Security insights

Markus.tauber@researchstudios.at

www.markus.tauber.co.at

www.researchstudio.at

Sept. 2024

Why?


Friday July 12, 2019
Unforseen Risks
HOW CAN YOU BE SURE THERE ARE NO UNFORESEEN RISKS WITH THIS PLAN?
IT IS NOT POSSIBLE TO KNOW IF ONE HAS CONSIDERED EVERY RISK. THEREFORE, WE CAN NEVER BE SURE.
SO. . . I CAN STILL BLAME YOU FOR ANY PROBLEMS THAT POP UP?
YES, THAT PART OF THE PROCESS IS STILL INTACT.
DILBERT.COM @SCOTTADAMSSAYS
7-12-19 2019 Scott Adams, Inc./Dist. by Andrews McMeel

© Dilbert

Outline I

- Introduction
- Secure Onboarding in Arrowhead
- Security Standards & Guidelines
- Integration of continuous standard compliance verification in Arrowhead

Introduction

& where I work

- Research Studios Austria, Not-for-Profit Research Organisation, since 2002
- 7 Research Studios in Salzburg, Linz, Vienna, and St Pölten (Austria)
- RSA Studios focus-topics include Geo-Informatics, IoT- & Cloud-Infrastructures, Digital Knowledge Transfer, Augmented & Virtual Reality up to Big Data Analytics, AI,..
- Possibility of Internships, etc.
- For papers, past projects – check www.markus.tauber.co.at

Digital Production & the Green Deal

Research Topics in emerging Trends

Integration into structured academic training

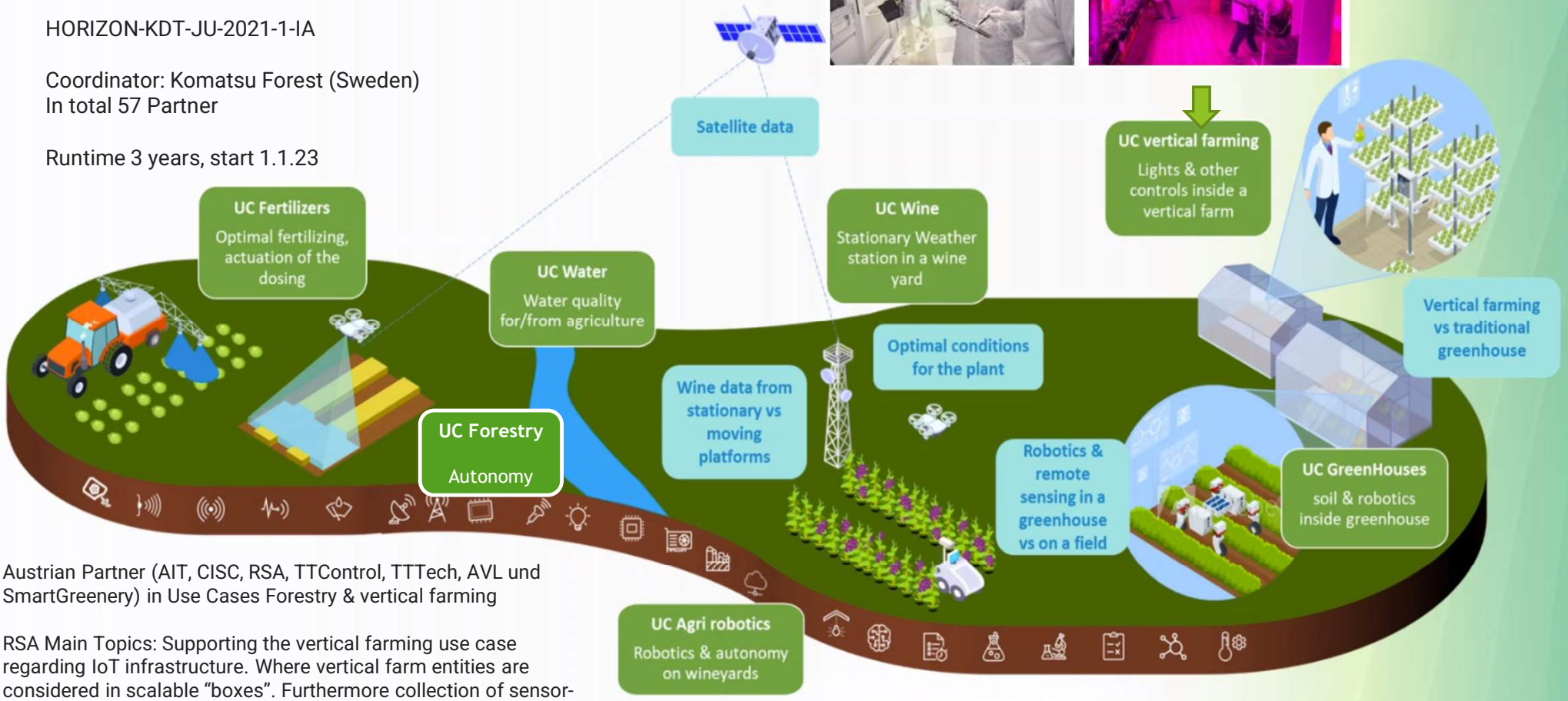
What we do, example project:

AGRARSENSE - Smart, digitalized components and systems for data-based Agriculture and Forestry

HORIZON-KDT-JU-2021-1-IA

Coordinator: Komatsu Forest (Sweden)
In total 57 Partner

Runtime 3 years, start 1.1.23



Austrian Partner (AIT, CISC, RSA, TTControl, TTTech, AVL und SmartGreenery) in Use Cases Forestry & vertical farming

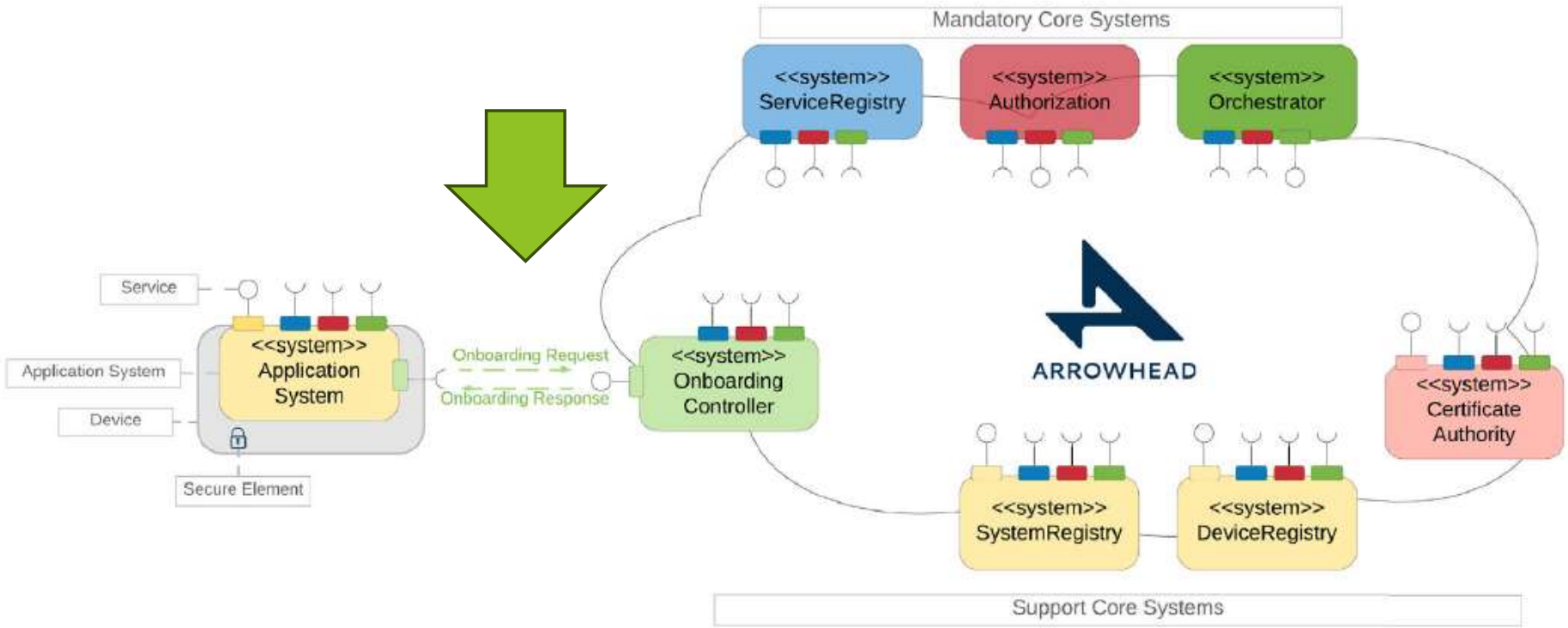
RSA Main Topics: Supporting the vertical farming use case regarding IoT infrastructure. Where vertical farm entities are considered in scalable “boxes”. Furthermore collection of sensor-data and investigation of the correlation of physical and digital scalability (considering synergies to data space topics)

Fraunhofer :: csem SPINVERSE

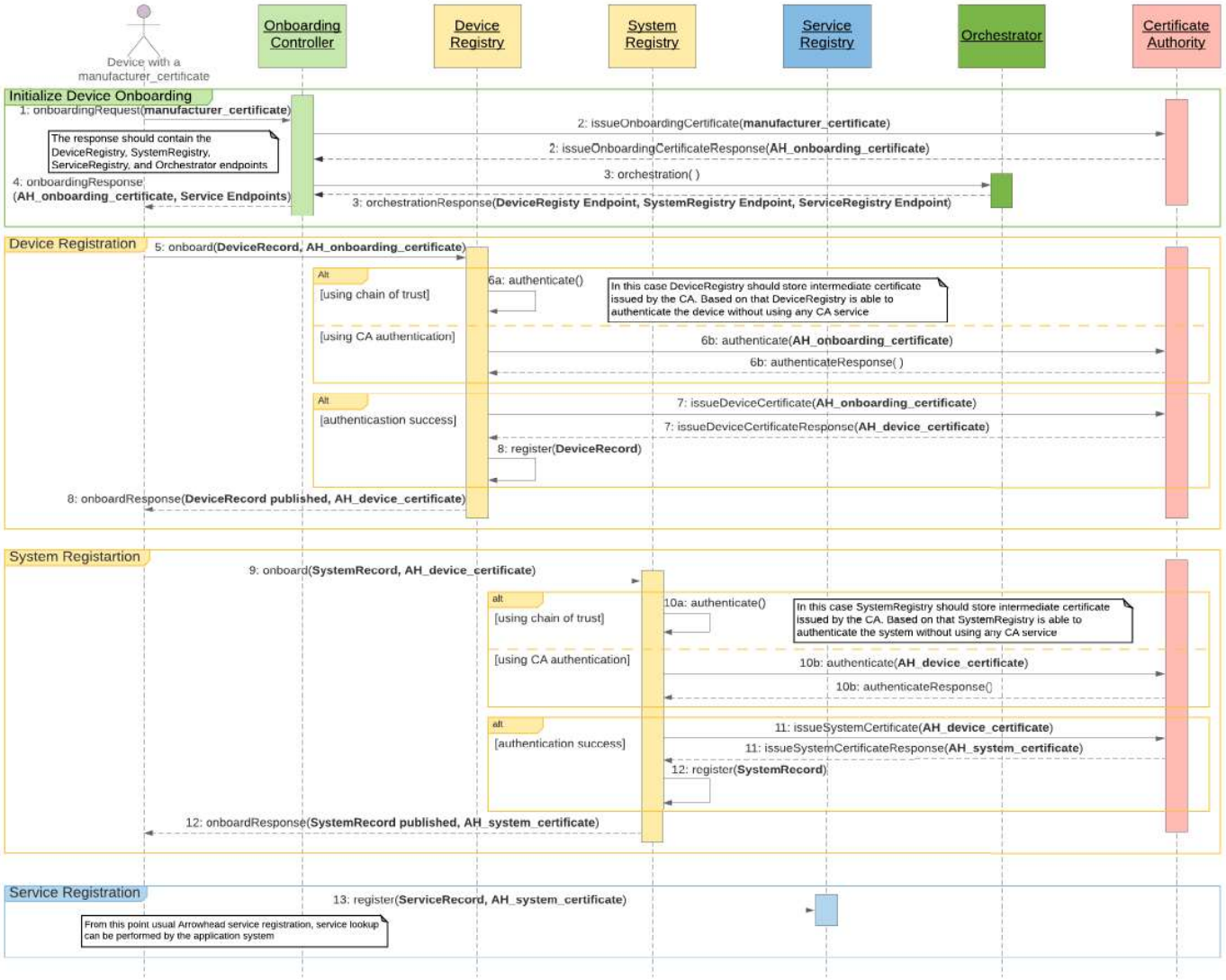
Secure onboarding

Disclaimer: Work in progress, draft code in git

Secure onboarding to the Arrowhead local cloud (Disclaimer: Draft Code in git)



Onboarding Procedure



Security Standards

Security Guidelines & Info

- ISO/IEC 27000:2016 Overview of “information security management systems” (ISMS), terms, and definitions commonly used in the ISMS standards.
- ISO/IEC 27001:2013 requirements for implementing, maintaining, and continually improving ISMS (includes risk assessment)
- ISO/IEC 27002:2013 guidelines for organizational information security standards and information security management practices including controls (based on 27001)
- ISO/IEC 27017:2015 provides controls and implementation guidance for both cloud service providers and cloud service customers (in addition to 27002).
- ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in *ISO/IEC* 29100 for the public cloud computing environment.
- IEC 62443 is an international series of standards that address cybersecurity for operational technology in automation and control systems. The standard is divided into different sections and describes both technical and process-related aspects of automation and control systems cybersecurity in industrial internet of things.

ISO27017 – examples

Duties and responsibilities between Cloud Service Customer & Cloud Service Provider must be defined and documented regarding e.g. Operations Security Controls (12)

	Security Control		Security Objectives	
(12) Operations Security	12.1 Operational procedures and responsibilities	12.1.1	**Documented Operating Procedures** Operating procedures should be documented and made available to all users who need them.	
		12.1.2	**Change Management** Changes that affect information security should be controlled.	
		12.1.3	**Capacity Management** The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	
		12.1.4	**Separation of Development, Testing and Operational Environments** These environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.	
	12.2 Protection from malware	12.2.1	**Controls against Malware** To ensure that information and information processing facilities are protected against malware.	
	12.3 Backup	12.3.1	**Backup** Backup copies should be taken and tested regularly in accordance with an agreed backup policy.	
	12.4 Logging and Monitoring	12.4.1	**Event Logging** Event logs recording user activities, errors and information security events should be produced, kept and regularly reviewed.	
		12.4.2	**Protection of Log Information** Logging facilities and log information should be protected against tampering and unauthorized access.	
		12.4.3	**Administrator and Operator Logs** System administrator should be logged and the logs protected and regularly reviewed.	
		12.4.4	**Clock Synchronization** The clocks of all relevant information processing systems should be synchronized to a single reference time source.	
	12.5 Control of operational software	12.5.1	**Installation of Software on Operational Systems** Procedures should be implemented to control the installation of software on operational systems.	
	12.6 Technical vulnerability management	12.6.1	**Management of Technical Vulnerabilities** Information about technical vulnerabilities should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	
		12.6.2	**Restrictions on Software Installation** Rules governing the installation of software by users should be established and implemented.	
	12.7 Information systems audit considerations	12.7.1	**Information Systems Audit Controls** Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.	

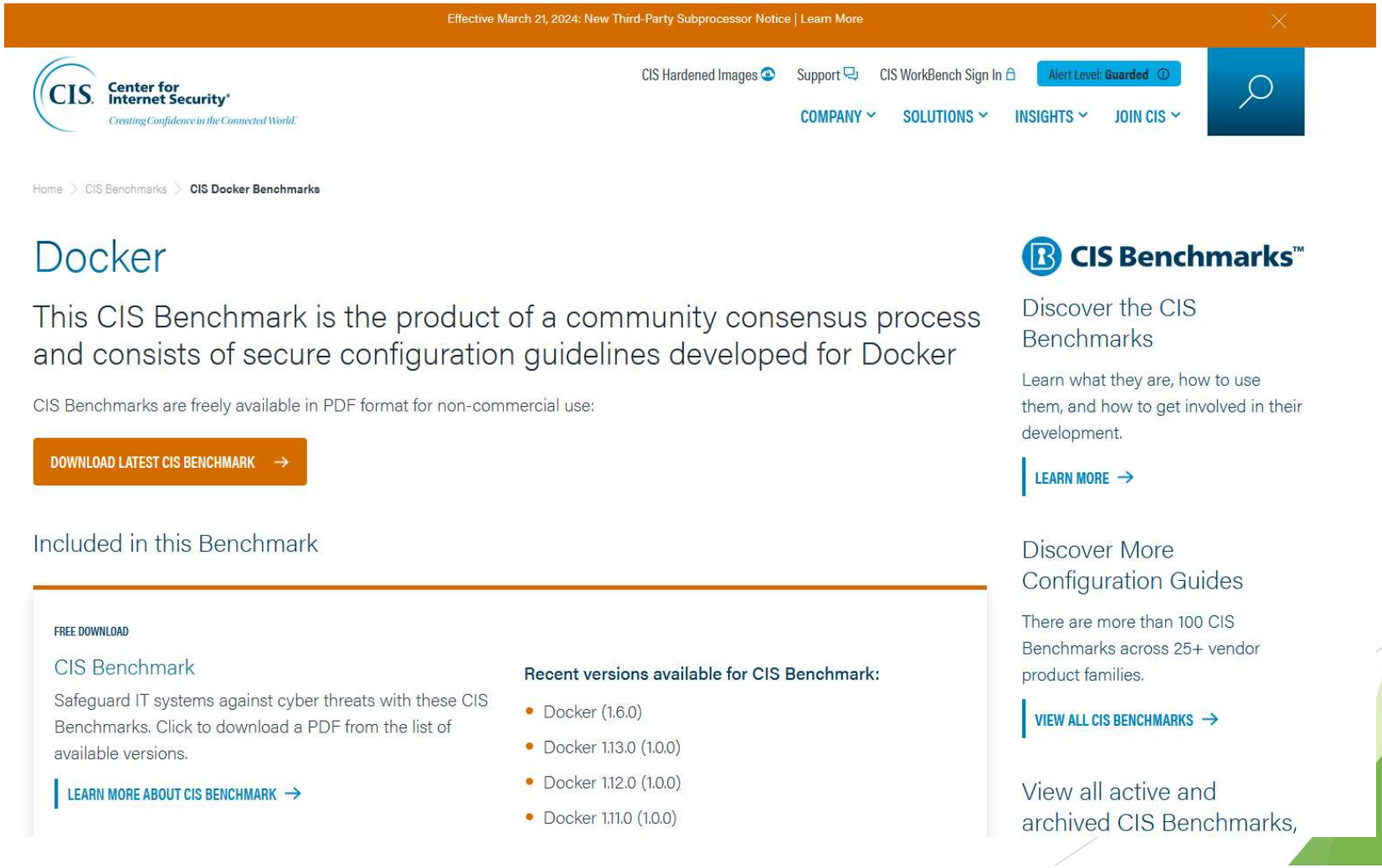
CIS Benchmarks

Examples for IoT

URL https://www.cisecurity.org/cis-benchmarks (register for free)

CIS Control 1: Inventory and Control of Hardware Assets			Applicability	
Sub-Control	Control Title	Control Description	Included?	Justification
1.1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	•	Active discovery tools should be implemented to identify IoT devices, although some types of scans could leave devices in a nonfunctional state. The types of scans run against high-value or critical IoT assets should be contemplated before they are run, with the outcomes known beforehand.
1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	•	A passive asset discovery tool may not identify all IoT devices but is a solid step forward to understanding the devices on the network.
1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	•	This Sub-Control should be applicable to IoT devices using Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6).

More ..


Effective March 21, 2024: New Third-Party Subprocessor Notice | Learn More
CIS Center for Internet Security
Creating Confidence in the Connected World
CIS Hardened Images
Support
CIS WorkBench Sign In
Alert Level: Guarded
COMPANY
SOLUTIONS
INSIGHTS
JOIN CIS
Home > CIS Benchmarks > CIS Docker Benchmarks
Docker
This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for Docker
CIS Benchmarks are freely available in PDF format for non-commercial use:
DOWNLOAD LATEST CIS BENCHMARK
Included in this Benchmark
FREE DOWNLOAD
CIS Benchmark
Safeguard IT systems against cyber threats with these CIS Benchmarks. Click to download a PDF from the list of available versions.
LEARN MORE ABOUT CIS BENCHMARK
Recent versions available for CIS Benchmark:
Docker (1.6.0)
Docker 1.13.0 (1.0.0)
Docker 1.12.0 (1.0.0)
Docker 1.11.0 (1.0.0)
CIS Benchmarks™
Discover the CIS Benchmarks
Learn what they are, how to use them, and how to get involved in their development.
LEARN MORE
Discover More Configuration Guides
There are more than 100 CIS Benchmarks across 25+ vendor product families.
VIEW ALL CIS BENCHMARKS
View all active and archived CIS Benchmarks,

1.1.1 Ensure a separate partition for containers has been created (Manual)

Profile Applicability:

- Level 1 - Docker - Linux

Description:

All Docker containers and their data and metadata is stored under `/var/lib/docker` directory. By default, `/var/lib/docker` should be mounted under either the `/` or `/var` partitions dependent on how the Linux operating system in use is configured.

Rationale:

Docker depends on `/var/lib/docker` as the default directory where all Docker related files, including the images, are stored. This directory could fill up quickly causing both Docker and the host to become unusable. For this reason, you should create a separate partition (logical volume) for storing Docker files.

Impact:

None.

Audit:

At the Docker host execute one of the below commands:

```
grep '/var/lib/docker\s' /proc/mounts
```

This should return the partition details for the `/var/lib/docker` mountpoint.

```
mountpoint -- "$(docker info -f '{{ .DockerRootDir }}')"
```

This should return whether the configured root directory is a mount point.

Remediation:

For new installations, you should create a separate partition for the `/var/lib/docker` mount point. For systems which have already been installed, you should use the Logical Volume Manager (LVM) within Linux to create a new partition.

Default Value:

By default, `/var/lib/docker` is mounted under the `/` or `/var` partitions dependent on how the OS is configured.

References:

1. https://www.projectatomic.io/docs/docker-storage-recommendation/
2. https://docs.docker.com/storage/

1.1.2 Ensure only trusted users are allowed to control Docker daemon (Manual)

Profile Applicability:

- Level 1 - Docker - Linux

Description:

The Docker daemon currently requires access to the Docker socket which is, by default, owned by the user `root` and the group `docker`.

Rationale:

Docker allows you to share a directory between the Docker host and a guest container without limiting the access rights of the container. This means that you can start a container and map the `/` directory on your host to the container. The container would then be able to modify your host file system without any restrictions. This means that you could gain elevated privileges simply by being a member of the `docker` group and subsequently start a container which maps the root `/` directory on the host.

Impact:

Provided the proceeding instructions are implemented, rights to build and execute containers as normal user would be restricted.

Audit:

Execute the following command on the docker host and ensure that only trusted users are members of the `docker` group.

```
getent group docker
```

Remediation:

You should remove any untrusted users from the `docker` group. Additionally, you should not create a mapping of sensitive directories from the host to container volumes.

Default Value:

Not Applicable

References:

1. https://docs.docker.com/engine/security/#docker-daemon-attack-surface
2. http://www.projectatomic.io/blog/2015/08/why-we-dont-let-non-root-users-run-docker-in-centos-fedora-or-rhel/

Continuous Security Standard compliance evaluation in Arrowhead

Disclaimer: Work in progress, draft code in git

Compliance

- ID: [MSI-5] - Secure Boot
- Source: [ISO 27002, ISO 27017, ISO 15408]
- Definition: Secure boot supports integrity by checking and identifying if the firmware of each device, operating system and software is valid. Without secure boot, attackers can easily take advantage of several pre-boot points including the system firmware and running a non-secure operating system
- Monitoring plugin: Secure boot can be monitored by integrating probes that check if the operating system uses Unified Extensible Firmware Interface (UEFI)
- Monitoring Value: True or False
- Monitoring Script (Agent)

```
#!/usr/bin/python3
import os, sys
if(os.path.exists('/sys/firmware/efi')):
            print('OK - System was booted using EFI')
            sys.exit(0);
else
            print('CRITICAL - System was not booted using EFI')
            sys.exit(2);
```

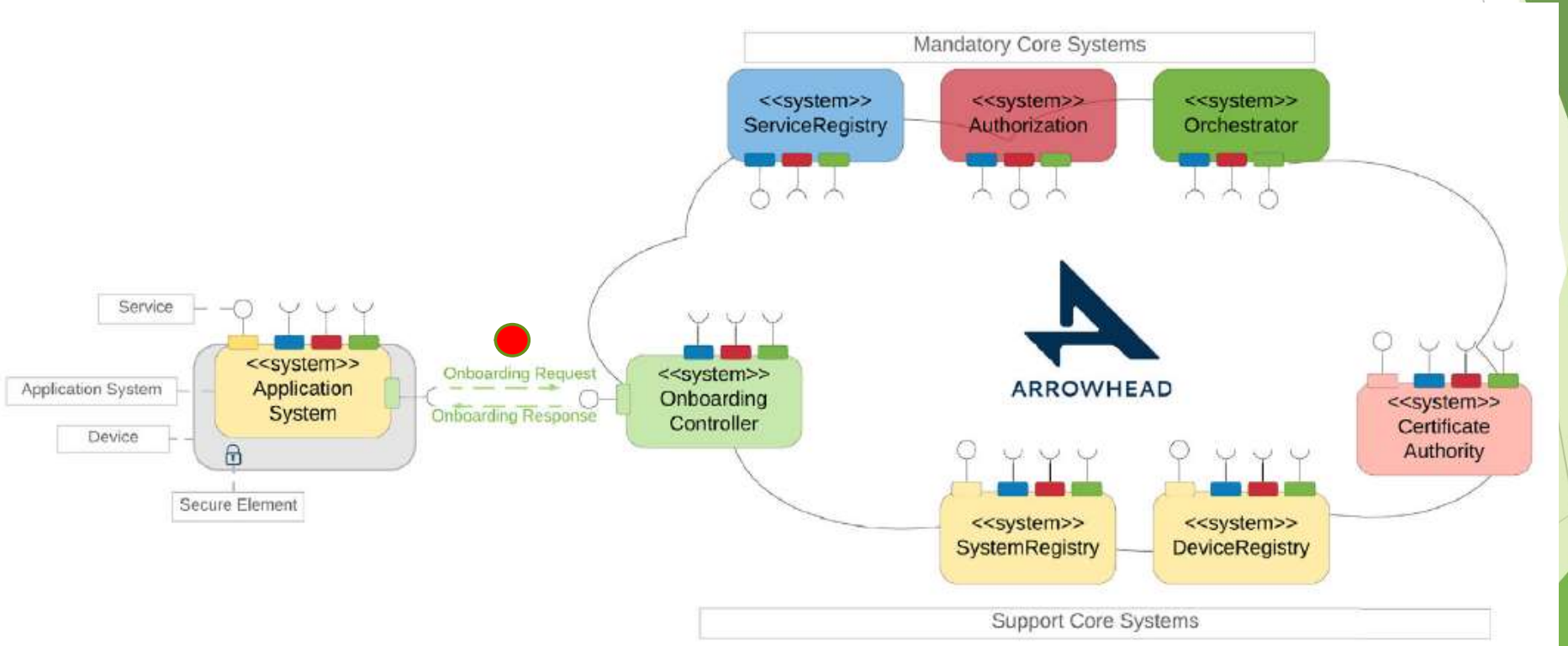
More Code …

Strong Password
ISO / IEC 27002 mapping: 11.5.3
NIST Special Publication 800-53 mapping: IA-5
Catalog of Control Systems Security mapping: 2.15.16

```
379 def win_strong_password_check():
380     rV = {'requirestrongkey': '0'}
381     aReg = ConnectRegistry(None, HKEY_LOCAL_MACHINE)
382     aKey = OpenKey(aReg, r'SYSTEM\CurrentControlSet\services'
383                    '\Netlogon\Parameters')
384
385     n, v, t = EnumValue(aKey, 4)
386     rV['requirestrongkey'] = v
387
388     wspc = Check('266715bc-ca34-4adb-9c9d-f
389     return wspc
```

```
147 def strong_password_check():
148     # For those methods that return more than one value, OrderedDicts should
149     # be used because it actually looks nicer. Can be changed if performance
150     # suffers.
151     rV = OrderedDict()
152     f = '/etc/pam.d/common-password'
153     if os.path.isfile(f) is not True:
154         rV['null'] = 'null'
155         spc = Check('266715bc-ca34-4adb-9c9d-f83021978e26', rV)
156         return spc
157
158     with open(f, 'r') as strong:
159         r = re.compile('password\t*\[success=1.default=ignore\]\t'
160                        '*pam_unix.so')
161         for line in strong:
162             if r.search(line) is not None:
163                 argline = line.rsplit()
164
165         for e in argline[6:]:
166             rV[e.split('=')[0]] = e.split('=')[1]
167
168         spc = Check('266715bc-ca34-4adb-9c9d-f83021978e26', rV)
169
170         return spc
```

Security in IoT Frameworks



Reflect on Security & Literatur

- We are never secure, but we can be compliant with security standards!
- Silia Maksuti, Ani Bicaku, Mario Zsilak, Igor Ivkic, Balint Péceli, Gabor Singler, Kristof Kovács, Markus Tauber, Jerker Delsing "Automated and Secure Onboarding for System of Systems," in IEEE Access, vol. 9, pp. 111095-111113, 2021, doi: 10.1109/ACCESS.2021.3102280.
- Ani Bicaku, Mario Zsilak, Peter Theiler, Markus Tauber and Jerker Delsing, "Security Standard Compliance Verification in System of Systems," in IEEE Systems Journal 2021, doi:10.1109/JSYST.2021.3064196
- IoT – adds another layer to take care off!
  - Eaves dropping
  - Noise Jamming
  - …

Security insights

Markus.tauber@researchstudios.at

www.markus.tauber.co.at

www.researchstudio.at

Sept. 2024