How to stay agile when applying security assurance to SDN/NFV projects

September 2016

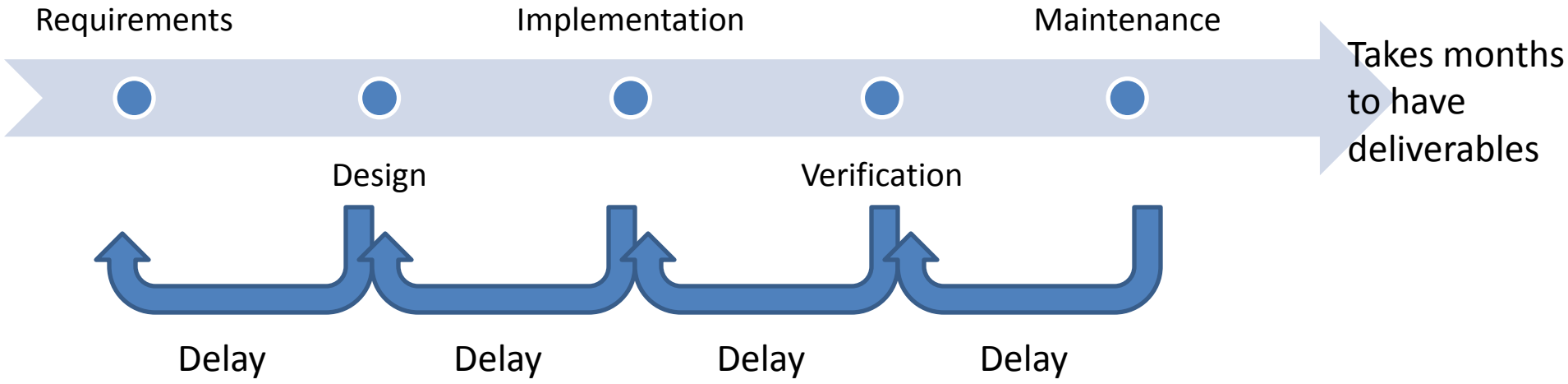
Bell

Agenda

- Waterfall methodology
- Agile methodology
- The mandate
- What was achieved fast
- Pro’s and con’s of Agile
- Tips

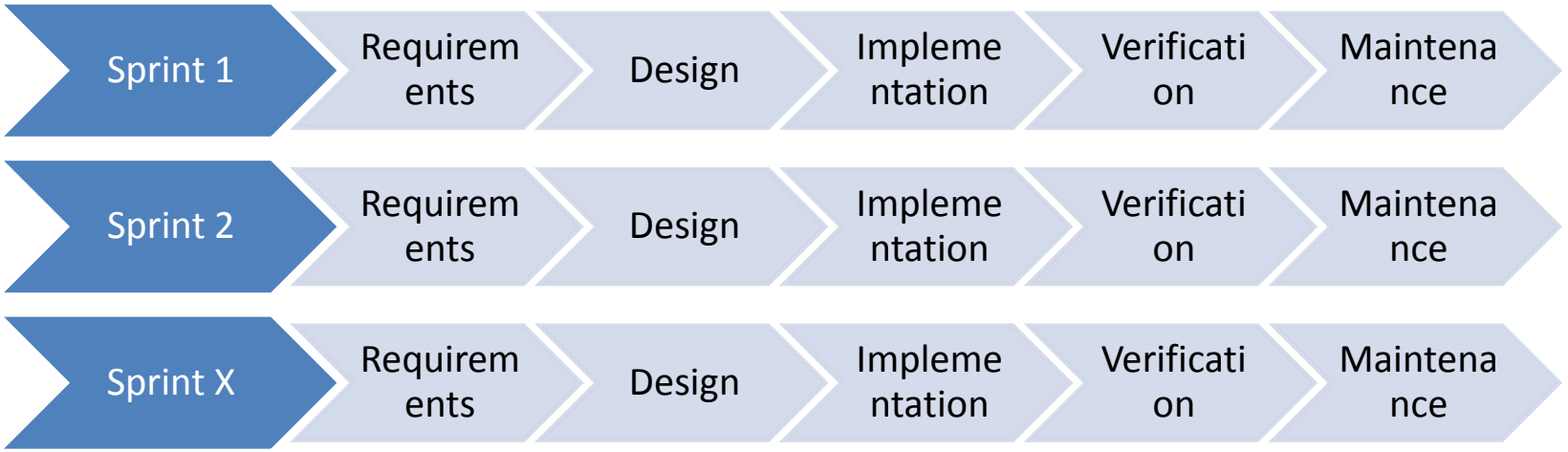
Waterfall methodology

In the waterfall methodology the security needs are documented in the requirements. It normally refer you to the existing policies/directives. The implementation team need to interpret these documents and find ways to be compliant.



Agile methodology

In the Agile methodology the security expert is part of the team of each sprint, he can explain the expected outcome of the policy/directive and be part of the solution



It all starts by a mandate

Mandate:

Identify the security requirements and implement the security controls of the SDN infrastructure.

Deliverables:

Infrastructure secured

Process for securing new sites produced

Visual Management that will help to see the work progress & problems

Achievements

In 8 weeks (4 sprints):

- Alignment on the 5 major 'Corporate Security standards' – review, understanding and expectations
- Solutions to detect malware
- Process for security patching
- Patch process validated in lab
- Password management process build
- DNS, NTP, and VA scan process and implementation
- FW design completed with agreed next steps
- OS hardening requirements identified and reviewed, mitigation plan in place
- Design tenant vs security zones

If you use Agile

Pro's:

Deliver small steps faster – infrastructure can be used sooner

Good way to develop people

Solution agreed by everyone – no rework

Con's:

Resource dedicated, hard to support many project at the same time

Not all security controls in place when the infrastructure can be used

Tip:

How do you prioritize and select which security controls to include in each sprint?

Answer: a common set of security services needs to be available so that each sprint can consume the security services without be burdened with the delivery. E.g. Logging, authentication, encryption, VA scanning…

Tips for doing Security Assessment in Agile

Do not be afraid to ask questions

There are no bad questions

Failure is okay

Benefits are always gained and can be built upon, even in ‘failure’

A security failure could lead to information exposure that would hurt the business and loyalty/trust of customers. Some failures are not acceptable, the risk need to be identified before starting an experiment

Find ways to make it work

Don’t look at how the solution will not work but more how it will work