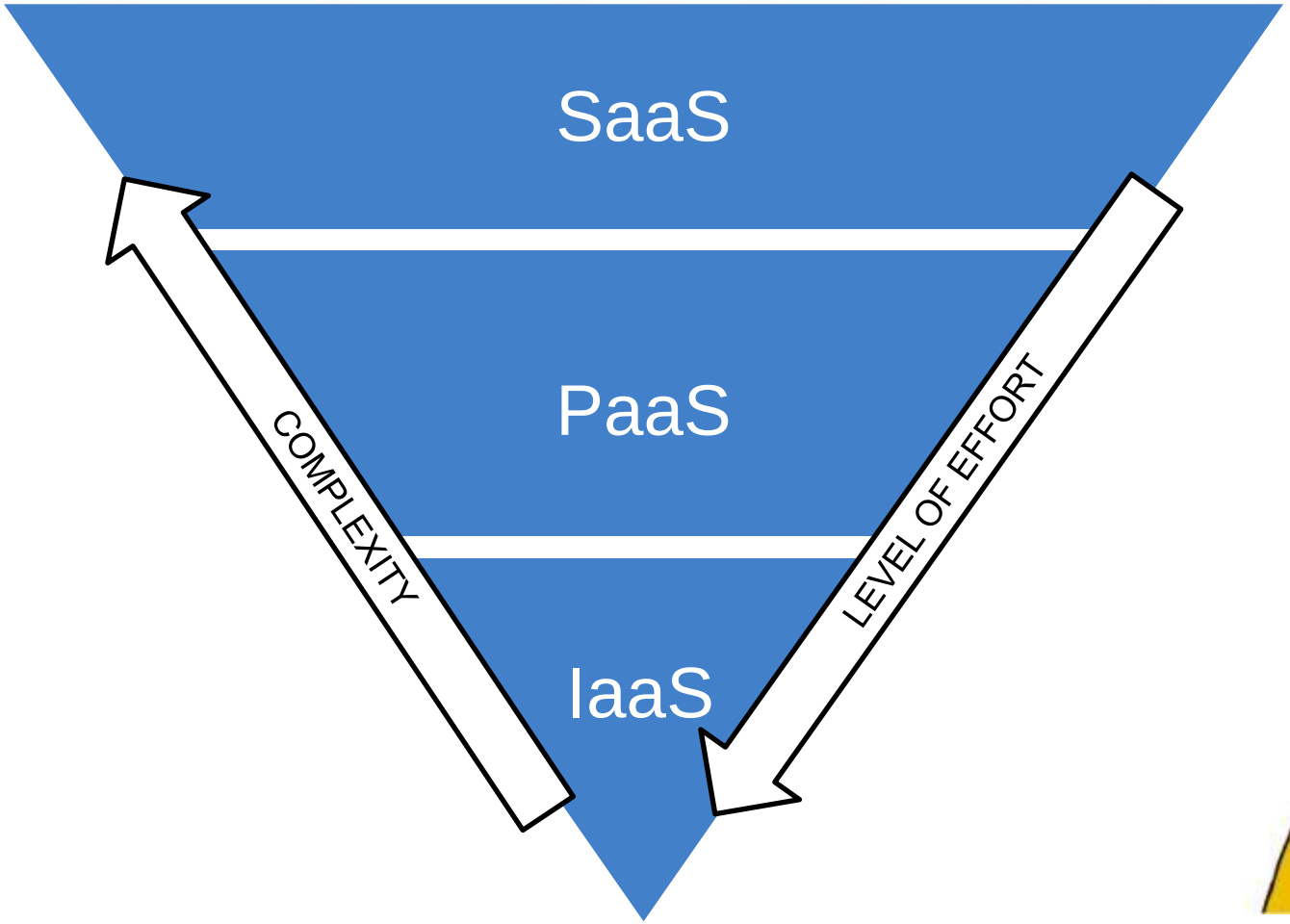


"Carbs, Dairy, Proteins...
…Pyramids …Duhrr,
Infrastructure, Platforms…

…just gimme
a Donut Hole, Dude!"

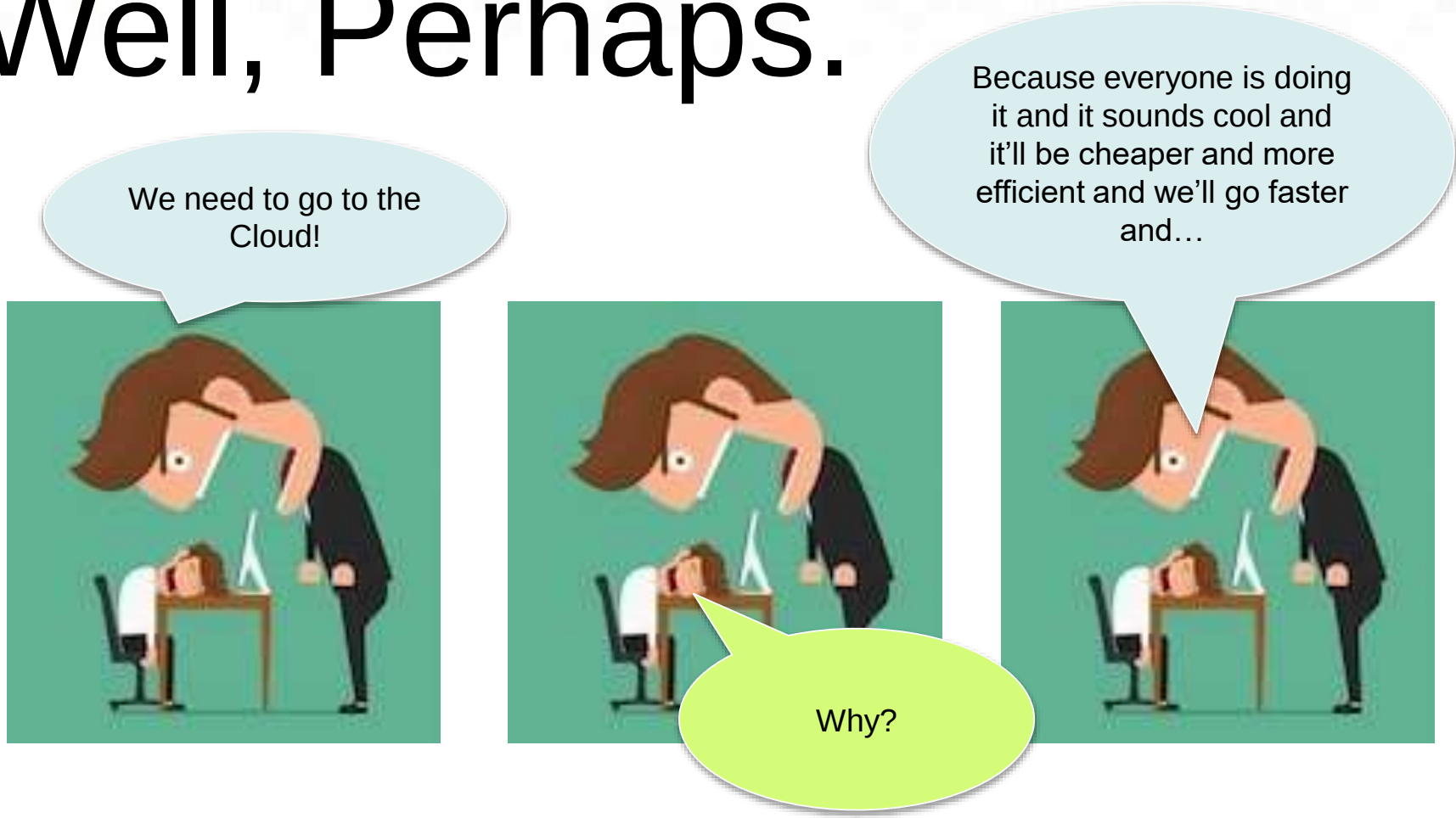
Cloud Computing in 2020

DevOps Inverts the Pyramid of Cloud Service Complexity



So, We're Going to the Cloud!

Well, Perhaps.



So, We're Going to the Cloud

"But doesn't the Cloud:"

"Cause you to rebuild everything?"

"Force people to change tools?"

"Costs too much?"

"Lock you into a Provider?"

"Confuse Everyone?"

"Have Security Issues?"

So, We're Going to the Cloud

So, We're Going to the Cloud

There's a Realistic Solution:

HYBRID-CLOUD

An Operating Environment Comprised of two or more clouds.
(I.e. On-Prem / Off-Prem combos, 2 or more CSP OEs).

So, We're Going to the Cloud

There are answers!

"Causes you to rebuild everything?"

A: Only if you need specific systems (VMs/routers/switches)

Services vs. systems and On-prem vs. cloud

"Force people to change tools?"

A: Only change what needs changing (cost/quality/speed)

"Costs too much?"

A: Multiple vendors push down costs

Cost benefit of on-prem vs cloud

Services vs. systems (on demand, non 24/7)

Read the fine print!

So, We're Going to the Cloud

There are answers!

"Locks you into a Provider?"

A: Discipline to develop agnostic tech is required!

"Confuses Everyone?"

A: Training is readily available! (From vendors themselves and 3rd party Integration firms (like Exeter).

"Has Security Issues?"

A: It's now built-in:

CSPs Must be Pre-Certified FedRAMP/FISMA/RMF ATOs

Hybrid cloud spreads threat-obstructions across the Cloud Application System Surface

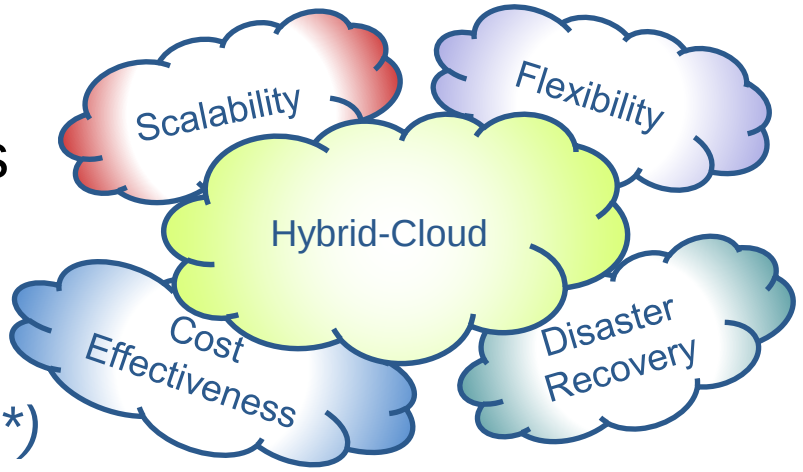
(On-Premises & Off-Premises Commercial and Government CSP)

So, We're Going to the Cloud

EXETER

The cloud isn't just another Datacenter full of Servers, Disks, CPU, and RAM anymore!

In practice today supporting our DoD customers, Exeter Technicians leverage the following Cloud capabilities:



- Store/build/deploy code *(AWS code*)*
- Instantly provision coding labs *(AWS Cloud9)*
- Write Re-usable customer solution functions & calculations *(AWS lambda, IBM cloud functions)*
- Recovery Solutions & Back-up Data *(AWS S3, Glacier)*
- Build APIs *(AWS API Gateway, IBM cloud functions)*

About that Cloud Security thing…

EXETER

So, is it DevSecOps, SecDevOps, or DevOpsSec?

(Is there really a difference in these Security-related DevOps terms?)

- **DevSecOps** - Developers don't have the simple tools, or skills to secure applications from the beginning, and InfoSec teams are potentially brought in too late to address security concerns.
  - As a result, DevSecOps represents the scenario we are in today – a situation where security doesn't get the prioritization it deserves.
- **DevOpsSec** - This version literally places security at the end of the line, after discrete development, deployment, and operations activities.
  - It's easy to release applications with the rationale, "We'll patch as we catch bugs." Yet from security's perspective, patching simply can't keep up. *For example, the 2017 Equifax breach was caused by a missed patch on an open-source application.*

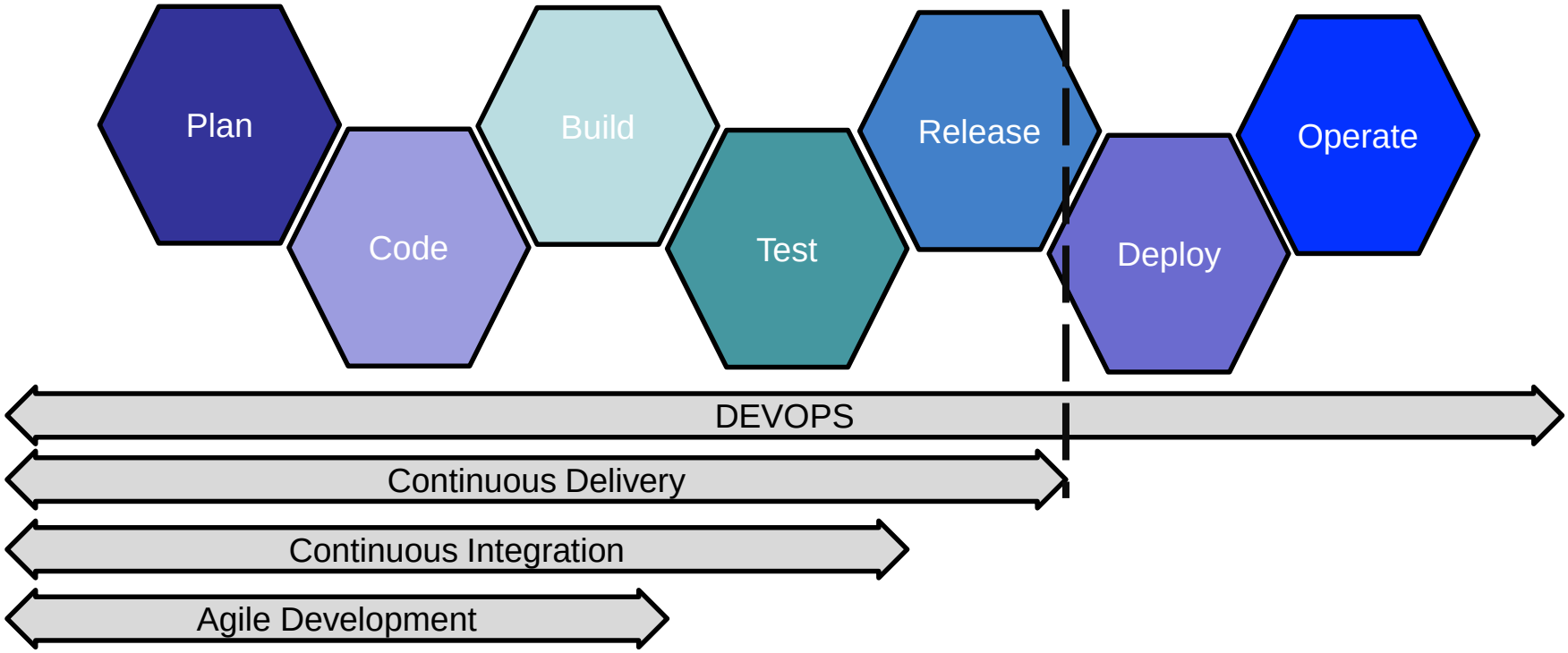
About that Cloud Security thing…

The most successful Migrations & Cloud Operators practice:

- **SecDevOps –** Integrates security efforts and best practices into the DevOps continuous integration and continuous deployment pipeline.
  - Security requirements are **taken into account before** development to ensure security is included throughout the product lifecycle.
  - This approach addresses previous shortcomings by automating and integrating security solutions as part of the core development process.

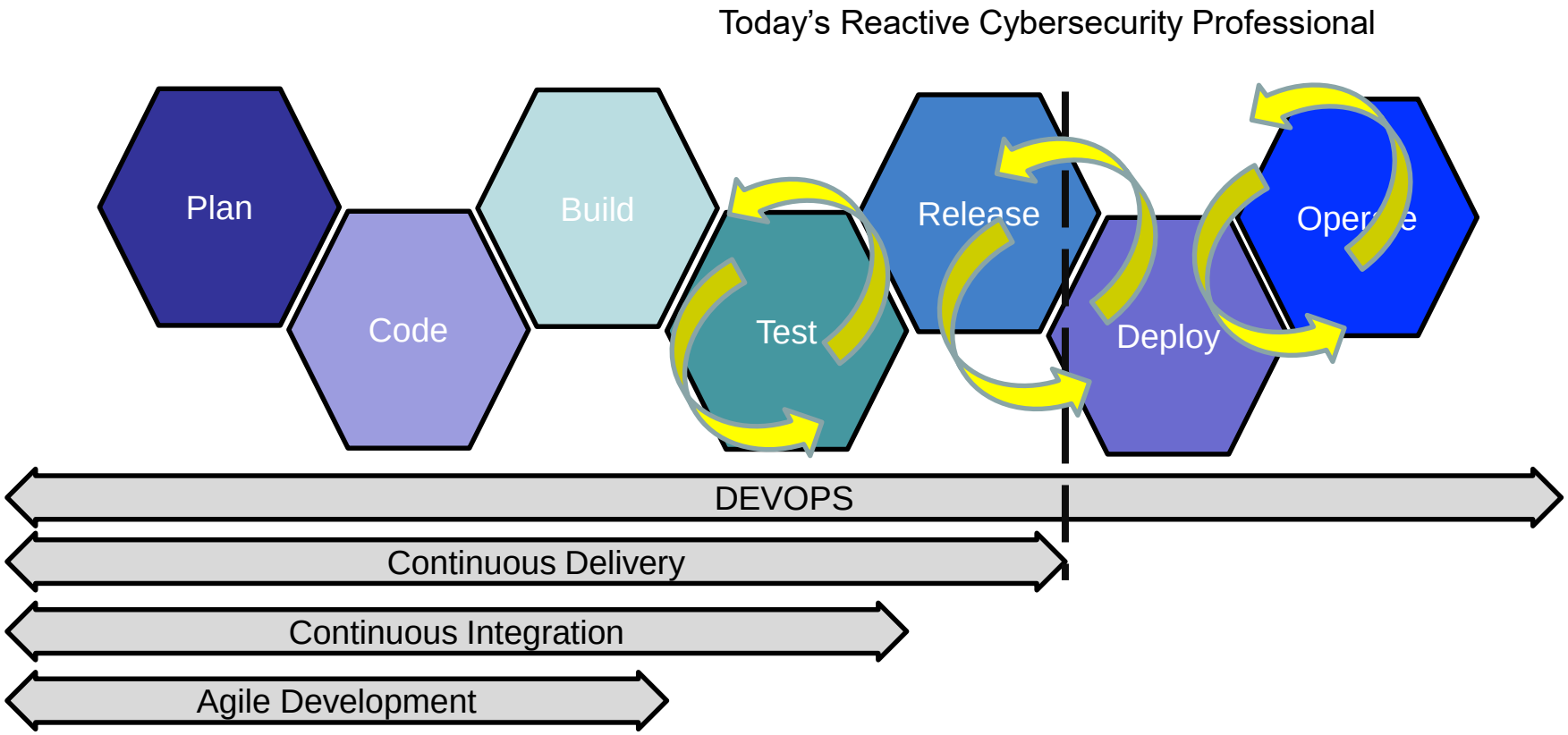
About that Cloud Security thing…

So, where do IA / Cybersecurity Professionals execute today's job in Tomorrow's Cloud?



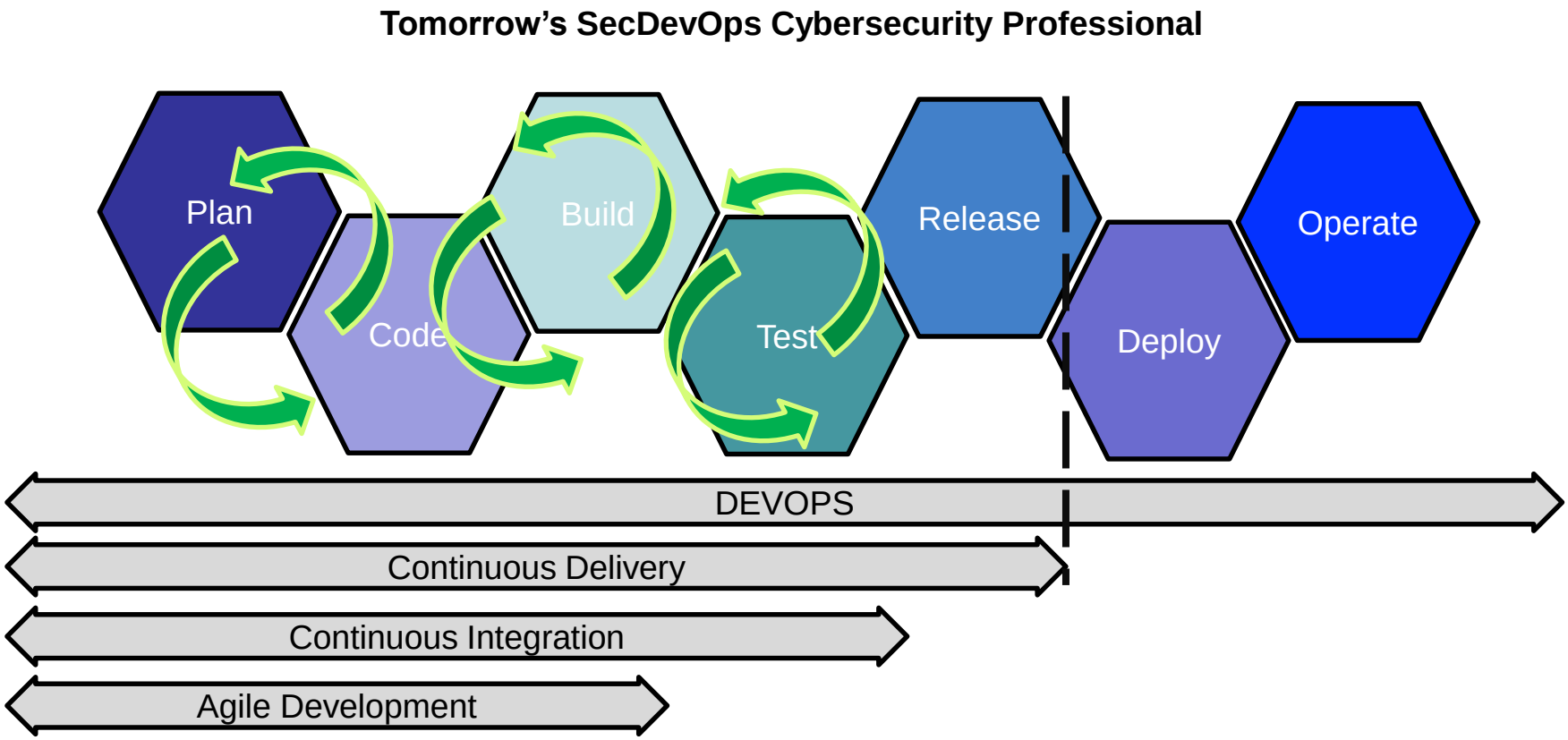
About that Cloud Security thing…

So, where do IA / Cybersecurity Professionals execute today's job in Tomorrow's Cloud?

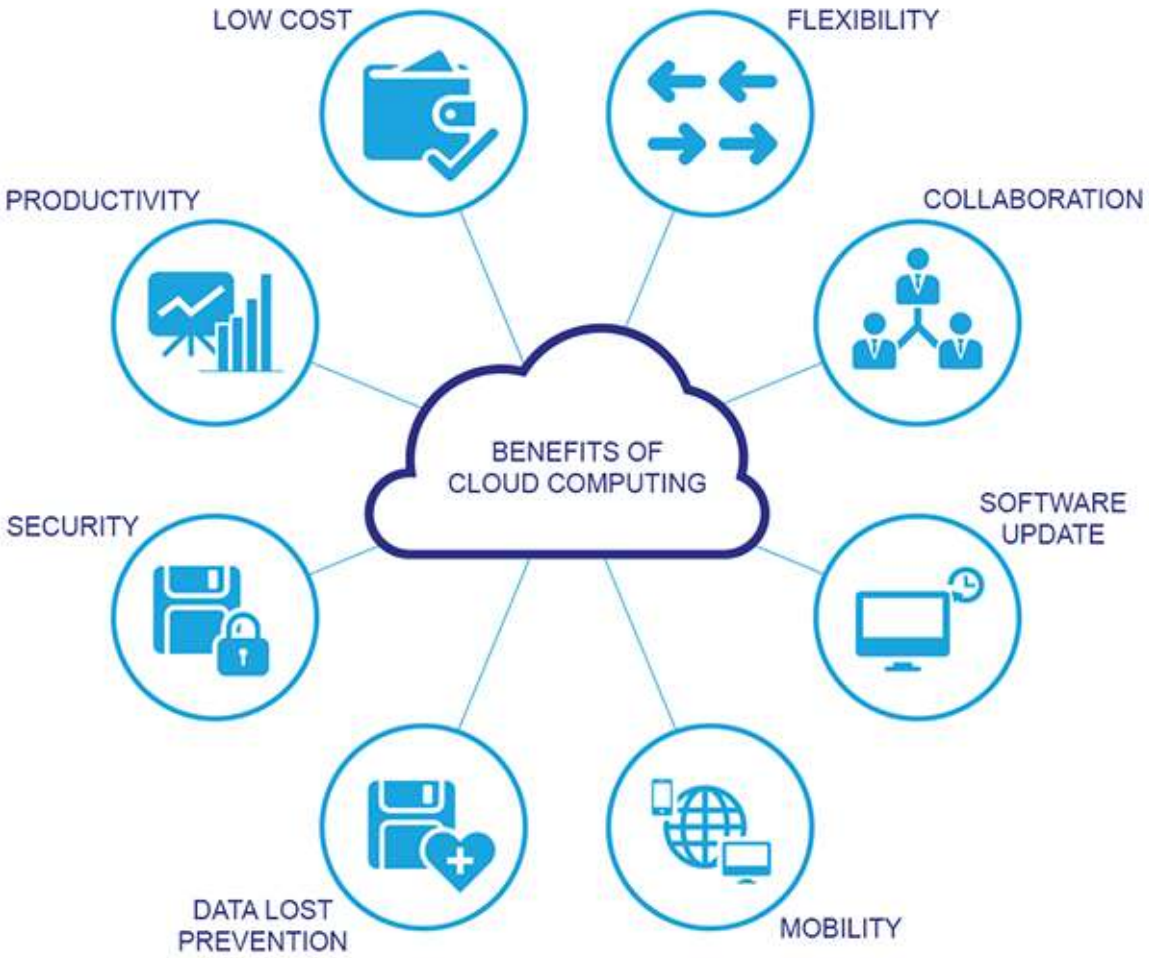


About that Cloud Security thing…

So, where do IA / Cybersecurity Professionals execute today's job in Tomorrow's Cloud?



Summary


LOW COST
FLEXIBILITY
PRODUCTIVITY
COLLABORATION
BENEFITS OF
CLOUD COMPUTING
SECURITY
SOFTWARE
UPDATE
DATA LOST
PREVENTION
MOBILITY

Summary

Cloud Migration Solutions Do not happen overnight.

In fact,
it's doubtful in 30 Days;

I probably wouldn't
buy-in thinking 60-90 Days;

And I'd probably stop
thinking in terms of "Days".

Summary

Cloud Migration Solutions
Do not happen overnight.

Initiate the effort with the intention of getting it right, or it will never act as an Asset.

Summary

Threats & Risks

The Struggle is real, Ya'll!

Summary

SecDevOps

The only way to gain velocity is to promote our Security Professional's to the front of the line!

...or lifecycle processes; you know what I mean, San Diego!

Thank You for Listening

Thank You for Listening

Questions Welcomed !

Some Real-World Success

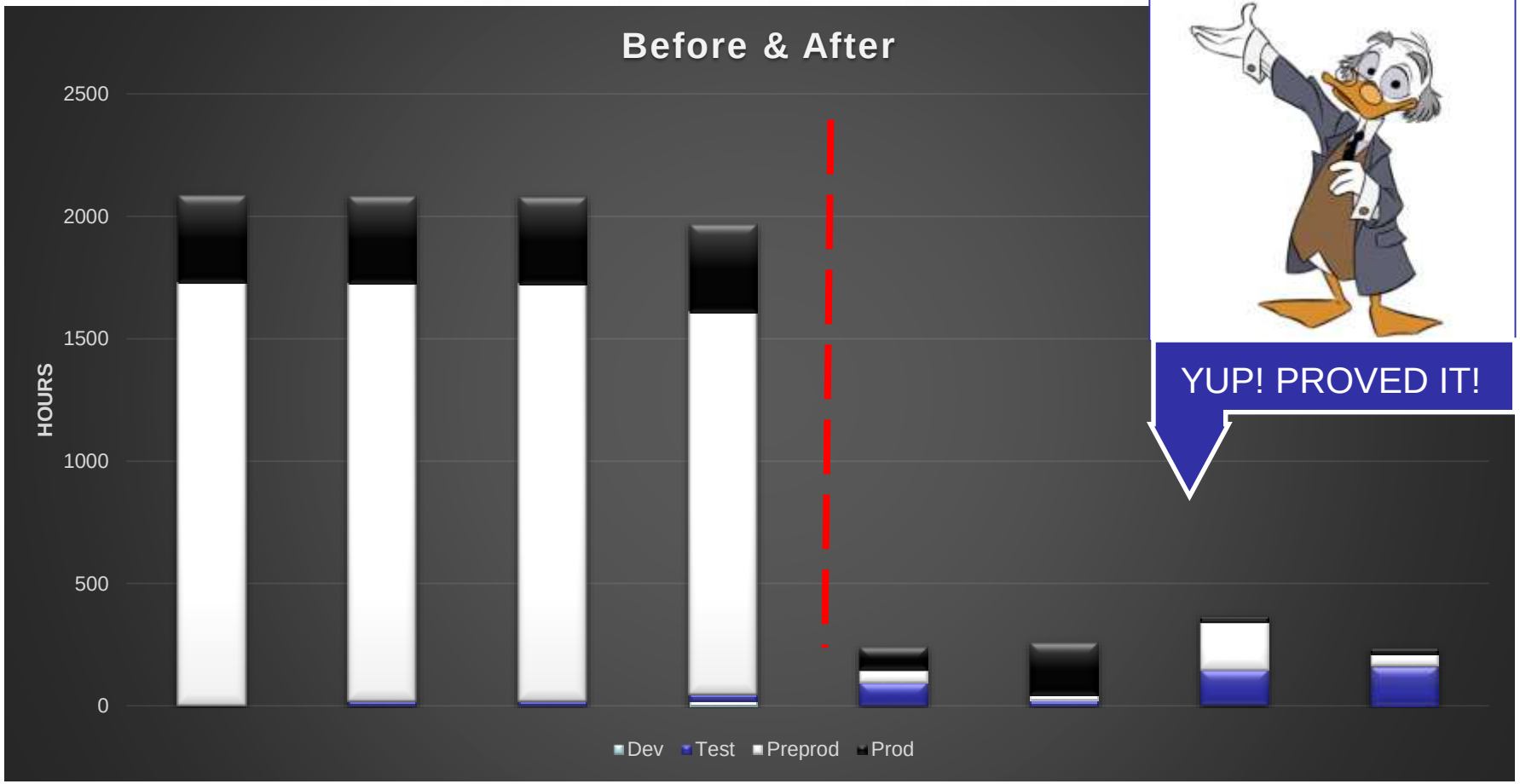
Proof is in the pudding!

In 2019, using Agile & Continuous Exeter has completed refactoring of 2x high-complexity Government applications to commercial + Govt hybrid cloud. During the efforts, we gained expertise:

- Automating RMF within Hybrid-Cloud.
- Transitioning several Apps from Waterfall to practicing Agile/Continuous Delivery
- Deploying the first production app deployed in DISA MilCloud 2.0
- The first migrated app to be RMF Accredited in AWS GovCloud & DISA MilCloud.

Some Real-World Success

So, how did Hybrid-Cloud help?

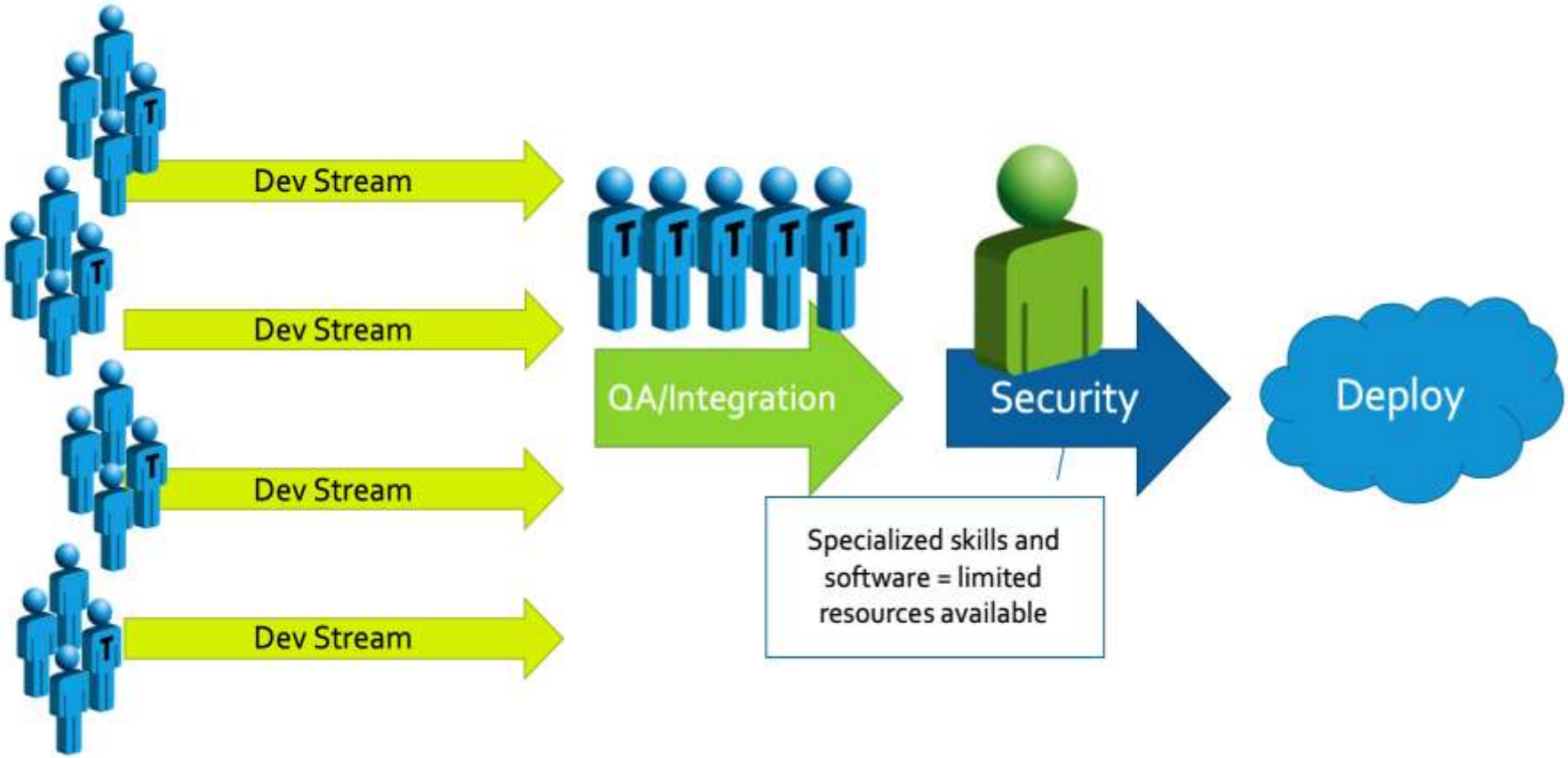


The SecDevOps Methodology

- Traditional waterfall models task Security at the end of the SDLC to review and react.
- SecDevOps tasks IA/Cyber Engineers at the beginning, in the planning stages.
- At Exeter, Security Engineers participate when DevOps teams plan their Stories and Features during Quarterly Iteration Planning meetings building threat models at the feature or service level.
- Because SecDevOps engineers now have insight into both the code, system architecture, and the operating environments Apps run in, they can better:
  - ✓ Proactively Address Vulnerabilities
  - ✓ Identify how a malicious actor might try to attack
  - ✓ Automate IA Validation tests and finding remediation methods.
  - ✓ Fold-in Security maintenance (NOTAM, IAVA, TCNOs, etc.)

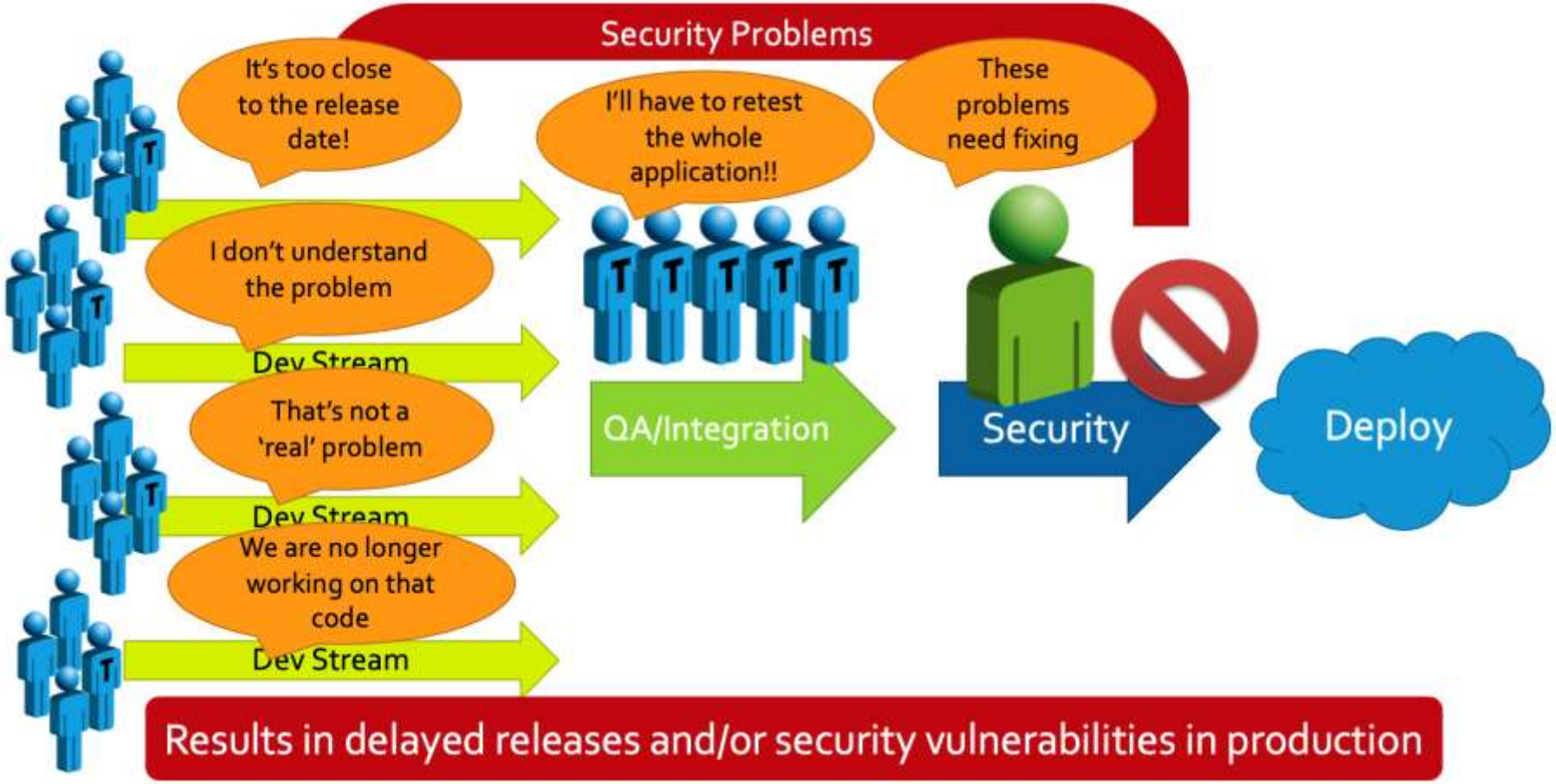
About that Cloud Security thing…

The SecDevOps Methodology



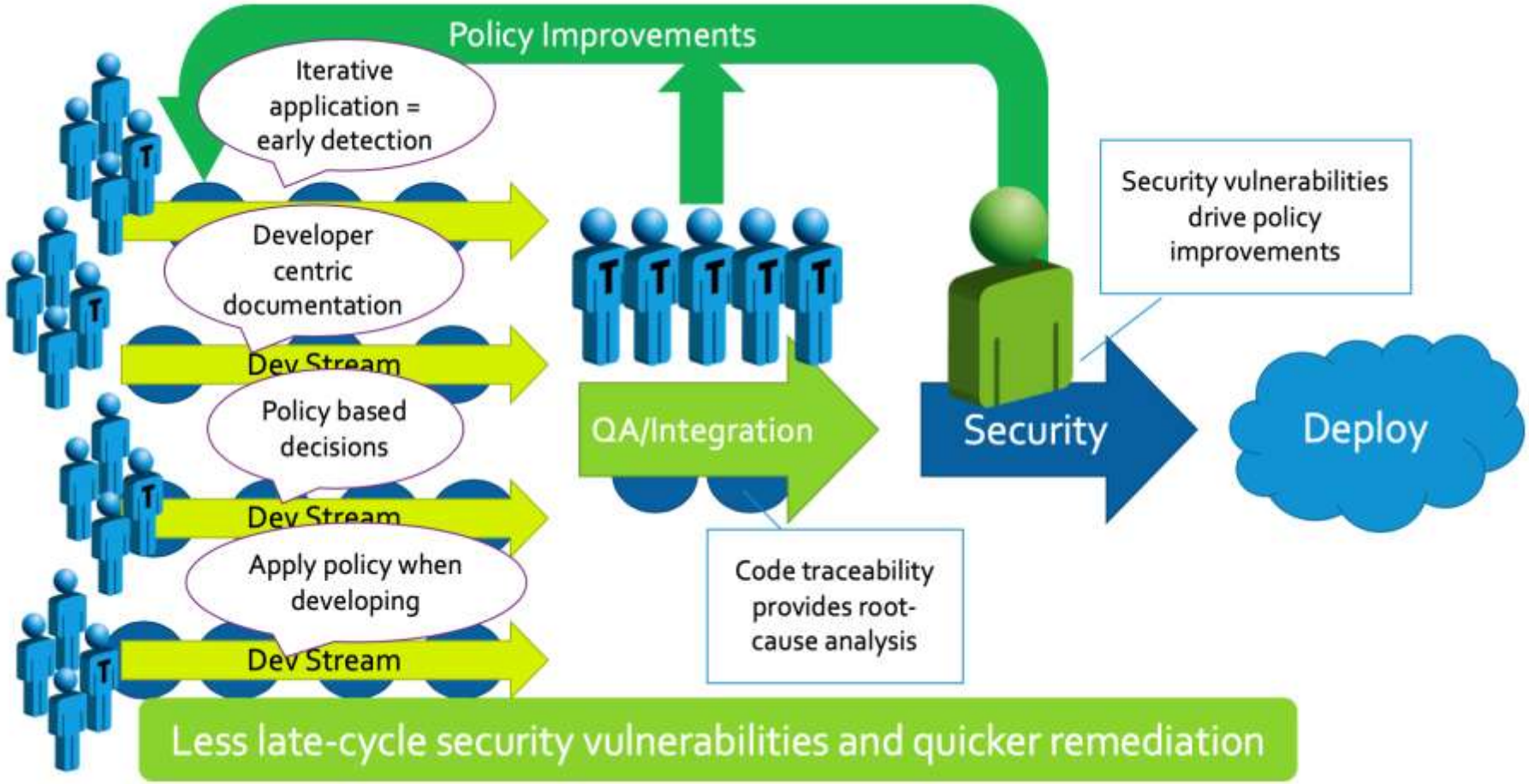
About that Cloud Security thing…

The SecDevOps Methodology



About that Cloud Security thing…

The SecDevOps Methodology



About that Cloud Security thing…

SecDevOps, Day-to-Day Basics

- Your developers have learned how the entire technology stack works.
- Operations Engineers now understand how the software runs in the stack.
- To be fast, Security Experts need to be involved at all levels of the stack.
- SecDevOps Engineers must be capable of assimilating each aspects of the system

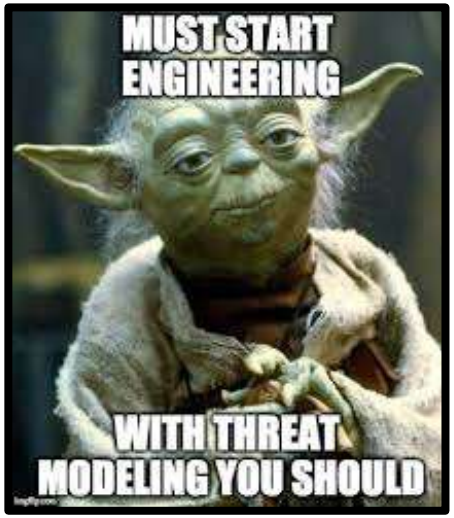
About that Cloud Security thing…

SecDevOps, Day-to-Day Basics

- Normal Security Maintenance is folded into Backlog, or normal O&M after hours (i.e. IAVA, NOTAM, TCNO, etc.)

- RMF re-aligned and integrates Threat Models and Correlations in Design, Dev, Build, & Test Phases.

- Test-Driven Development (TDD) intersects End-User capability demand with Cybersecurity in each Feature and Story.



About that Cloud Security thing…

Monitoring & Tooling Advice for SecDevOps

Security visibility is necessary to a successful SecDevOps team.

- Monitor every logfile in the ecosystems housing your Continuous Delivery Tool Chain(s).
- Constantly scan the customer-facing interfaces, ecosystem logfiles, especially those monitored within your Cloud Orchestration middleware.
- Orchestration toolchains cross-check for vulnerabilities with TCNO, IAVA, and other defined risks dynamically or on-demand within your ecosystem.
  - (This includes, out-of-date package, expired PKI Certificates, or simple default passwords).
- Build custom integrations to perform inventory management across your Cloud or Hybrid-Cloud OEs.
- Security Professionals can also be instrumented with dynamic system Cloud Orchestration Suite Toolsets to find intrusion threats and known vulnerabilities

About that Cloud Security thing…

Some Pro's & Con's of SecDevOps

CON: In many organizations, there aren't as many security engineers as there are development teams.

PRO: We can train and empower Developers to become Security Experts while insulating them with automated security monitoring tools.

About that Cloud Security thing…

Some Pro's & Con's of SecDevOps

CON: In many organizations, there aren't as many security engineers as there are development teams.

PRO: We can train and empower Developers to become Security Experts while insulating them with automated security monitoring tools.

CON: Going fast is key, but teams may sometimes forget to apply process to their feature requirements and run out of bandwidth to address security.

PRO: It's up to a SecDevOps team to figure out ways to inject themselves into that process and start conversations and educate teams about the risks they could be introducing into their systems.

About that Cloud Security thing…

Some Pro's & Con's of SecDevOps

CON: In many organizations, there aren't as many security engineers as there are development teams.

PRO: We can train and empower Developers to become Security Experts while insulating them with automated security monitoring tools.

CON: Going fast is key, but teams may sometimes forget to apply process to their feature requirements and run out of bandwidth to address security.

PRO: It's up to a SecDevOps team to figure out ways to inject themselves into that process and start conversations and educate teams about the risks they could be introducing into their systems.

…and a couple more significant PROs!

PRO: The rise of SecDevOps has sparked passion and innovation as security teams constantly discover new ways to work and invest in teams and products.

About that Cloud Security thing…

Some Pro's & Con's of SecDevOps

CON: In many organizations, there aren't as many security engineers as there are development teams.

PRO: We can train and empower Developers to become Security Experts while insulating them with automated security monitoring tools.

CON: Going fast is key, but teams may sometimes forget to apply process to their feature requirements and run out of bandwidth to address security.

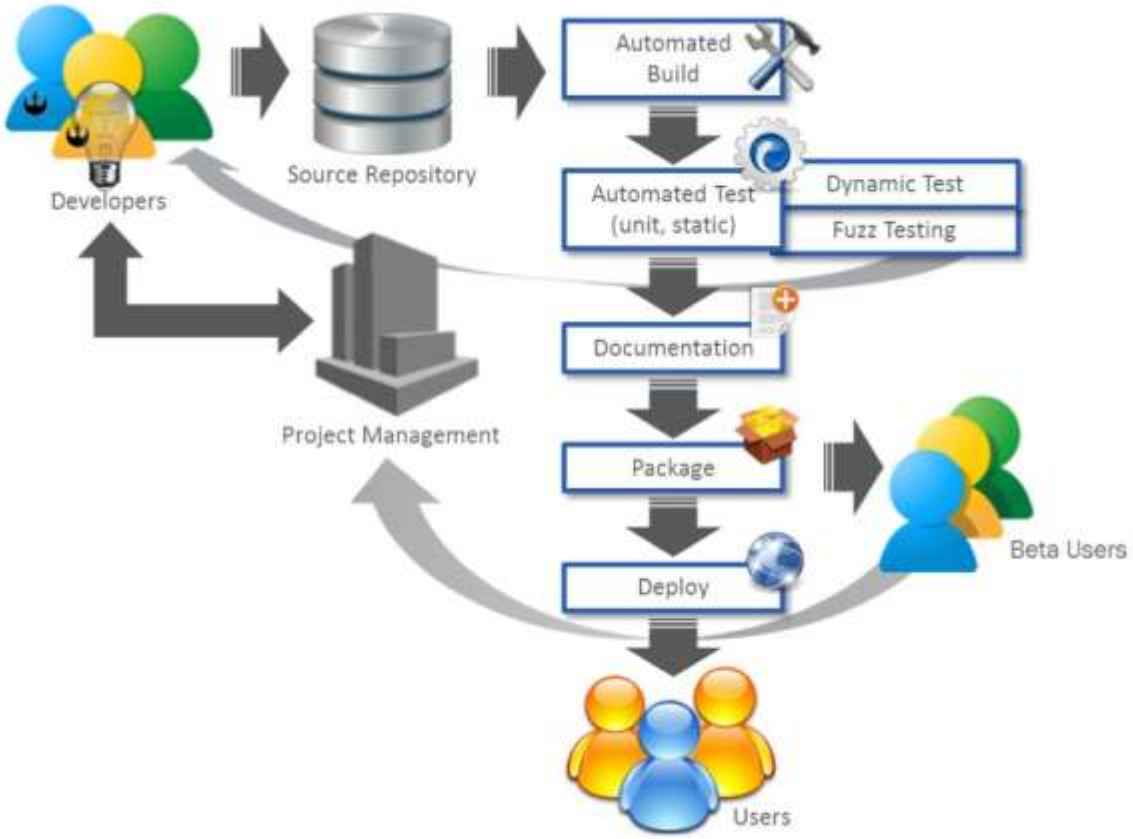
PRO: It's up to a SecDevOps team to figure out ways to inject themselves into that process and start conversations and educate teams about the risks they could be introducing into their systems.

…and a couple more significant PROs!

PRO: The rise of SecDevOps has sparked passion and innovation as security teams constantly discover new ways to work and invest in teams and products.

PRO: These security teams are open sourcing many of the tools they have created so other developers can try out these ideas in their own environments.

Remember Software Factories?



Remember Software Factories?

Software Factory End Goals Include:

- Achieving **Innovation** via:
  - Common toolsets
  - Autonomously Advancing Tech
  - Real-time Response to need
  - Automation!
  - Going faster!

= Continuous and **Rapid Capability** is delivered to End-Users.