Insights and selected topics from an enterprise security architecture – From Cybersecurity Hygiene to Dev, to Ops and in between

Dr. Fatbardh Veseli
Enterprise Cybersecurity Architect
E.ON Digital Technology GmbH

10.12.2024
Goethe University Frankfurt

slido

Please download and install the Slido app on all computers you use

How is your mood today?

ⓘ Start presenting to display the poll results on this slide.

About...

Automating Server Hardening – From Dev to Ops and in between

Personal Career & Life Tips

Open Talk ...
Ask me anything

About...

slido

Please download and install the Slido app on all computers you use

Do you know E.ON?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

What is the main business of E.ON?

ⓘ Start presenting to display the poll results on this slide.

Who we are

The E.ON Group is one of Europe's largest energy companies, operating in 15 countries with energy networks and energy infrastructure and providing innovative customer solutions. Thus, we are decisively driving forward the energy transition in Europe and are committed to sustainability, climate protection, and the future of our planet.

And these are not just words: We act - instead of just make promises. We lead the way - not just follow.
We rely on the power of the community – and not on individual interests, without having an overarching goal.
Discover who we are, what we do, what we stand for, and more.

Employees 74 thousand	Customers 48 millions
Energy networks 1.60 millions of kilometres	Regulated asset base 36 billion euro
Renewable energy systems 900 thousand	Adjusted EBITDA 8.10 billion euro

e·on

it's on us

to make new energy work.

» After years of fundamental change and reorganisation of the Group, we are shaping the new energy system. This is our ambition as the playmaker of Europe's energy transition. «

Leonhard Birnbaum, CEO of E.ON SE

E.ON Digital Technology

~1600
Employees

München
Essen
Berlin
Hannover
Würzburg and more!

Hybrid Working

International
Network

Data, Analytics and IoT
Future Lab
AI and Smart Energy
Solutions

Du-Culture
Team spirit
Growth
Purpose

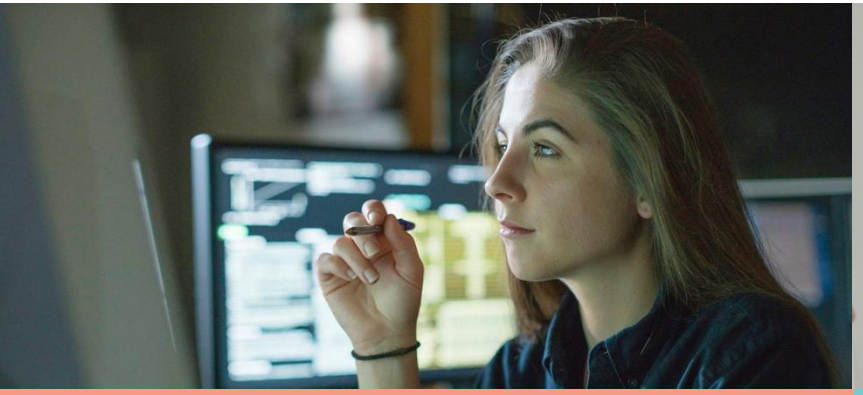
EDT – A great place to work

The **regulations** and **benefits** for employees of E.ON Digital Technology GmbH are the basis for our cooperation, working conditions, personal development and work-life balance.

Your Story at E.ON

Start @ E.ON Digital Technology

Opportunities for your Career Path



Master Thesis

You will be given a topic from E.ON and we will supervise you during your final Thesis.

Intern/Working Student

Gain first working experience and connections through our Emerging Talents Program, which supports you during an Internship or Working Student job

Entry Position

Shape your future after your graduation with a direct entry @E.ON Digital Technology.

One-Pager CV

Dr. Fatbardh Veseli

Enterprise Cybersecurity Architect

E.ON Digital Technology GmbH
Frankfurt am Main

EDUCATION

- *Dr. rer. nat.,* Goethe University Frankfurt, Computer Science
- *M.Sc.* Information Security, NTNU, Norway
- *B.Sc.* Mathematics – Computer Science, Uni Prishtina, Kosovo
- B.Sc. Management & Informatics, Uni Prishtina, Kosovo

CERTIFICATIONS

- *Security & Privacy*: CISSP, ISO 27001 Lead Auditor, IAPP CIPM (Certified Information Privacy Manager), IAPP CIPT (Certified Information Privacy Technologist)
- *Architecture*: TOGAF Certified, Capgemini Certified Architect (L1), AZ 900 Microsoft Azure Fundamentals
- *Management*: Professional Scrum Master (PSM I), Certified SAFE 5 Agilist, ITIL v4 Foundation, Prince2 Practitioner, Connected Manager (Harward)

PROFESSIONAL EXPERIENCE

Combining over 17 years of research and industry experience

Industries & Sectors

- Public Sector
- Automotive
- Transport
- Research & Education
- Policy Making

Hobbies

- Basketball
- Football
- Cycling

ADDITIONAL ROLES

- Member, ENISA AHWG Privacy Engineering
- Senior Lecturer, Riinvest College
- Reviewer in a number of conferences and workshops
- Father and husband, among other roles

Automating Server Hardening – From Dev to Ops and in between

Link to the slidedeck

Summary


Background
Concept Development & Refinement
Implementation & Rollout
Guiding your Users – Overarching Topics

Background

slido

Please download and install the Slido app on all computers you use

What do you understand under the term “ISMS” (Information Security Management System)?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

Which of the following constitute a Cybersecurity Framework?

ⓘ Start presenting to display the poll results on this slide.

ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls

- **8.9 Configuration management**
  - *"Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed."*
  - *"The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks"*
  - *"(Standard templates for the secure configuration of hardware, software, services and networks should be defined) using publicly available guidance (e.g. pre-defined templates from vendors and from independent security organizations); "*
- **8.18 Use of privileged utility programs: "***removing or disabling all unnecessary utility programs*"
- **8.27 Secure system architecture and engineering principles**; (Secure system engineering should involve) "*hardening of systems*".

slido

Please download and install the Slido app on all computers you use

What is system hardening?

ⓘ Start presenting to display the poll results on this slide.

Wait, what again?

But, how?

Concept Development & Refinement

The concretisation step

From the high level standard (ISO/IEC 27002) to something more tangible

slido

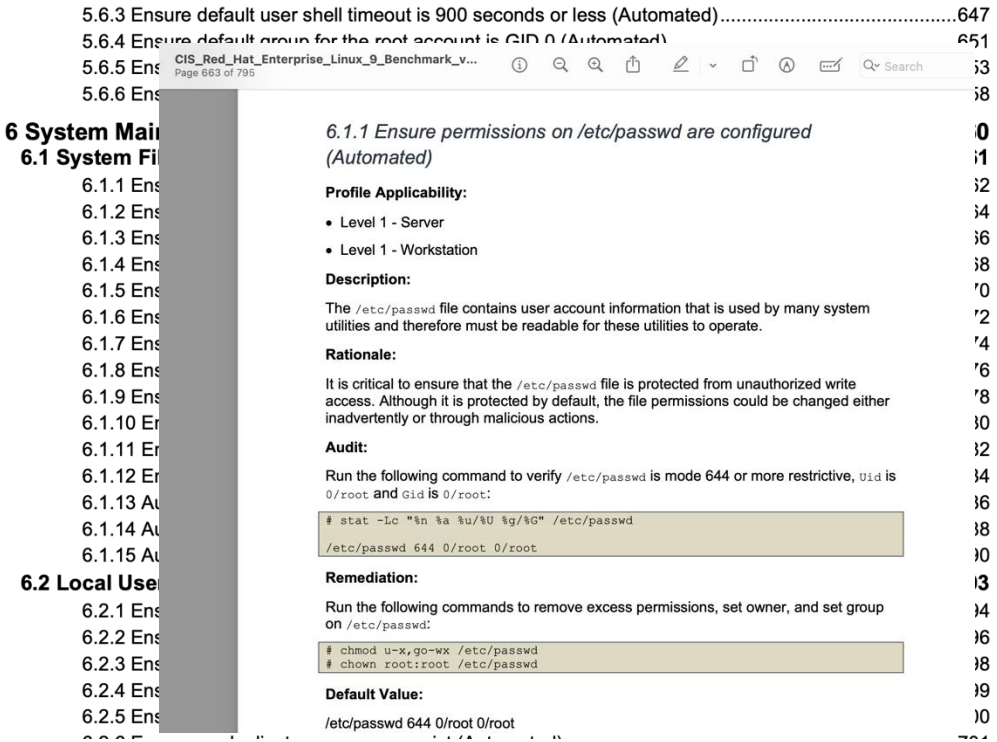
Please download and install the Slido app on all computers you use

Now imagine you are responible for a business application that is running on a Windows Server 2022 (VM) in AWS. How do you do harden this system?

ⓘ Start presenting to display the poll results on this slide.

CIS Benchmarks

- **Center for Internet Security (CIS)**
  - Community-based organization, driven by practitioners
  - Produces de-facto “standard” for system hardening
- **OS specific benchmarks**
  - A benchmark contains a number of configuration recommendations
  - Usually a couple of hundreds of recommendations per benchmark
  - Benchmark versions updated regularly
- Provides **Build Kits** (Scripts) to implement those benchmarks



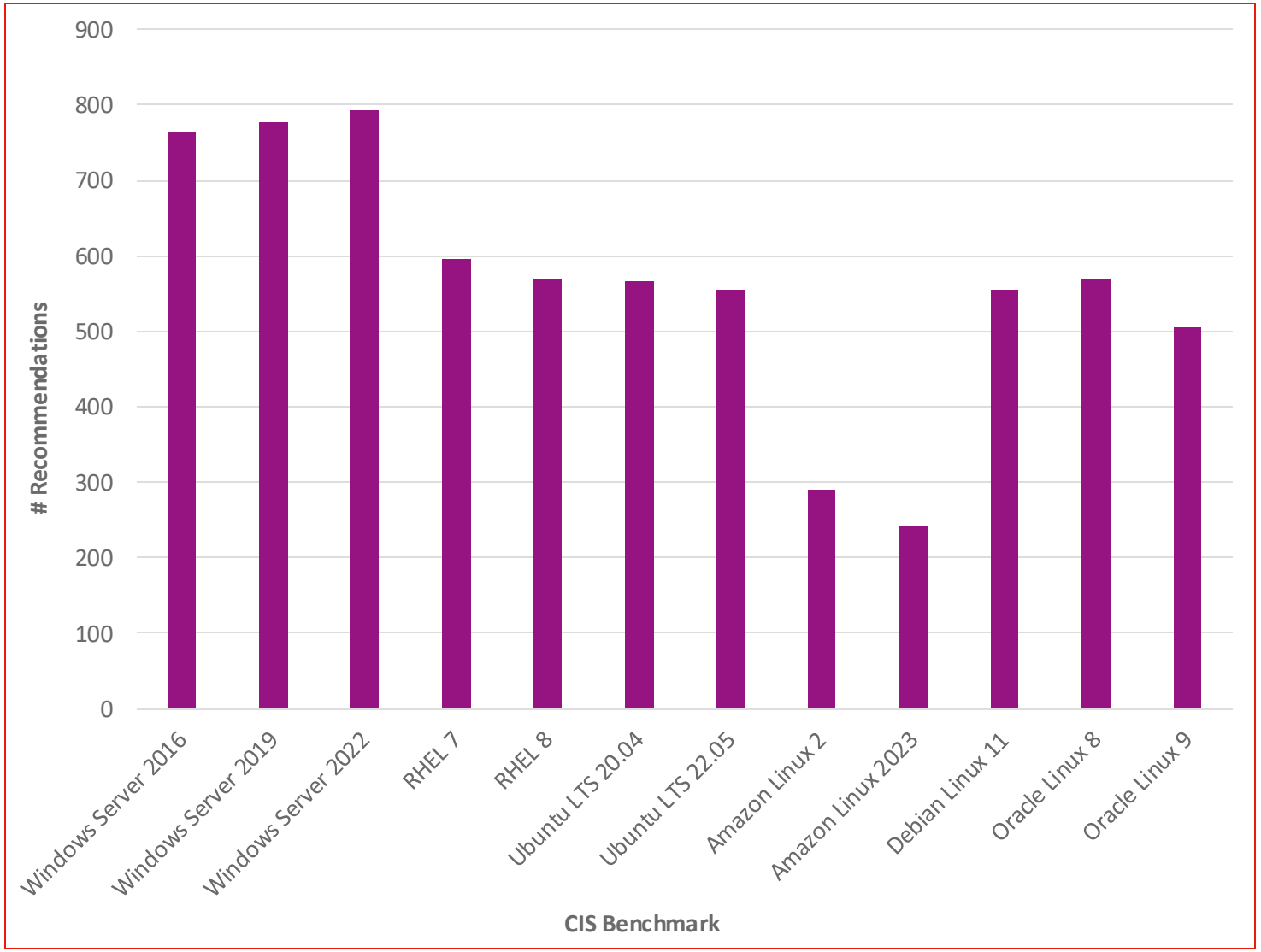
slido

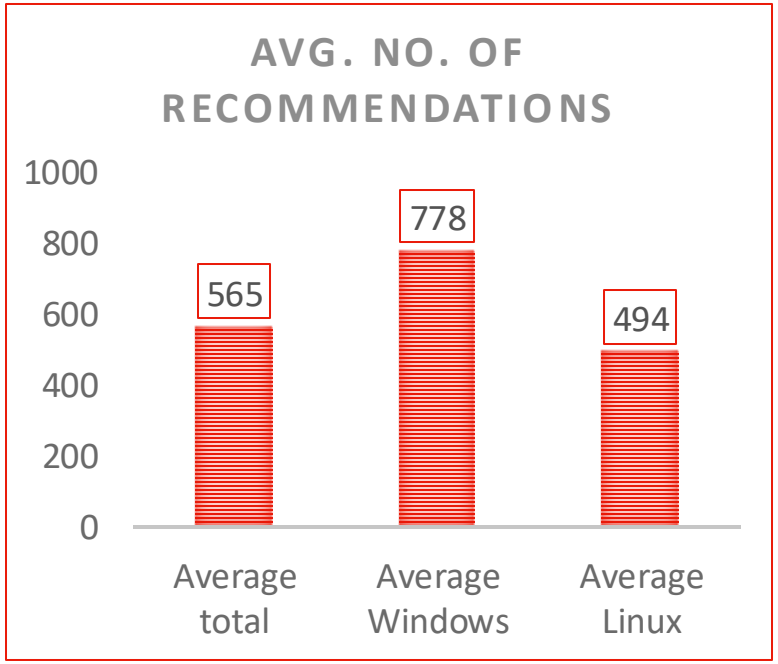
Please download and install the Slido app on all computers you use

How many configuration recommendations does a CIS Benchmark contain on average?

ⓘ Start presenting to display the poll results on this slide.

Number of CIS Recommendations per Benchmark





How to implement this?

- Option 1) **Manually**
  - Seriously?
  - Not an option
- Option 2) **Automate via e.g. script**
  - Sure, why not
  - Sounds like fun

slido

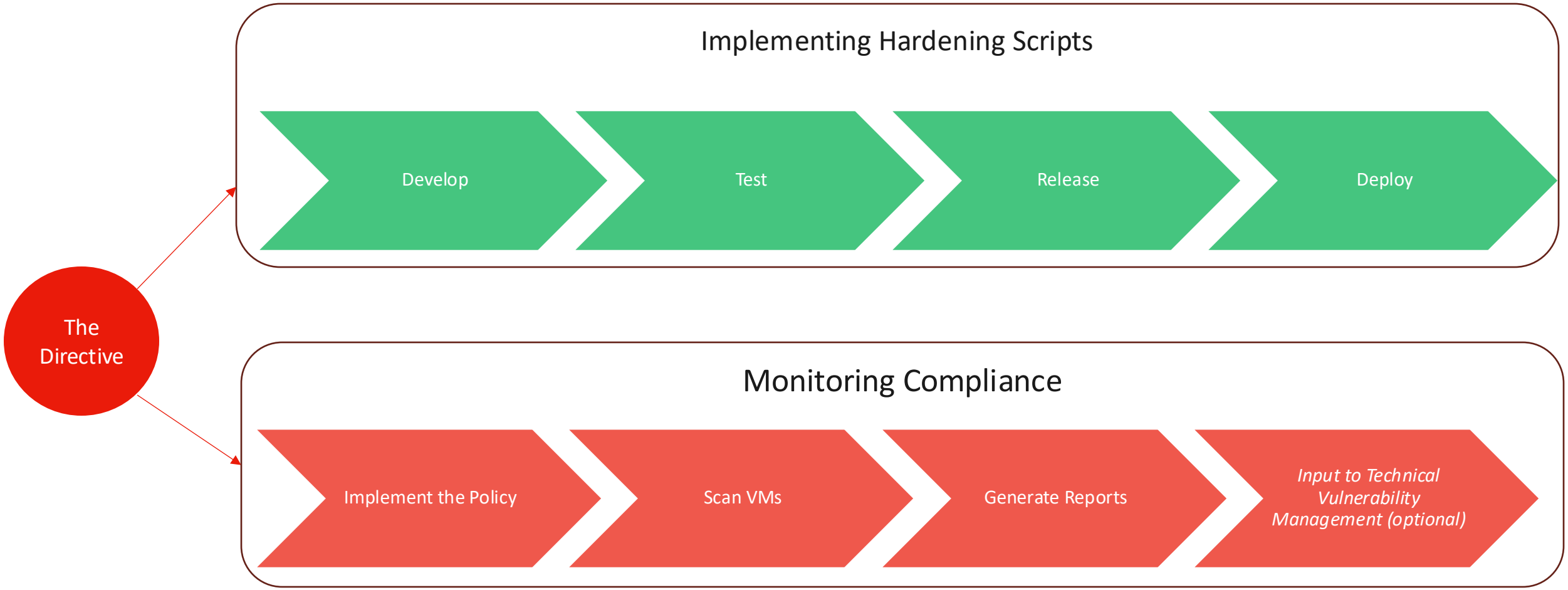
Please download and install the Slido app on all computers you use

Now you are an architect at E.ON and need to make sure that you apply these changes to 10,000 Servers. How do you do that?

ⓘ Start presenting to display the poll results on this slide.

Or, the implementation step

Topical Streams



Implementation & Rollout

slido

Please download and install the Slido app on all computers you use

What do you understand under “agile”?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

Name an agile method that you know

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

What is Scrum?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

Which roles belong to a Scrum team?

ⓘ Start presenting to display the poll results on this slide.

Organisation – Split Dev and Ops

Regular sync (biweekly)

Silo 1: Core (Dev)

- **Product Owner: CSA 1**
- **Scrum Master: CSA 1, CSE 1**
- **Development team (2 consultants for Linux-based OS, 2 consultants for Windows-based OS)**

Silo 2: Cloud Automation (Dev)

- Integrate the scripts cloud native technology
  - Automation for Azure, AWS, GCP
  - Also working in agile (sprints)

Silo 3: Hardening Deployment team public cloud (Ops)

- Select servers
- Deploy

Silo 4: Hardening Deployment team Managed Private Cloud (Ops)

- Select servers
- Request change
- Get change approved
- Deploy

slido

Please download and install the Slido app on all computers you use

What is DevOps?

ⓘ Start presenting to display the poll results on this slide.

Organisation – Towards one team

Regular sync (biweekly)

Silo 1: Core (Dev)

- **Product Owner**
- **Scrum Master**
- **Development team**

Silo 2: Cloud Automation (Dev)

- Integrate the scripts cloud native technology
- Automation for Azure, AWS, GCP
- Also working in agile (sprints)

Step 1) Partly Joint Teams

Silo 3: Hardening Deployment team public cloud (Ops)

- Select servers
- Deploy

Silo 4: Hardening Deployment team Managed Private Cloud (Ops)

- Select servers
- Request change
- Get change approved
- Deploy

Next: ONE product team

Our core toolset in the development

Jira

- Implementation of Scrum
- Scrum board for transparency of our tasks
- Backlog with User Stories
- Starting of our sprints

Confluence

- Central place for documentation
- Results
- Guidance
- Best Practices
- FAQ
- Hardening Script Artifacts

GitLab

- Development of the hardening scripts
- Internal subgroup with one repository per OS script
- Approval workflow for changes
- CI/CD pipeline for automated testing
- Release workflow

X

- Reporting Public Cloud

Y

- Reporting Private Cloud

AWS EC2

- Test environment

Windows:
LGPO files

Linux:
Bash files

slido

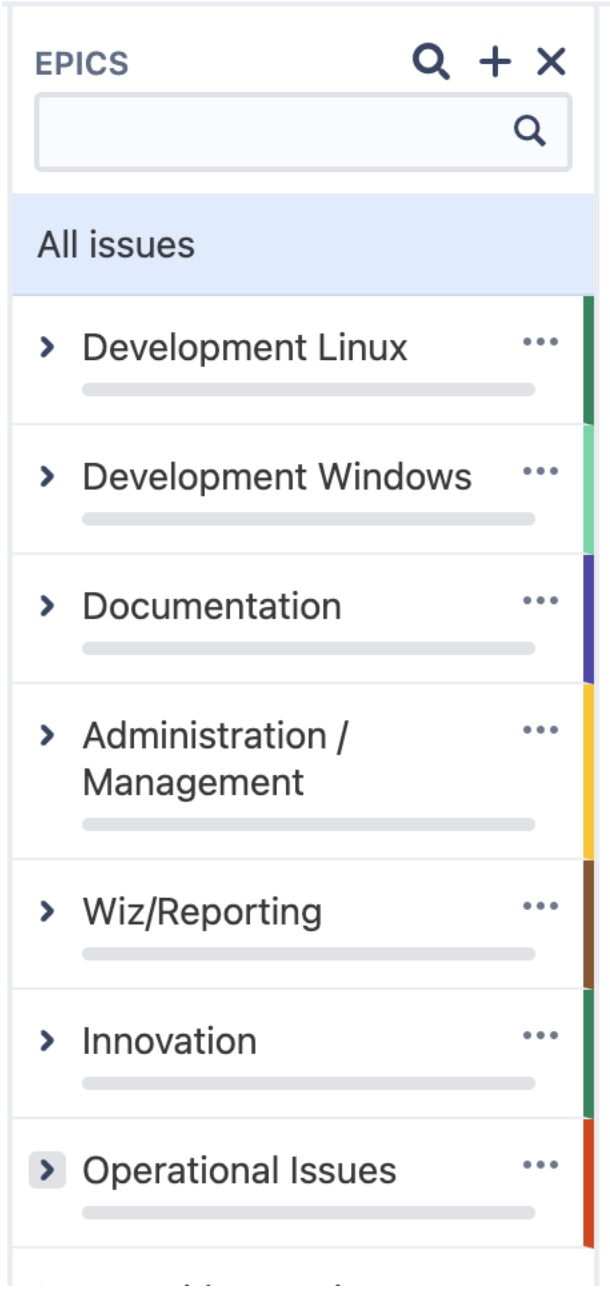
Please download and install the Slido app on all computers you use

Demo?

ⓘ Start presenting to display the poll results on this slide.

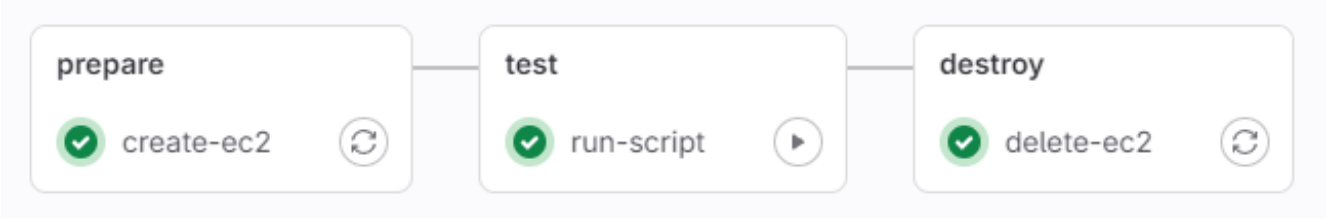
Innovation Management

- **Every fourth sprint an innovation sprint**
  - Automation
  - New features
- An **own Epic** in Jira to collect Stories related to Innovation

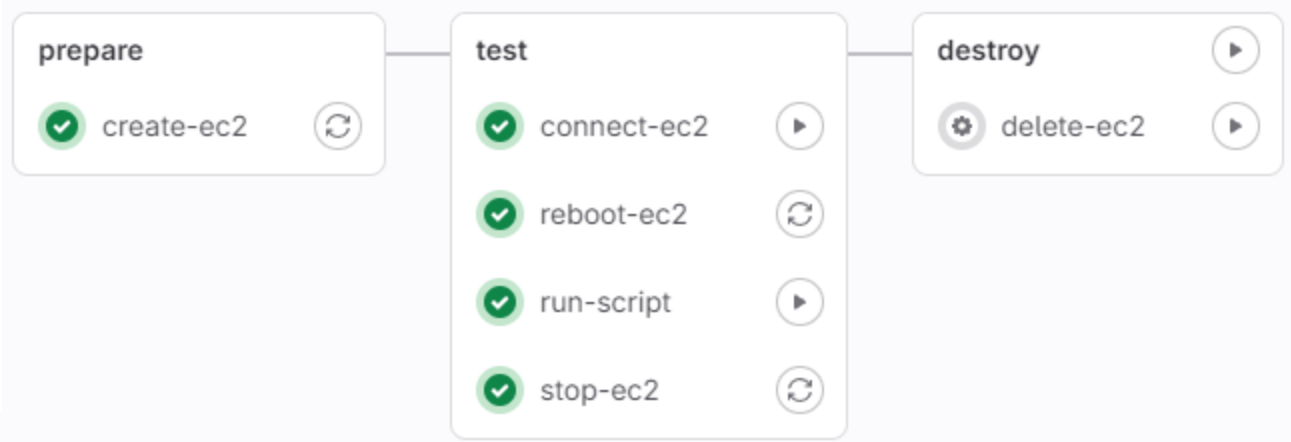


CI/CD pipeline for automated testing and release

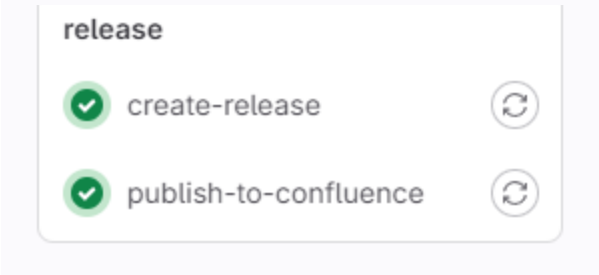
Pipeline for feature branch



Pipeline for main branch/merge request



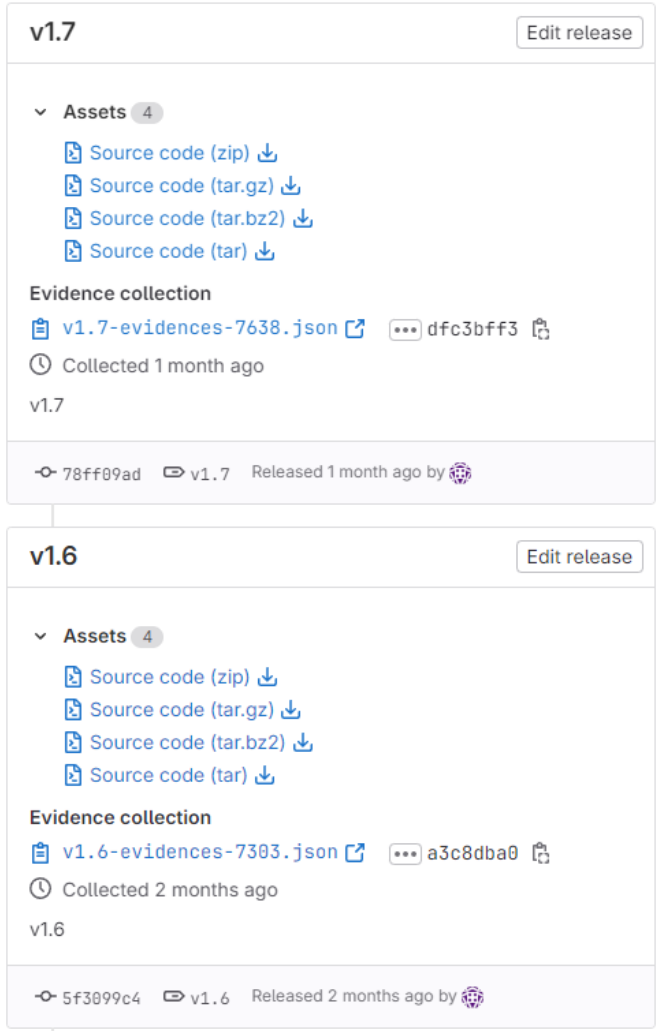
Pipeline for release



Guiding your Users – Overarching Topics

Where to find the scripts?

Either on GitLab (Releases) …



… or on Confluence.

How to use the scripts?

For Linux Servers:

- Hardening Scripts consists of basic *bash scripts*
- More information is described in the README

```
sudo ./cis_lbk.sh --auto-approve --profile L2S
```

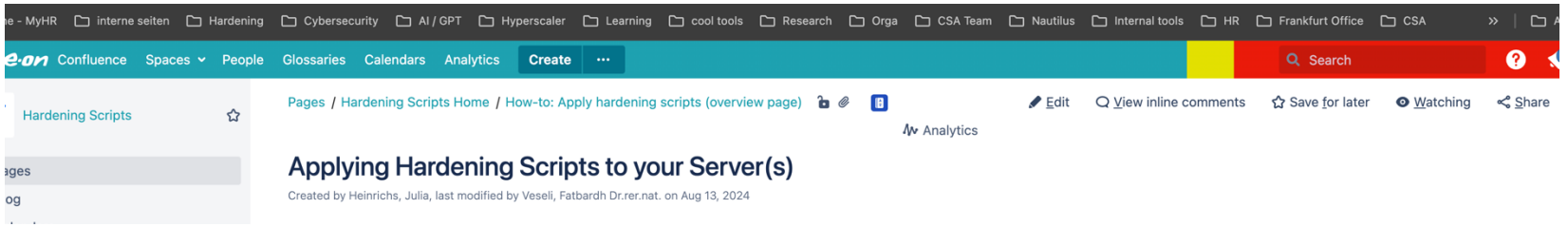
Name	Last commit	Last update
benchmark	Add benchmark	7 months ago
functions	Update recommendati...	1 month ago
.gitignore	gitignore	6 months ago
.gitlab-ci.yml	Add job to stop ec2	1 month ago
README.md	Update README	4 months ago
cis_lbk.sh	Set apt commands to ...	6 months ago
exclusion_list.txt	Remove recommenda...	1 month ago

README.md

Ubuntu Linux 20.04 LTS

The CIS Linux Build Kit (CIS-LBK) is a set of functions used to remediate a Linux system in accordance with the guidance in the corresponding CIS Benchmark defined in the CSD-17 Implementation of CIS Benchmarks.

How to use the scripts?



4.2.1. Apply hardening scripts

1. Open a Command Prompt (cmd) as an Administrator.
2. Change to the directory where LGPO.exe is located and run the corresponding GPO import commands:
   a. Import the GPO files within "User-L1" directory

```
lgpo.exe /g ACTUAL_PATH\User-L1\{ACTUAL GUID}
```

> Note: Replace the ACTUAL_PATH and {Actual_GUID} with the correct path to the directory containing the build kits respectively to the corresponding GUI

Example for Windows Server 2022:

```
lgpo.exe /g \Server2022v2\User-L1\{F0128B1F-844A-4C17-9AD1-BD32F85F7BB9}
```

> Note: Make sure to use a lowercase **/g** in the above command

ated in CSD-17 Implementation of CIS

fully read the section about How to comply to

on average change more than 500 configuration
ry to ensure a smooth hardening process.

   b. Import the GPO files within "User-L2" directory (similar to above)

```
lgpo.exe /g ACTUAL_PATH\User-L2\{ACTUAL GUID}
```

   c. Import the GPO files within "MS-L2" directory (similar to above)

```
lgpo.exe /g ACTUAL_PATH\MS-L2\{ACTUAL GUID}
```

   d. Import the GPO files within "MS-L1" directory (similar to above)

```
lgpo.exe /g ACTUAL_PATH\MS-L1\{ACTUAL GUID}
```

Personal Career & Life Tips

General Career & Life Tips*

- Stay curious
- Learning is fun– keep it that way
- Try to improve the worl around you, not just make money
- Success is a lot about you, not what others want you to value
- Career is important, but you come first
- Integrate small ceremonies in your daily routine – don't wait for the weekend
- Pay attention to your family and friends
- Socialize with people who have a positive influence on you
- Reduce time on social media and digital devices
- Choose a good "boss" and manage him well
- Maintain a hobby

*__Disclaimer__: *The views expressed in this slide are solely my own and do not reflect the opinions or views of my employer.*

Personal notes*

The world suffers a lot. Not because of the violence of bad people, but because of the silence of good people.

- Unknown

***Disclaimer**: *The views expressed in this slide are solely my own and do not reflect the opinions or views of my employer.*

Open Talk …
Ask me anything

slido

Please download and install the Slido app on all computers you use

Audience Q&A

ⓘ Start presenting to display the audience questions on this slide.

slido

Please download and install the Slido app on all computers you use

How did you like the guest lecture?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

What did you find particularly useful?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

What can be improved / added / removed for next time?

ⓘ Start presenting to display the poll results on this slide.