# Leidensweg und Trefferbild
# CIS Benchmark und Härtung für Anfänger

Axel vom Stein – BSS Bohnenberg GmbH

Martin Klier – Performing Databases

BSS MATERIALFLUSSGRUPPE

performing databases

# Speaker

- Martin Klier, Oracle ACE Director
- Performing Databases since 2014

- Solution Architect and Database Expert
- My focus:
  - Performance & Tuning
  - Highly Available Systems
  - Cluster and Replication

- Linux since 1997
- Oracle Database since 2003

Oracle ACE Director

SYMPOSIUM 42
Proud Member of symposium42

# Speaker

- Axel vom Stein, Oracle ACE Pro
- Technical Project Manager, Head of IT
- Working for BSS since 2001

- Oracle:
  - since 2001
  - started out as a developer (PL/SQL, C, C#)
  - interest moved more towards DBA topics

- My focus:
  - teaching trainees and young professionals
  - HA - concepts
  - standardization & automation

Oracle ACE Pro

Oracle ACE

# The Oracle ACE Program

400+ technical experts helping peers globally

- The Oracle ACE Program recognizes and rewards community members for their technical and community contributions to the Oracle community
- 3 membership levels: Director, Pro, and Associate
- Nominate yourself or a colleague at ace.oracle.com/nominate
- Learn more at ace.oracle.com

✉ aceprogram_ww@oracle.com    Facebook.com/OracleACEs    X @oracleace    in Oracle ACE Program Group

# ora2know
# The German Oracle Database Community

MATERIALFLUSSGRUPPE

performing databases

ora2know

The German Oracle Database Community

https://www.ora2know.de

# Logistics / Warehousing

BSS
MATERIALFLUSSGRUPPE

performing
databases

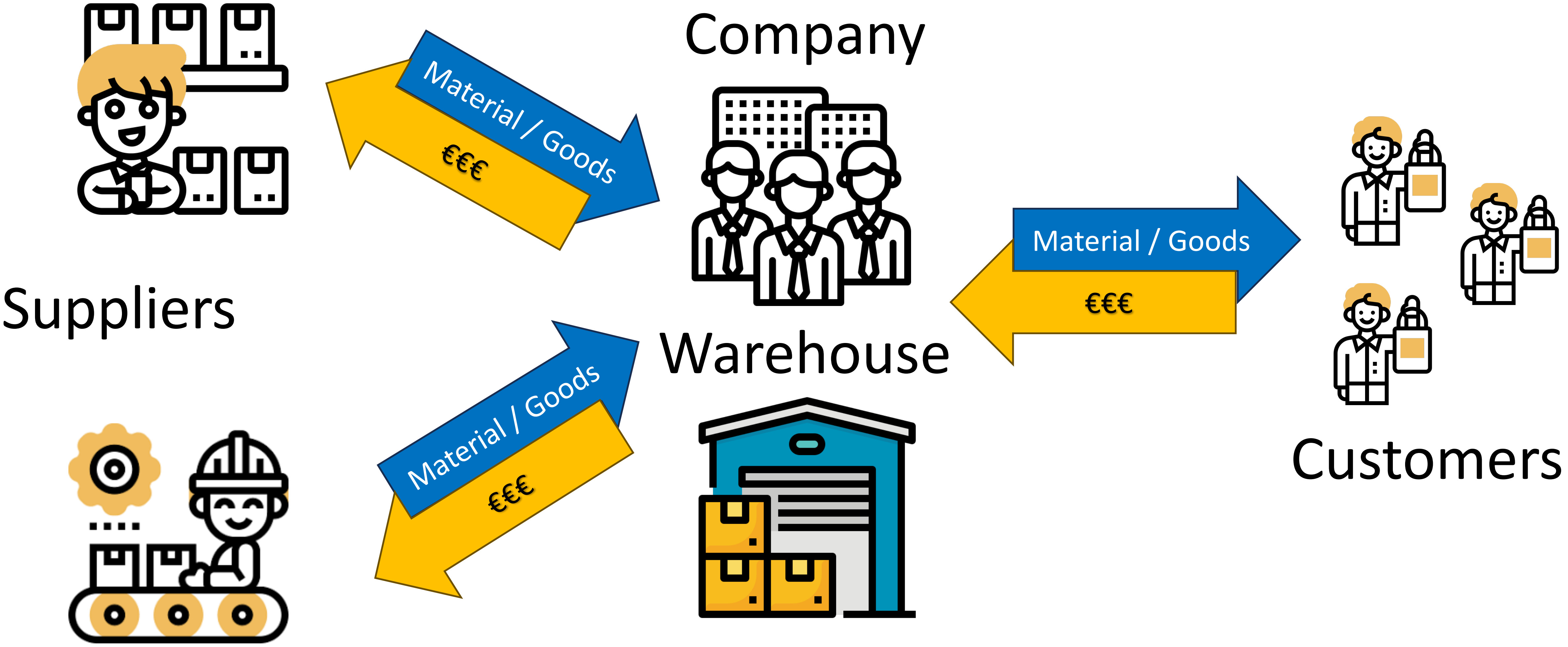
# Logistics Warehousing

# Logistics – Security

Who let the dogs loose?
Who sent the CISO after the warehouse?

Easy answer: Importance!

# Logistics – Importance



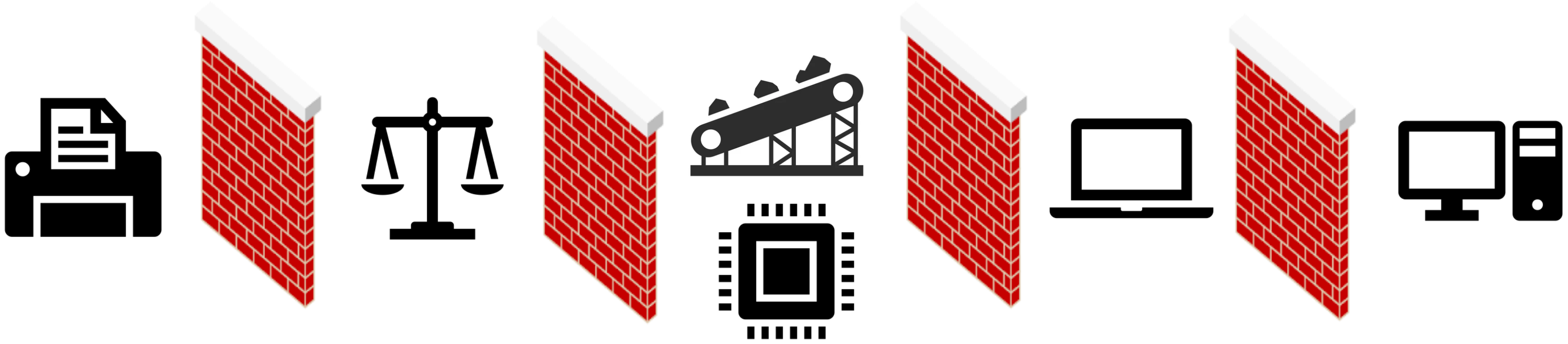
# Logistics – Responsibility

CEO? Logistics is just an expensive asset.
CFO? Wants to earn and not to lose money.
CIO? Bears the IT load on shoulders.
CISO? Priority: Security First. Who needs a business?
COO? The shop must run!
CTO? ...
C...?

Head of Logistics?
**CLO**! (Nice – “Klo” is the German word for ”loo”)

It depends!

# Logistics – Challenges



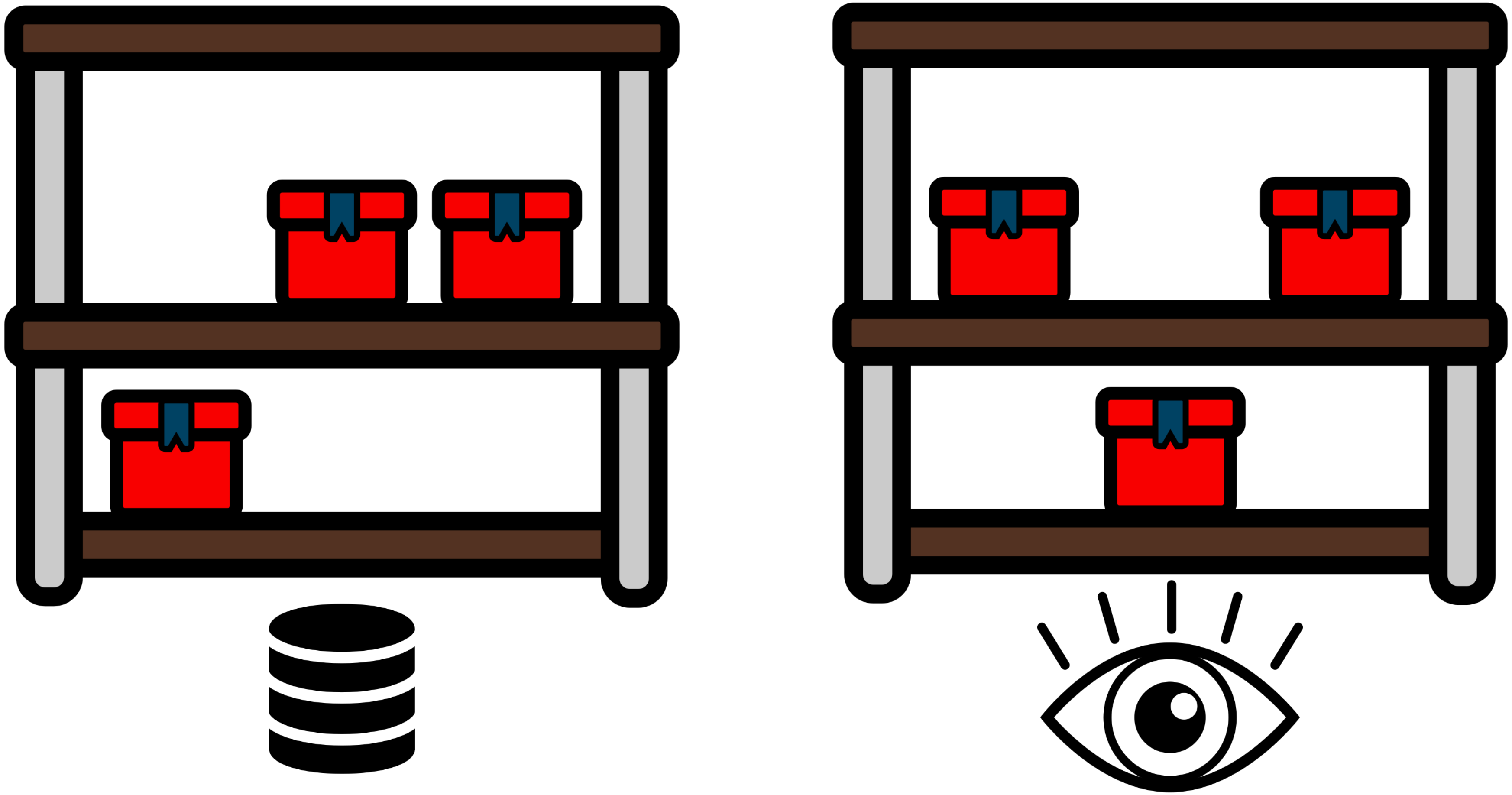
Let’s communicate!

Non-IT pain: Physical security with truck drivers, technicians, craftsmen ....

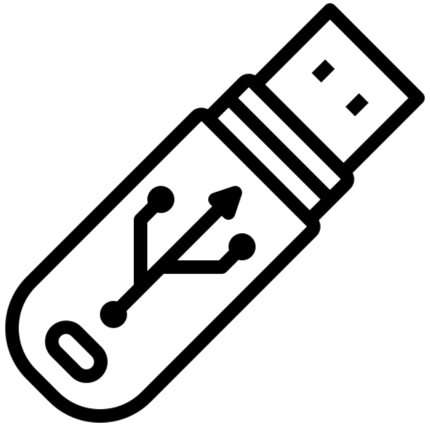
# Security is a Feature!

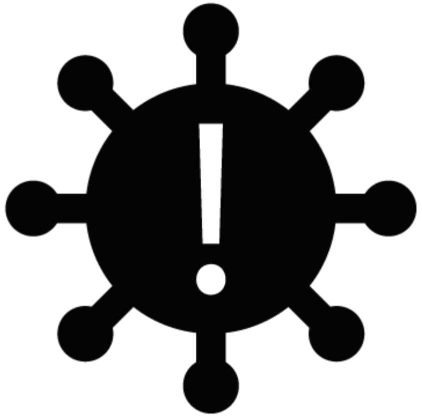
Security is a good feature for our product.

# Logistics – Worst Case



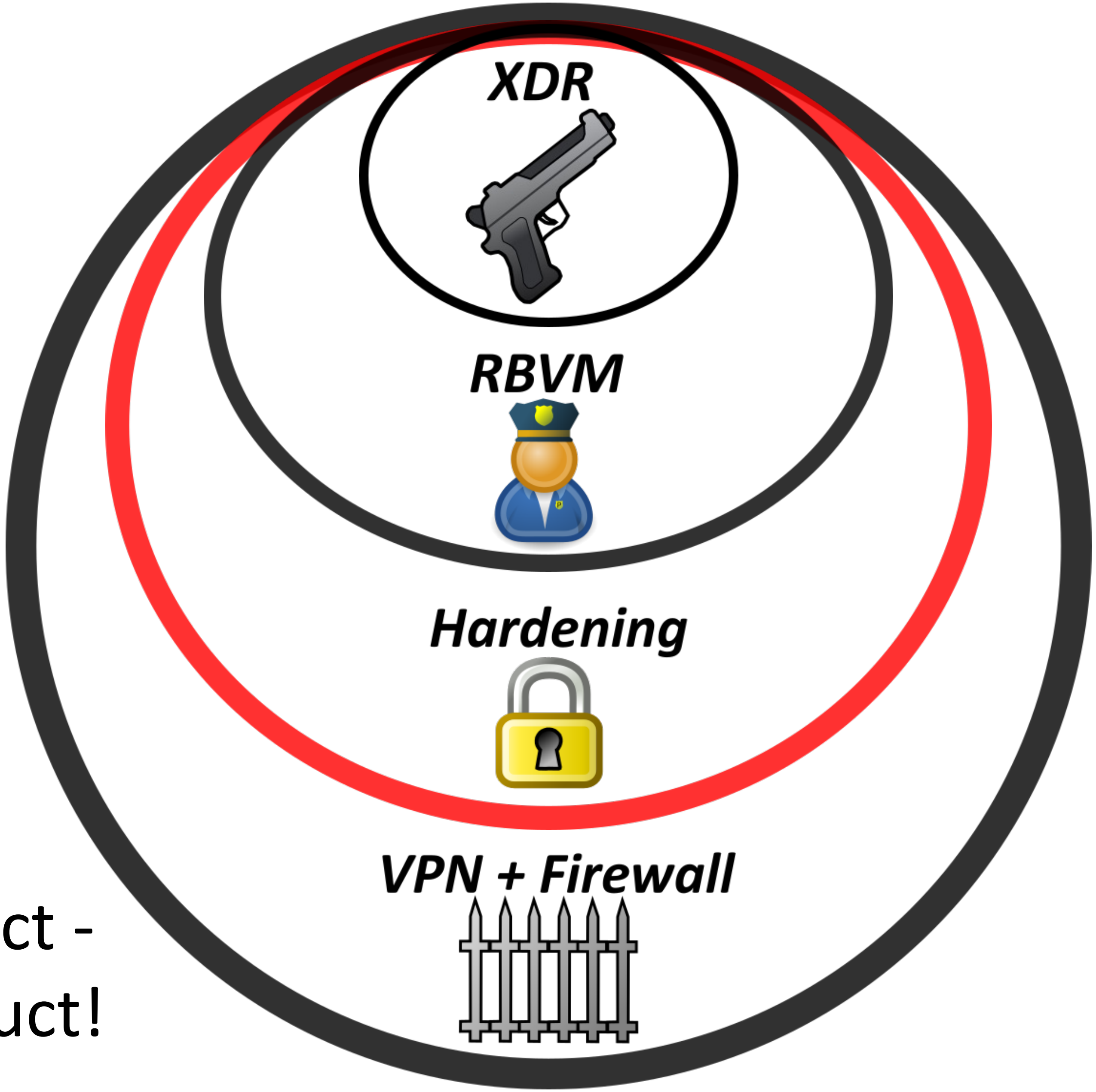
# Attacks – From the Inside?





Be prepared - You never know their strategy!

# Hardening



It’s not just a project -
prepare your product!

# Hardening – Why?

- Don’t be the one to blame – it’s expensive!
- Good feature for a product
- Rather do it by design than by pressure

- There is a lot of Evil out there!
- Better Safe than Sorry

# Hardening – Guidelines

- Own, self-defined rules
- **BSI** Base Protection = German Federal IT Security Agency
- **CIS** Level 1+2 = Center for Internet Security
- DISA* **STIG** = Security Technical Implementation Guide = CIS Level 3

* Defense Information System Agency

# Hardening – Guidelines

- Own, self-defined rules => Do not do it (only)
- BSI Base Protection => Not known outside Germany
- CIS Level 1+2 => International semi-standard
- DISA* STIG => Too strict for many non-military purposes

* Defense Information System Agency

# CIS Level 1 – Lower the Attack Surface

- Level 2 contains Level 1 => Start small

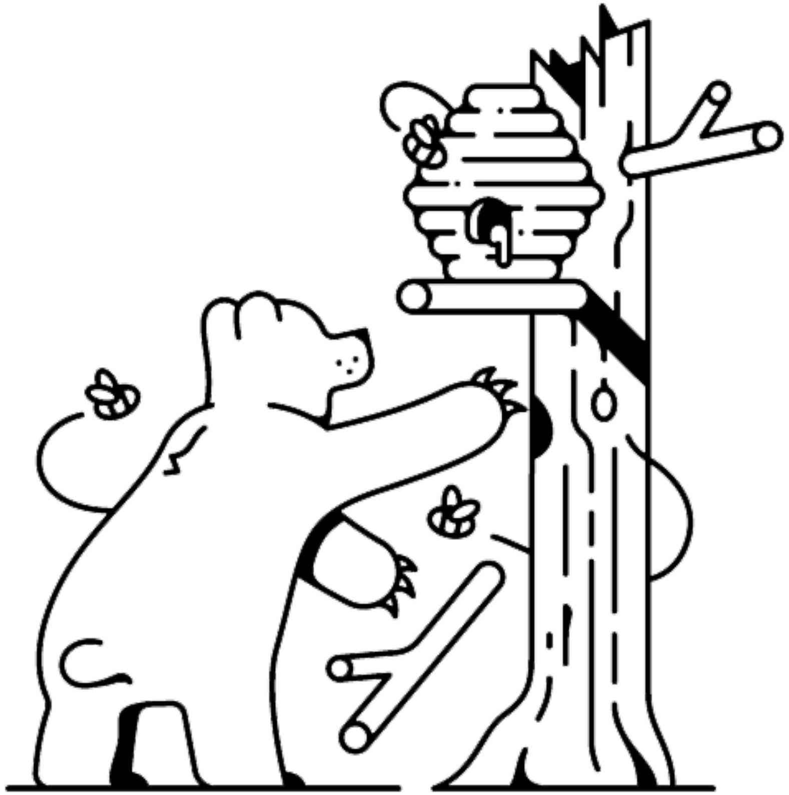
- Keep business impact at bay
- Oracle supports it with DBSAT

- “Keeping machines usable” (CIS quote!)
  (makes me feel bad about Level 2 or STIG ...)

# What is the Definition of Enough?

- Percent-counters happy with 80% Green?
  - 390 of 500 rules implemented?
    - Pen-Test survived?
      - Unpredictable CISO happy?
        - Admin has a good feeling?
          - Business still working?

=> Too many bees for the (little) honey!



# Know where you are – CIS Benchmark

# CIS Benchmark – Document

CIS. Center for Internet Security®

CIS Benchmarks™

CIS Oracle Linux 8 Benchmark

v3.0.0 - 10-30-2023

**pdf has 1011 pages**

# The right Benchmark-Tool … ?

|  | 💰 | ❌💰 |
|---|---|---|
| 🛢 | CIS CAT Pro<br>…? | ORACLE<br>DBSAT<br>Database Security Assessment Tool |
| 🐧 | CIS CAT Pro<br>Tenable<br>Rapid7 | OpenSCAP |

https://www.cisecurity.org/cis-securesuite/members/vendors

# How to do it

Oracle has a guide for OL8 and OpenSCAP:

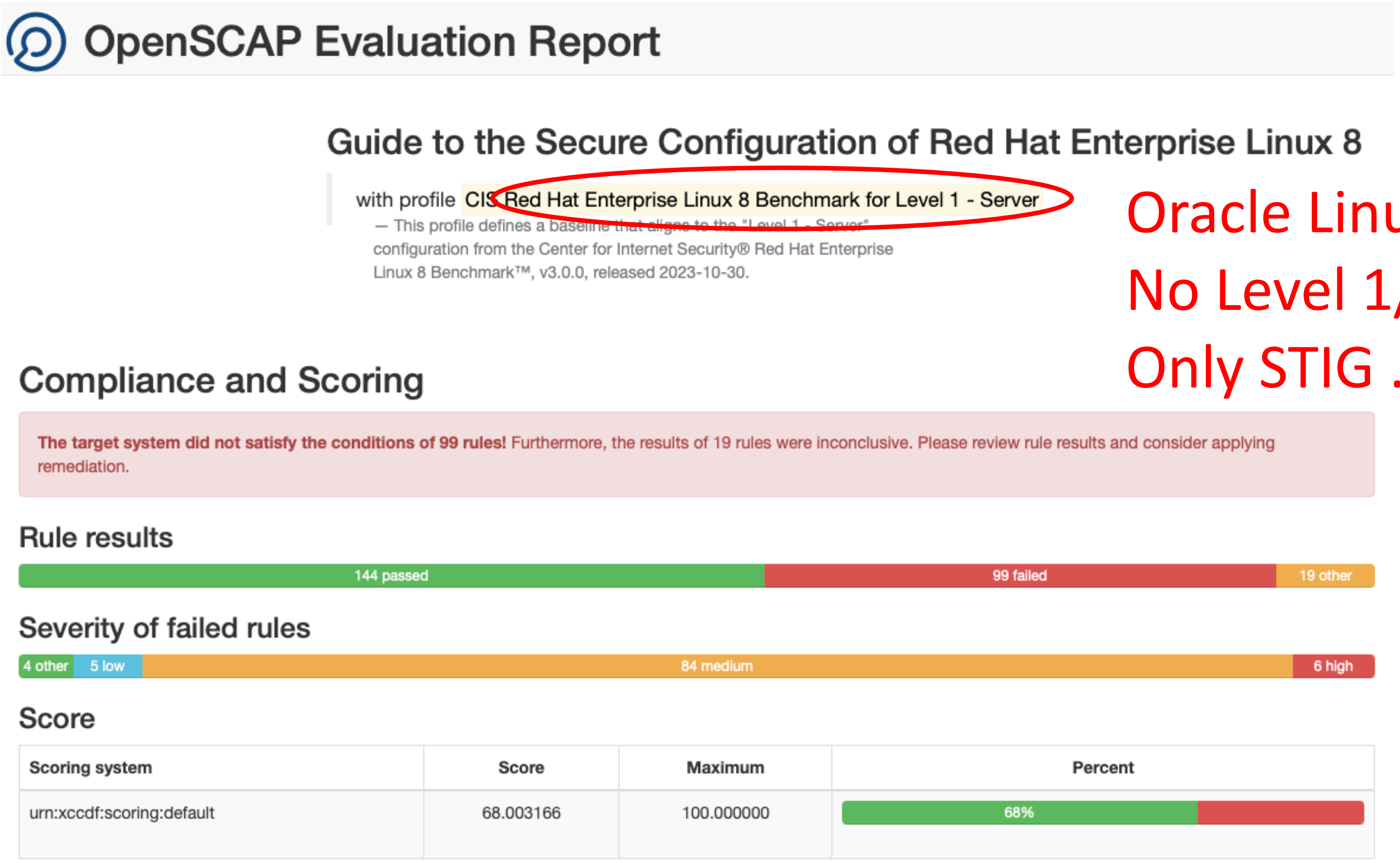
https://docs.oracle.com/en/operating-systems/oracle-linux/8/oscap/

Create the report:

```
oscap xccdf eval
--fetch-remote-resources
--datastream-id
     scap_org.open-scap_datastream_from_xccdf_ssg-rhel8-xccdf.xml
--xccdf-id scap_org.open-scap_cref_ssg-rhel8-xccdf.xml
--profile xccdf_org.ssgproject.content_profile_cis_server_l1
--report report-level1.html
     scap-security-guide-0.1.73/ssg-rhel8-ds-1.2.xml
```

Data Stream File

OpenSCAP



# OpenSCAP Evaluation Report

## Guide to the Secure Configuration of Red Hat Enterprise Linux 8

> with profile CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Server
>
> — This profile defines a baseline that aligns to the "Level 1 - Server" configuration from the Center for Internet Security® Red Hat Enterprise Linux 8 Benchmark™, v3.0.0, released 2023-10-30.

## Compliance and Scoring

**The target system did not satisfy the conditions of 99 rules!** Furthermore, the results of 19 rules were inconclusive. Please review rule results and consider applying remediation.

### Rule results

144 passed | 99 failed | 19 other

### Severity of failed rules

4 other | 5 low | 84 medium | 6 high

### Score

| Scoring system | Score | Maximum | Percent |
|---|---|---|---|
| urn:xccdf:scoring:default | 68.003166 | 100.000000 | 68% |

Oracle Linux 8

No Level 1/2

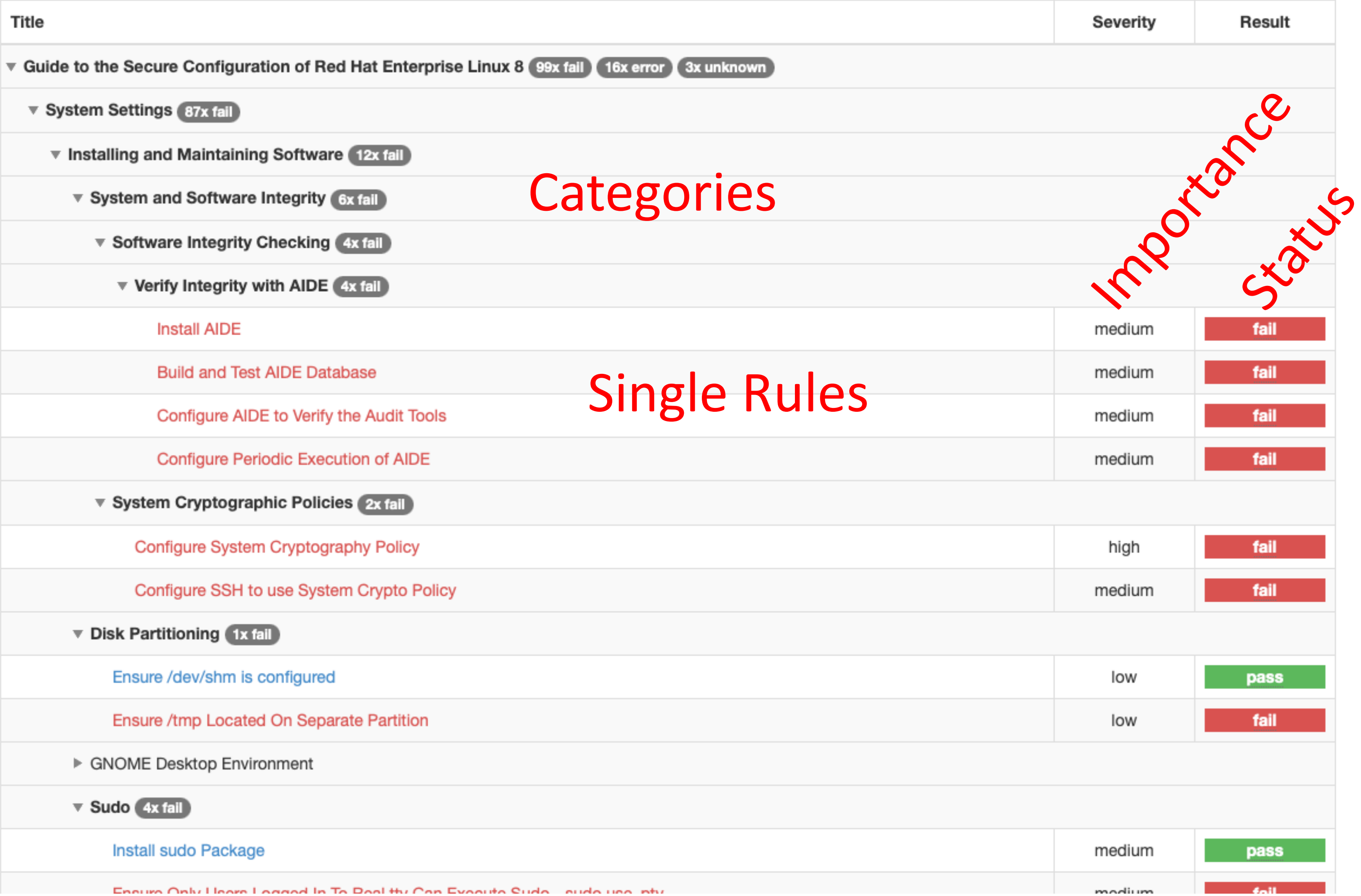
Only STIG ... ☹

Security
Content
Automation
Protocol

OpenSCAP

MATERIALFLUSSGRUPPE

performing databases



| Title | Severity | Result |
|---|---|---|
| ▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 8 99x fail 16x error 3x unknown | | |
| ▼ System Settings 87x fail | | |
| ▼ Installing and Maintaining Software 12x fail | | |
| ▼ System and Software Integrity 6x fail | | |
| ▼ Software Integrity Checking 4x fail | | |
| ▼ Verify Integrity with AIDE 4x fail | | |
| Install AIDE | medium | fail |
| Build and Test AIDE Database | medium | fail |
| Configure AIDE to Verify the Audit Tools | medium | fail |
| Configure Periodic Execution of AIDE | medium | fail |
| ▼ System Cryptographic Policies 2x fail | | |
| Configure System Cryptography Policy | high | fail |
| Configure SSH to use System Crypto Policy | medium | fail |
| ▼ Disk Partitioning 1x fail | | |
| Ensure /dev/shm is configured | low | pass |
| Ensure /tmp Located On Separate Partition | low | fail |
| ▶ GNOME Desktop Environment | | |
| ▼ Sudo 4x fail | | |
| Install sudo Package | medium | pass |
| Ensure Only Users Logged In To Real tty Can Execute Sudo - sudo use_pty | medium | fail |

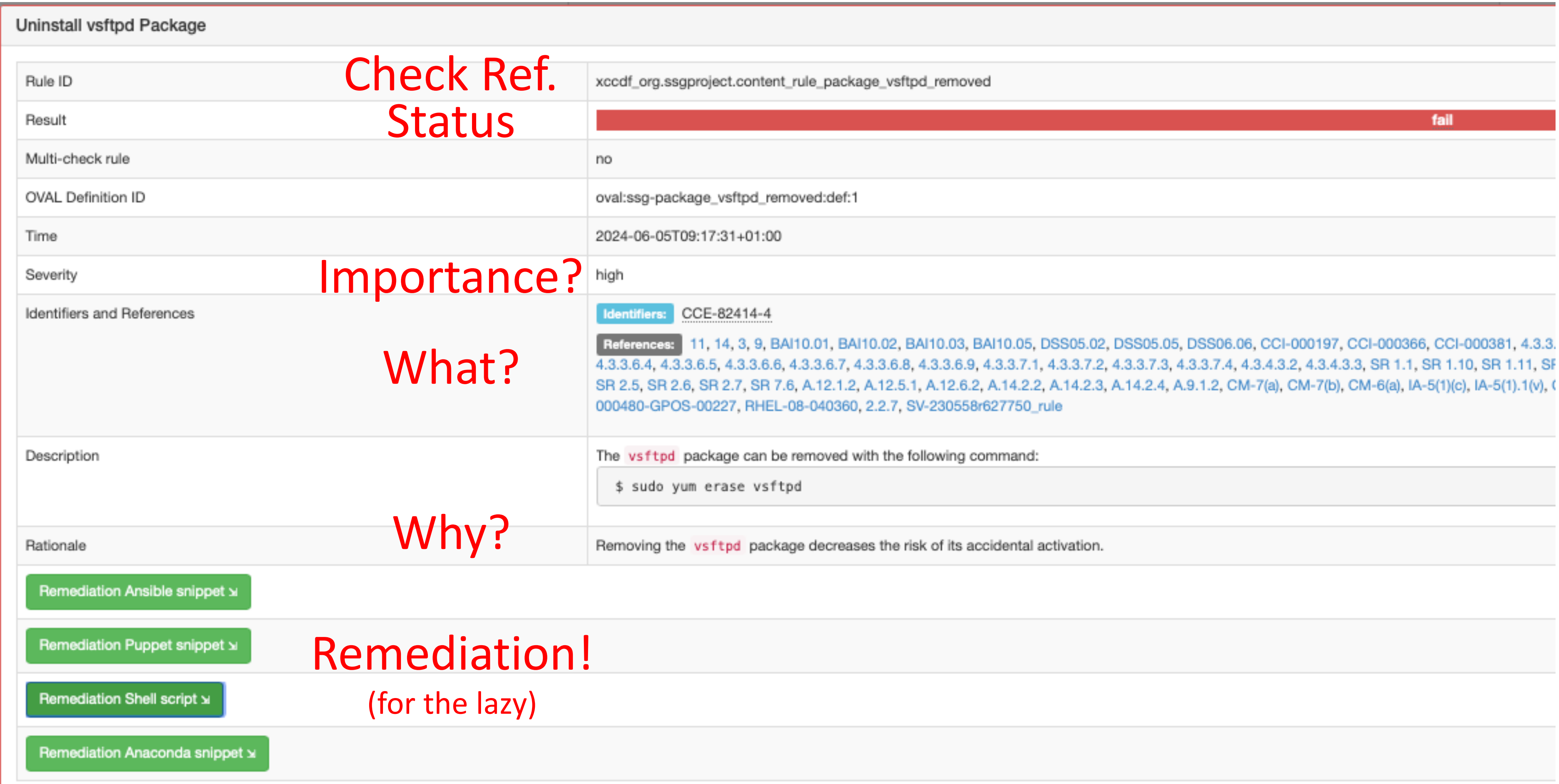
Categories

Single Rules

Importance

Status

# Detail: System Settings vs. Rules



### Uninstall vsftpd Package

| | |
|---|---|
| Rule ID | xccdf_org.ssgproject.content_rule_package_vsftpd_removed |
| Result | fail |
| Multi-check rule | no |
| OVAL Definition ID | oval:ssg-package_vsftpd_removed:def:1 |
| Time | 2024-06-05T09:17:31+01:00 |
| Severity | high |
| Identifiers and References | Identifiers: CCE-82414-4<br>References: 11, 14, 3, 9, BAI10.01, BAI10.02, BAI10.03, BAI10.05, DSS05.02, DSS05.05, DSS06.06, CCI-000197, CCI-000366, CCI-000381, 4.3.3. 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4, 4.3.4.3.2, 4.3.4.3.3, SR 1.1, SR 1.10, SR 1.11, SF SR 2.5, SR 2.6, SR 2.7, SR 7.6, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.9.1.2, CM-7(a), CM-7(b), CM-6(a), IA-5(1)(c), IA-5(1).1(v), ( 000480-GPOS-00227, RHEL-08-040360, 2.2.7, SV-230558r627750_rule |
| Description | The `vsftpd` package can be removed with the following command:<br>`$ sudo yum erase vsftpd` |
| Rationale | Removing the `vsftpd` package decreases the risk of its accidental activation. |

Remediation Ansible snippet
Remediation Puppet snippet
Remediation Shell script
Remediation Anaconda snippet

Check Ref.

Status

Importance?

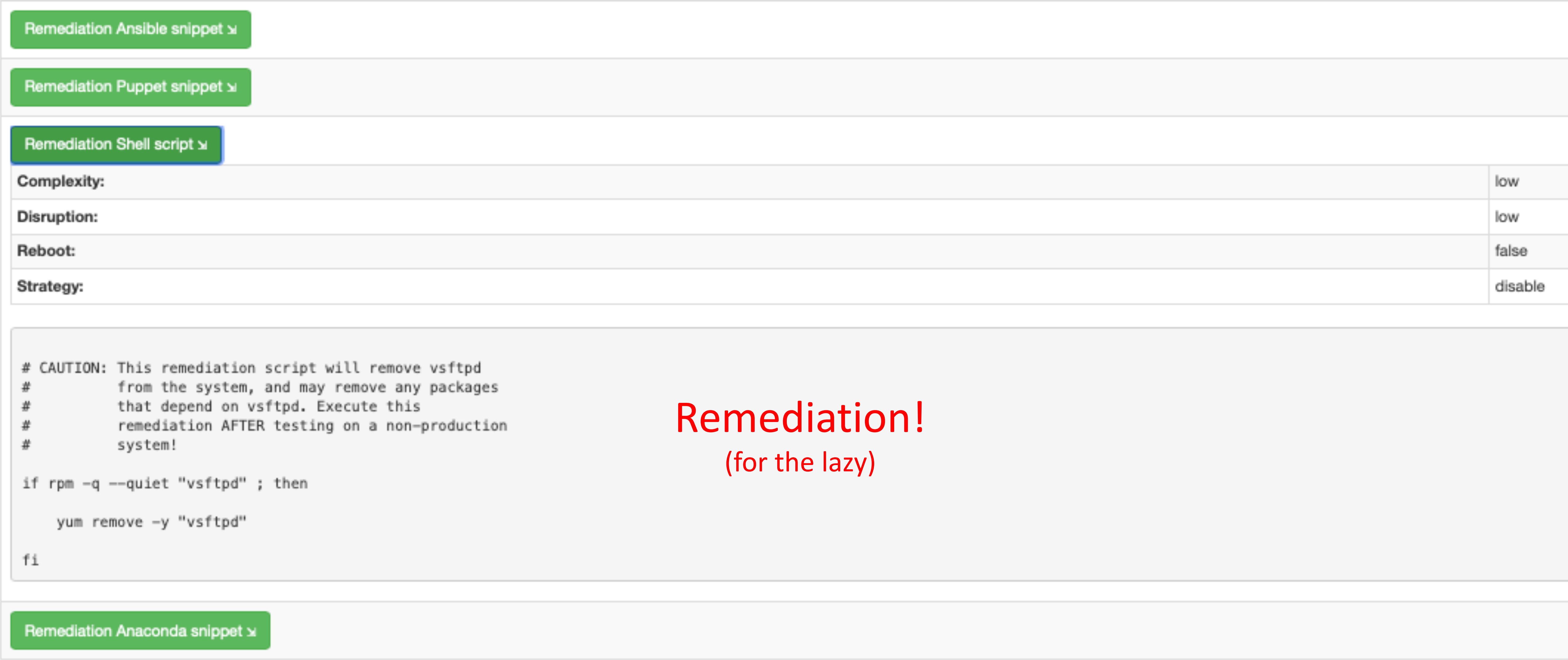
What?

Why?

Remediation!

(for the lazy)

# Suggested Remediation Scripts


Remediation Ansible snippet ↘
Remediation Puppet snippet ↘
Remediation Shell script ↘
Remediation Anaconda snippet ↘

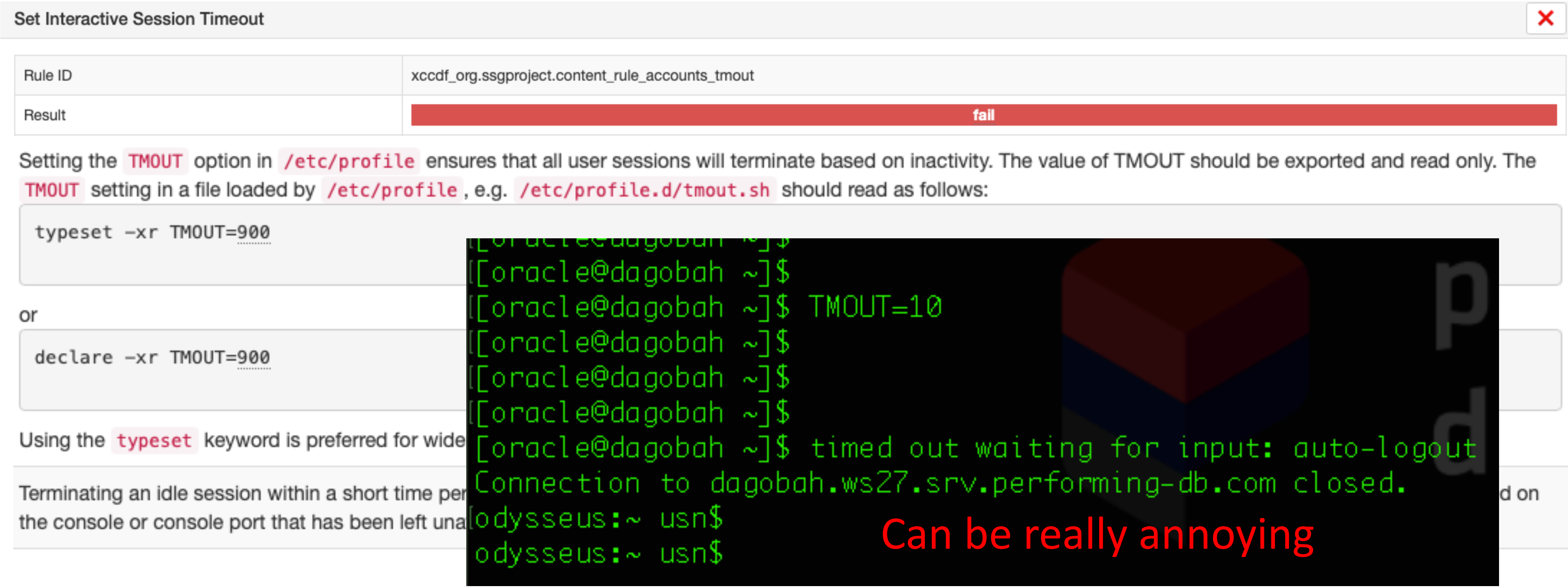
| | |
|---|---|
| **Complexity:** | low |
| **Disruption:** | low |
| **Reboot:** | false |
| **Strategy:** | disable |

```
# CAUTION: This remediation script will remove vsftpd
#          from the system, and may remove any packages
#          that depend on vsftpd. Execute this
#          remediation AFTER testing on a non-production
#          system!

if rpm -q --quiet "vsftpd" ; then

    yum remove -y "vsftpd"

fi
```

Remediation!

(for the lazy)

# Remediation ”Session Timeout”



Set Interactive Session Timeout

| | |
|---|---|
| Rule ID | xccdf_org.ssgproject.content_rule_accounts_tmout |
| Result | fail |

Setting the `TMOUT` option in `/etc/profile` ensures that all user sessions will terminate based on inactivity. The value of TMOUT should be exported and read only. The `TMOUT` setting in a file loaded by `/etc/profile`, e.g. `/etc/profile.d/tmout.sh` should read as follows:

```
typeset -xr TMOUT=900
```

or

```
declare -xr TMOUT=900
```

Using the `typeset` keyword is preferred for wide

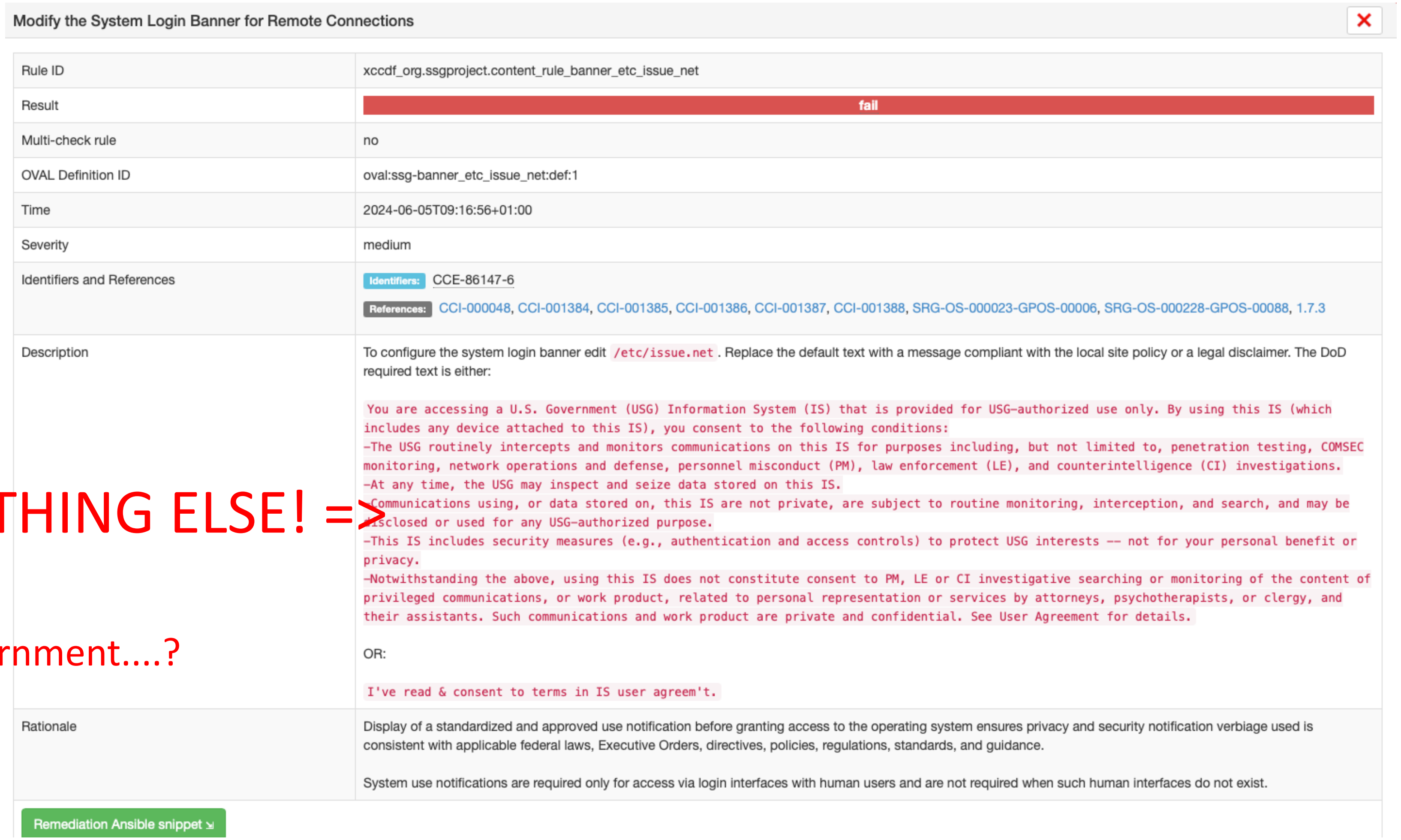
Terminating an idle session within a short time per … d on the console or console port that has been left una

```
[oracle@dagobah ~]$
[oracle@dagobah ~]$
[oracle@dagobah ~]$ TMOUT=10
[oracle@dagobah ~]$
[oracle@dagobah ~]$
[oracle@dagobah ~]$
[oracle@dagobah ~]$ timed out waiting for input: auto-logout
Connection to dagobah.ws27.srv.performing-db.com closed.
odysseus:~ usn$
odysseus:~ usn$
```

Can be really annoying

# Strange and Funny Things

“Modify the System Login Banner for Remote Connections”



Modify the System Login Banner for Remote Connections

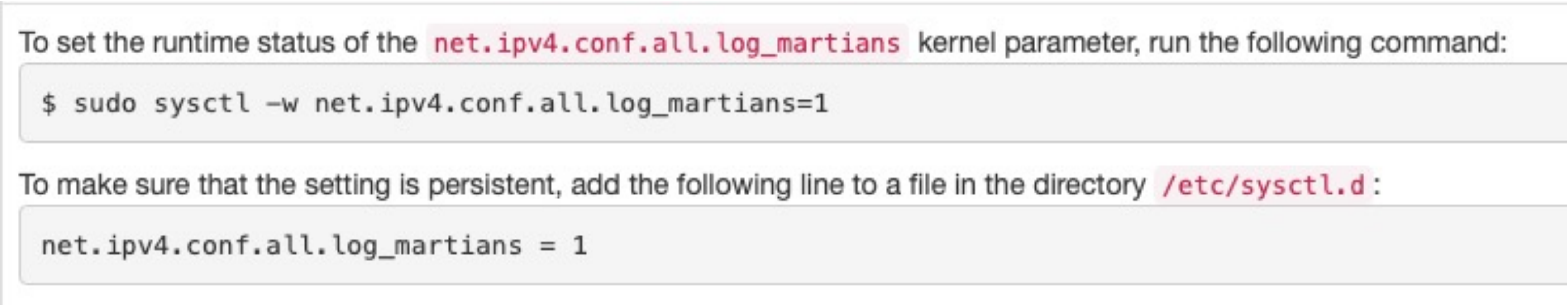
| | |
|---|---|
| Rule ID | xccdf_org.ssgproject.content_rule_banner_etc_issue_net |
| Result | fail |
| Multi-check rule | no |
| OVAL Definition ID | oval:ssg-banner_etc_issue_net:def:1 |
| Time | 2024-06-05T09:16:56+01:00 |
| Severity | medium |
| Identifiers and References | Identifiers: CCE-86147-6<br>References: CCI-000048, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388, SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088, 1.7.3 |
| Description | To configure the system login banner edit `/etc/issue.net`. Replace the default text with a message compliant with the local site policy or a legal disclaimer. The DoD required text is either:<br>`You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:`<br>`-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.`<br>`-At any time, the USG may inspect and seize data stored on this IS.`<br>`-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.`<br>`-This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for your personal benefit or privacy.`<br>`-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.`<br>OR:<br>`I've read & consent to terms in IS user agreem't.` |
| Rationale | Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.<br>System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist. |

THIS and NOTHING ELSE! =>

We are not US Government....?

# Strange and Funny Things

“Enable Kernel Parameter to **Log Martian Packets** on all IPv4 Interfaces”



To set the runtime status of the `net.ipv4.conf.all.log_martians` kernel parameter, run the following command:

```
$ sudo sysctl -w net.ipv4.conf.all.log_martians=1
```

To make sure that the setting is persistent, add the following line to a file in the directory `/etc/sysctl.d`:

```
net.ipv4.conf.all.log_martians = 1
```

WTH is this, and what’s the impact on my operations?

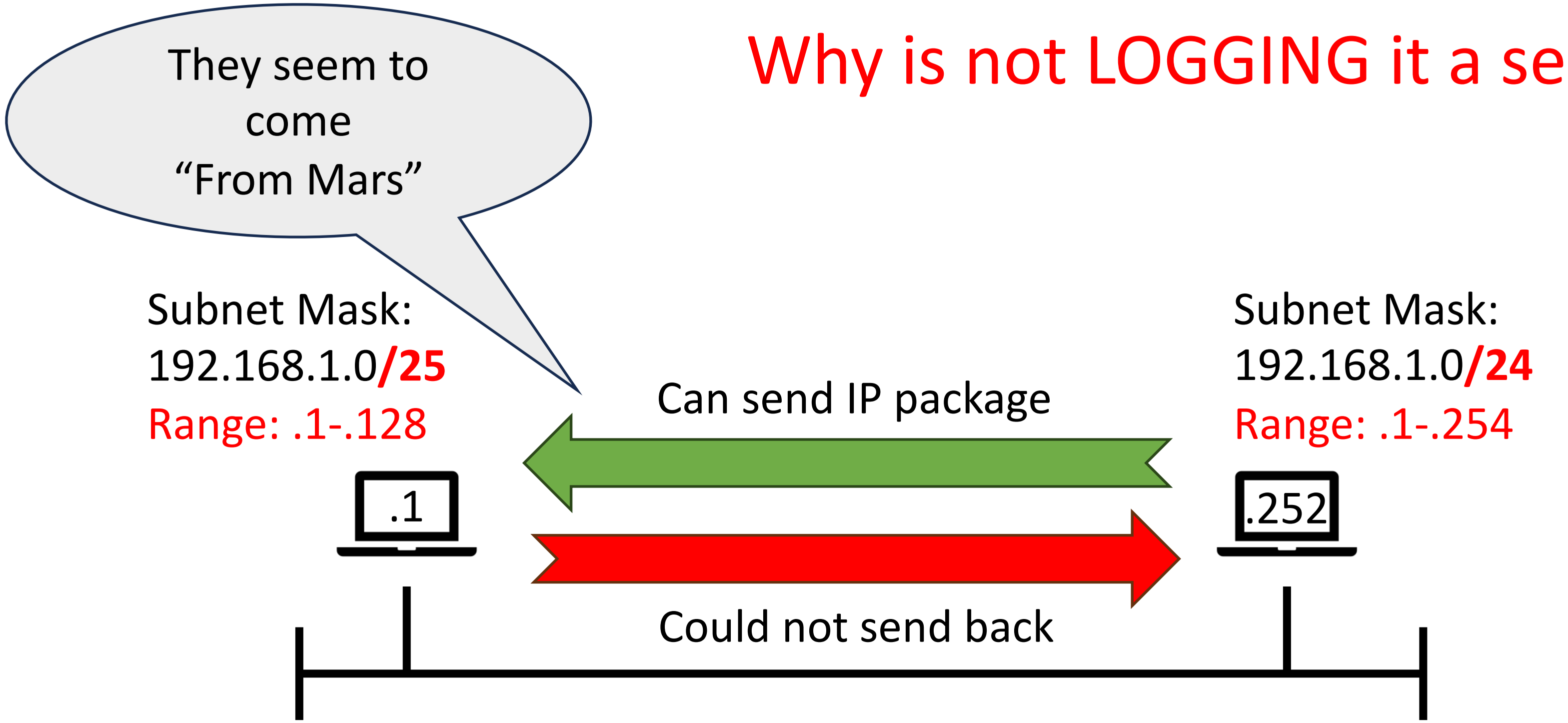
Aliens, congregate!

# Strange and Funny Things

“Enable Kernel Parameter to **Log Martian Packets** on all IPv4 Interfaces”

WTH is this, and what’s the impact on my operations?

Why is not LOGGING it a security issue?



They seem to come “From Mars”

Subnet Mask:
192.168.1.0/**25**
Range: .1-.128

Subnet Mask:
192.168.1.0/**24**
Range: .1-.254

Can send IP package

Could not send back

# SELinux
# Security Enhanced Linux

- Mandatory Access-Control (MAC) on resources
- De-facto additional Security “Layer”
- Required for CIS Level 1(++)
- Makes Oracle (RAC) setup fail, big time!

# Oracle DBSAT
# Database Security Assessment Tool

V.3.1.0 covers CIS, STIG and Oracle Best Practices (e.g. for GDPR etc.)

MOS DOC ID 2138254.1

Default config in **discover.conf** is quite simple:

DB_HOSTNAME
DB_PORT
DB_SERVICENAME
SCHEMA_SCOPE
EXCLUSION_LIST_FILE

Run it w/o SYS privileges – you need GRANTs:

CREATE SESSION
SELECT_CATALOG_ROLE
SELECT ON sys.registry$history
READ ON sys.dba_audit_mgmt_config_params
SELECT ON sys.dba_users_with_defpwd
READ ON sys.dba_credentials
EXECUTE ON sys.dbms_sql
AUDIT_VIEWER
CAPTURE_ADMIN

# Oracle DBSAT
# Database Security Assessment Tool

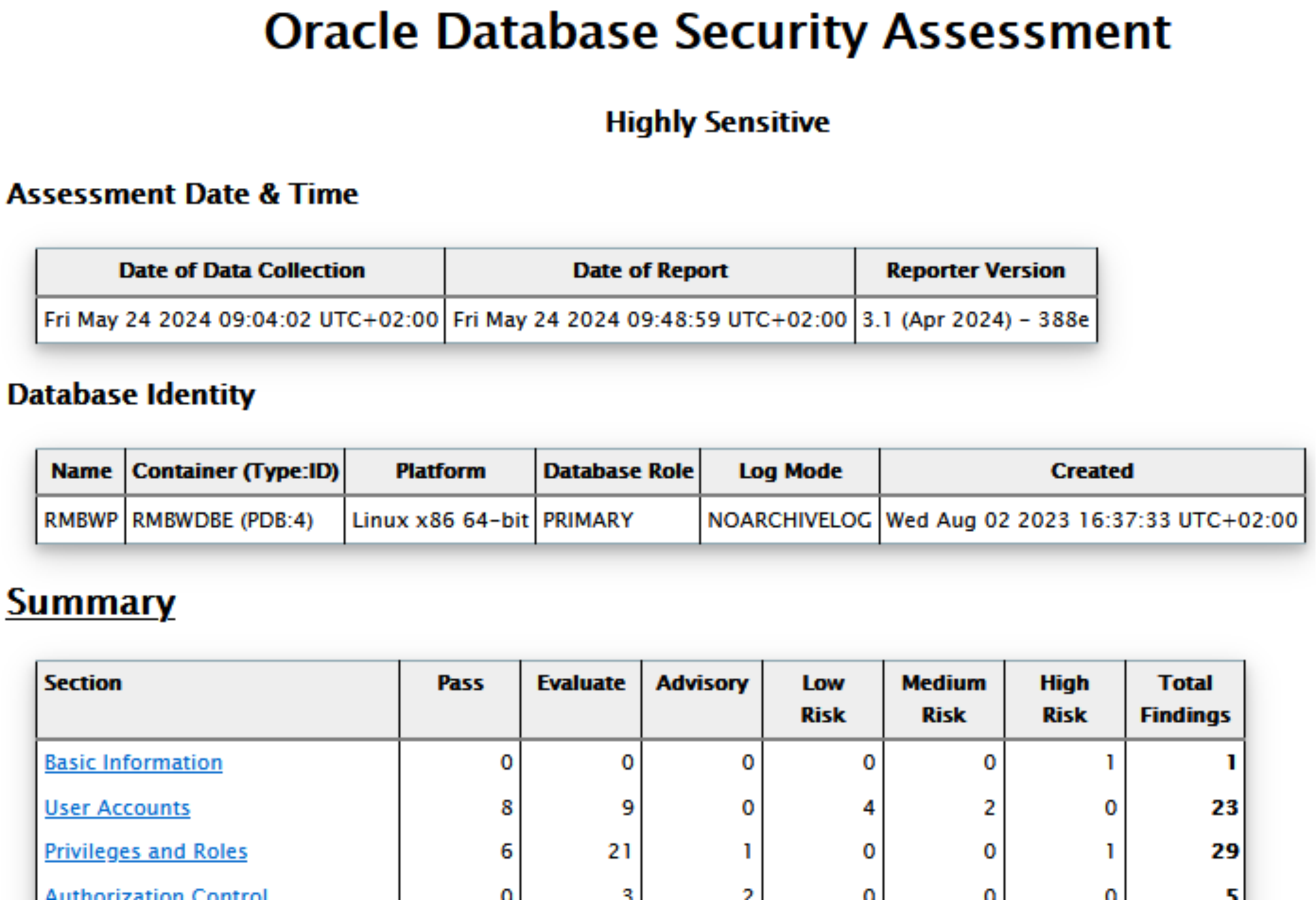
## Syntax

```
-- dbsat COLLECTOR
./dbsat collect bss_db_sat/secret@10.1.2.3:1521/MYDB dbsat.out
```

```
-- dbsat REPORTER
ZIP=/usr/bin/zip
UNZIP=/usr/bin/unzip
DBZIP=${ORACLE_HOME}/bin/zip

./dbsat report dbsat.out
```

# Oracle DBSAT
# Database Security Assessment Tool

Security Report:



## Oracle Database Security Assessment

**Highly Sensitive**

### Assessment Date & Time

| Date of Data Collection | Date of Report | Reporter Version |
|---|---|---|
| Fri May 24 2024 09:04:02 UTC+02:00 | Fri May 24 2024 09:48:59 UTC+02:00 | 3.1 (Apr 2024) - 388e |

### Database Identity

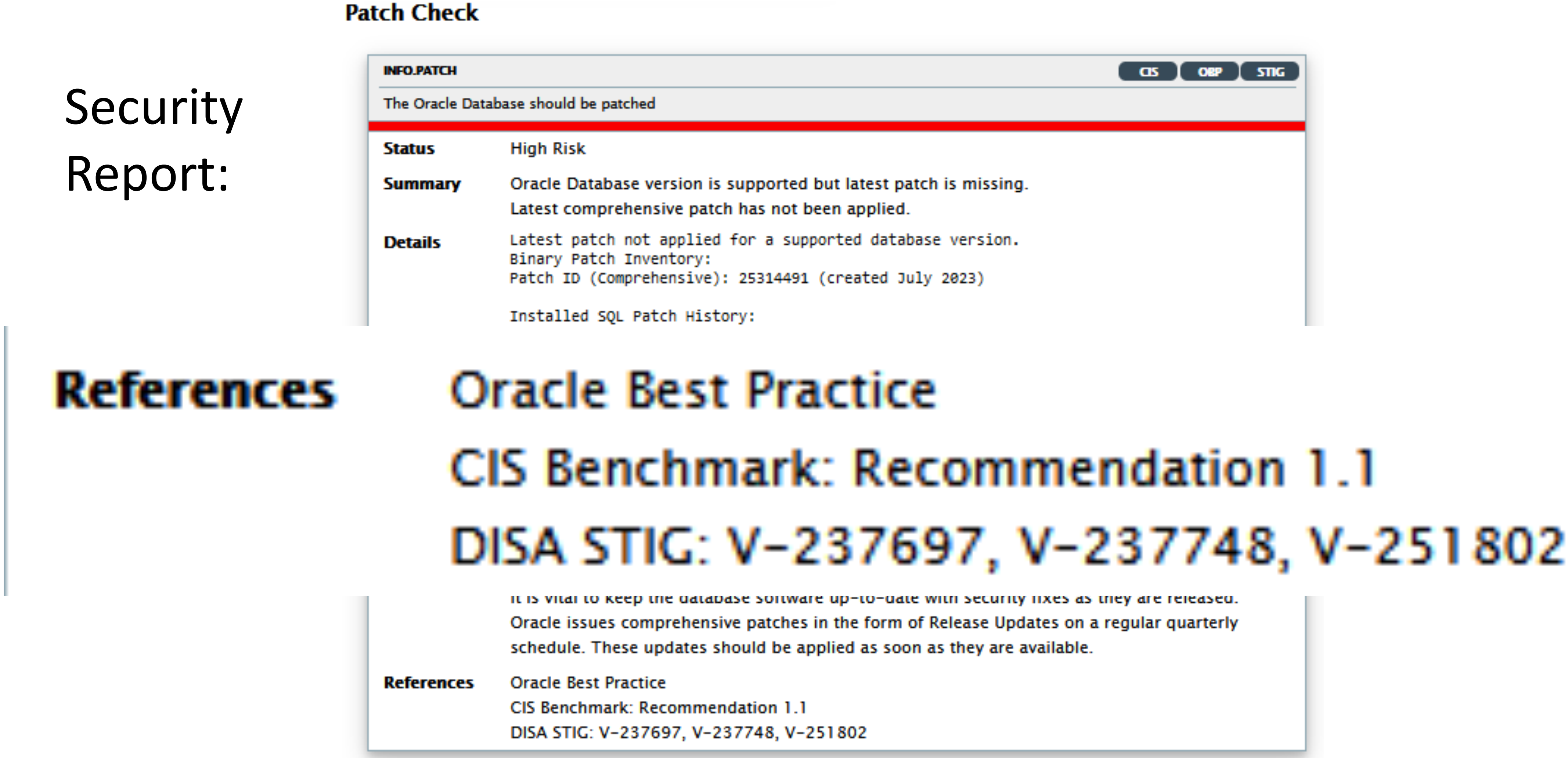
| Name | Container (Type:ID) | Platform | Database Role | Log Mode | Created |
|---|---|---|---|---|---|
| RMBWP | RMBWDBE (PDB:4) | Linux x86 64-bit | PRIMARY | NOARCHIVELOG | Wed Aug 02 2023 16:37:33 UTC+02:00 |

### Summary

| Section | Pass | Evaluate | Advisory | Low Risk | Medium Risk | High Risk | Total Findings |
|---|---|---|---|---|---|---|---|
| Basic Information | 0 | 0 | 0 | 0 | 0 | 1 | **1** |
| User Accounts | 8 | 9 | 0 | 4 | 2 | 0 | **23** |
| Privileges and Roles | 6 | 21 | 1 | 0 | 0 | 1 | **29** |
| Authorization Control | 0 | 3 | 2 | 0 | 0 | 0 | **5** |

# Oracle DBSAT
# Database Security Assessment Tool

Security Report:



**Patch Check**

**INFO.PATCH**

The Oracle Database should be patched

| | |
|---|---|
| **Status** | High Risk |
| **Summary** | Oracle Database version is supported but latest patch is missing.<br>Latest comprehensive patch has not been applied. |

**Details**

```
Latest patch not applied for a supported database version.
Binary Patch Inventory:
Patch ID (Comprehensive): 25314491 (created July 2023)

Installed SQL Patch History:
```

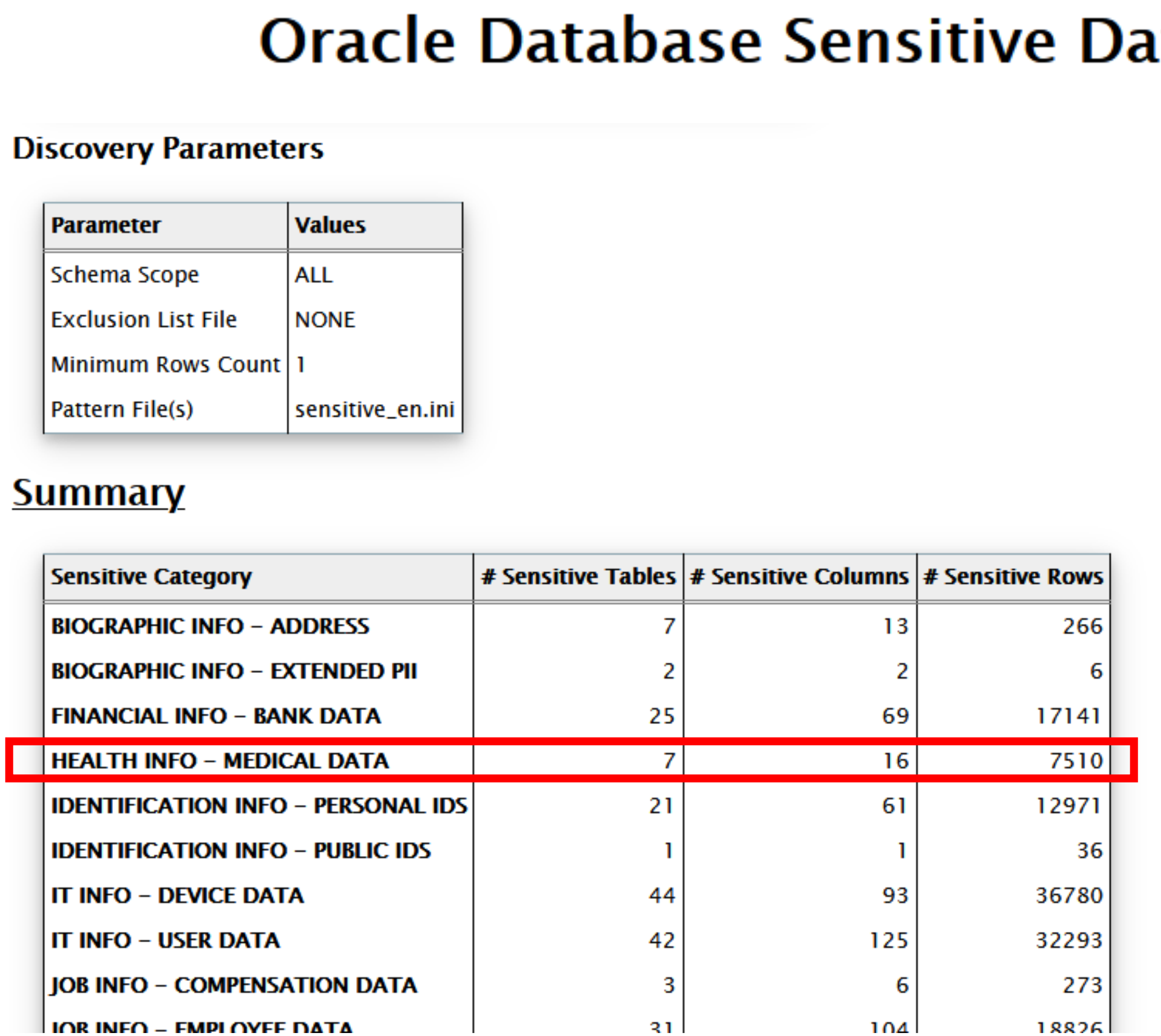
**References** Oracle Best Practice
CIS Benchmark: Recommendation 1.1
DISA STIG: V-237697, V-237748, V-251802

It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates on a regular quarterly schedule. These updates should be applied as soon as they are available.

**References** Oracle Best Practice
CIS Benchmark: Recommendation 1.1
DISA STIG: V-237697, V-237748, V-251802

# Oracle DBSAT
# Database Security Assessment Tool

Sensitive Data Report:



## Oracle Database Sensitive Data Assessment

### Discovery Parameters

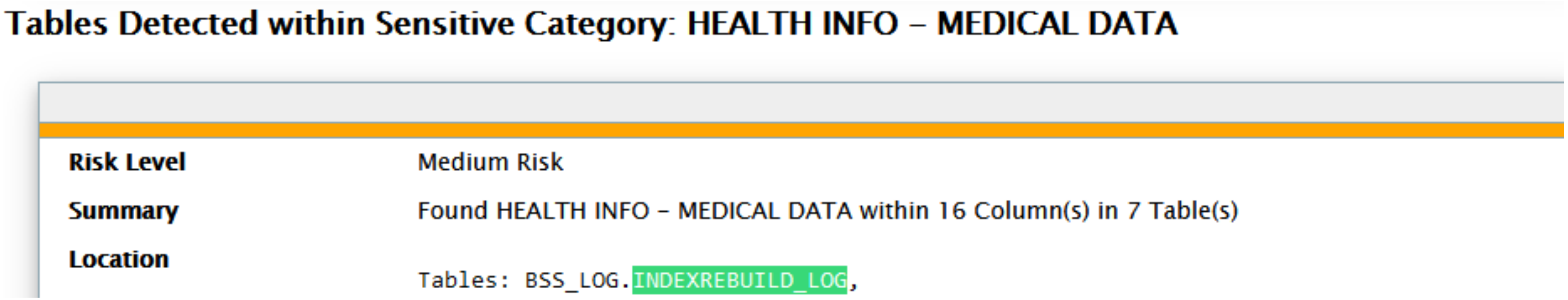
| Parameter | Values |
|---|---|
| Schema Scope | ALL |
| Exclusion List File | NONE |
| Minimum Rows Count | 1 |
| Pattern File(s) | sensitive_en.ini |

### Summary

| Sensitive Category | # Sensitive Tables | # Sensitive Columns | # Sensitive Rows |
|---|---|---|---|
| BIOGRAPHIC INFO – ADDRESS | 7 | 13 | 266 |
| BIOGRAPHIC INFO – EXTENDED PII | 2 | 2 | 6 |
| FINANCIAL INFO – BANK DATA | 25 | 69 | 17141 |
| HEALTH INFO – MEDICAL DATA | 7 | 16 | 7510 |
| IDENTIFICATION INFO – PERSONAL IDS | 21 | 61 | 12971 |
| IDENTIFICATION INFO – PUBLIC IDS | 1 | 1 | 36 |
| IT INFO – DEVICE DATA | 44 | 93 | 36780 |
| IT INFO – USER DATA | 42 | 125 | 32293 |
| JOB INFO – COMPENSATION DATA | 3 | 6 | 273 |
| JOB INFO – EMPLOYEE DATA | 31 | 104 | 18826 |

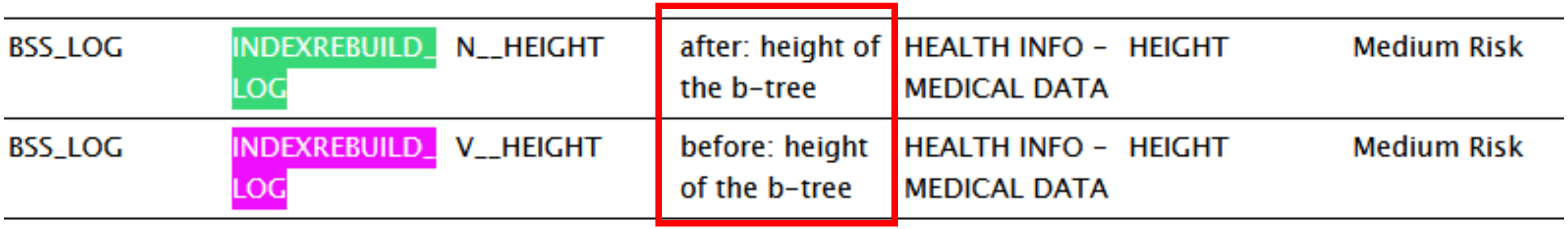
# Oracle DBSAT
# Database Security Assessment Tool

Sensitive Data Report:



Tables Detected within Sensitive Category: HEALTH INFO – MEDICAL DATA

| | |
|---|---|
| **Risk Level** | Medium Risk |
| **Summary** | Found HEALTH INFO – MEDICAL DATA within 16 Column(s) in 7 Table(s) |
| **Location** | `Tables: BSS_LOG.INDEXREBUILD_LOG,` |



| | | | | | | |
|---|---|---|---|---|---|---|
| BSS_LOG | INDEXREBUILD_LOG | N__HEIGHT | after: height of the b-tree | HEALTH INFO – MEDICAL DATA | HEIGHT | Medium Risk |
| BSS_LOG | INDEXREBUILD_LOG | V__HEIGHT | before: height of the b-tree | HEALTH INFO – MEDICAL DATA | HEIGHT | Medium Risk |

Fine-tune **discover.conf** and **sensitive_en.ini** for more sanity ☺

# Lessons Learned

# Two Ways to Hardening

- From Scratch (Security is a Feature, Security by Design)
- By Change (Never Change ...., Security by Option)

# Hardening from Scratch - Security by Design

- Needs to be planned
  - Product budget
  - Collisions w/ other features

- Maximum Principle
  - As much as possible
  - (Hopefully) no exceptions

# Hardening on Demand - Security by Option

- Pops up at a random time
  - Project budget = Customizing
  - Collisions w/ tested features
    AND project timelines

- Minimum Principle
  - As little as possible, just pass the benchmark
  - Exceptions are necessary

# Security …

| | KnowHow | Time & Money | Testing |
|---|---|---|---|
| by Design | Know, how to do it<br>“the right way” | Product phase<br>slower/expensive | Modular by<br>development progress |
| on Demand | Know a grown product<br>and its “hacks” very well | Do (much of) it again<br>in every project<br>“F.I.A.T.” | Monolithic<br>Test everything at once |

# Hardening Lessons Learned

- WTH are TCP SYNCookies ?
  You will forget special knowledge soon!
- You get off track quickly
  Deep dives into nothing ...
- Hardening makes maintenance complicated

# More Hardening Lessons Learned

- Report is “Green” – but it’s just a snapshot
  Maintain hardening continuously!

- Is “OK” for your tool also OK?
  OpenSCAP can be a bastard!

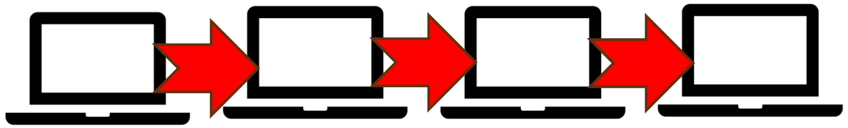
- Changes are quick.
  But Testing takes a lot of time (e.g. GRUB pw)

# Security Lessons Learned

- Part-time job? You need a Security Team!
  KnowHow, Priorities, Budget ...

- Hard to argument costs & efforts
  (Expensive insurance and never sick)

- Jumphost Chain from Hell



# What’s next?

# To be continued ... XDR

CROWDSTRIKE

Yes, we heard of Oracle (RAC) ...

ORACLE

Yes, we heard of Crowdstrike Falcon ....

# THANK YOU VERY MUCH!

martin.klier@performing-db.com
axel.vomstein@bss.gmbh