

**Horizon 2020 Marie Skłodowska-Curie**

**Research and Innovation Staff Exchange Evaluations (RISE)**



**A CybEr range tRaining platform for medicAl organisations and systems Security**

**D4.4: AERAS Monitoring, Assessment and Adaptation mechanisms – V2** [[1]](#footnote-2)†

**Abstract**: This deliverable constitutes the final output of Task 4.2 and apply the Evaluation and Adaptation methodology described in D4.2, evaluating its effectiveness and feasibility in a real pilot environment.

|  |  |
| --- | --- |
| Contractual Date of Delivery | 15/07/2025 |
| Actual Date of Delivery | 15/07/2025 |
| Deliverable Security Class | Public |
| Editor | Fulvio Frati (UMIL) |
| Contributors | Theodoros Christophides, Kostas Iordanou, Ioannis Panagiotou (CUT)  Nastasia Michael, Panagiotis Archontidis (LIBRA)  Esftratios Syrmas, Ioanna Stamouli (UPAT)  Dimitrios Dounas, Nikolas Ioannou, Konstantinos Papadamou (TRID)  Fulvio Frati (UMIL) |
| Quality Assurance | Evangelos Floros (PAGNI)  Kostantinos Panousis (EAIN) |

The *AERAS* Consortium

|  |  |  |
| --- | --- | --- |
| Universita degli Studi di Milano | UMIL | Italy |
| Technologiko Panepistimio Kyprou | CUT | Cyprus |
| Sphynx Analytics LTD | STS-CY | Cyprus |
| AEGIS IT RESEARCH GMBH | AEGIS | Germany |
| Panepistimiako Geniko Nosokomeio Irakleiou | PAGNI | Greece |
| Panepistimio Patron | UPAT | Greece |
| Trinomial Technologies LTD | TRID | Cyprus |
| Ethical AI Novelties | EAIN | Cyprus |
| Libra AI Technologies | LIBRA | Greece |

*Document Revisions & Quality Assurance*

**Internal Reviewers**

1. *Evangelos Floros (PAGNI)*
2. *Kostantinos Panousis (EAIN)*

**Revisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **By** | **Overview** |
| 1.0 | 10/06/2025 | Editor | Final version |
| 0.7 | 31/05/2025 | Editor | Deliverable ready for internal review |
| 0.3 | 15/05/2025 | Editor | Execution of second round of tests |
| 0.2 | 15/03/2025 | Editor | Organization of RiskRate analysis and first round of tests |
| 0.1 | 15/02/2025 | Editor | First Draft of the table of contents |

*Executive Summary*

Deliverable 4.4 constitutes the final output of Task 4.2 and describes the application of the RiskRate procedure, described in the Evaluation and Adaptation methodology, stated in D4.2 and that involves most of the procedures of AERAS, to a pilot’s environments.

The scope of the deliverable is to evaluate the feasibility and the effectiveness of the methodology, and put forward our idea of an integrated and holistic approach to risk evaluation.

D4.4 will be released as a concrete update of D4.2, highlighting the new parts where the work has focused in the last months of secondments.

*Table of Contents*

[1. Introduction 8](#_Toc199580126)

[1.2 Role of the Deliverable 9](#_Toc199580127)

[1.3 Relationship to other Deliverables 9](#_Toc199580128)

[1.4 Structure of the document 9](#_Toc199580129)

[2. Evaluation and Adaptation Checklist 10](#_Toc199580130)

[2.2 Phase 1: Pre-Training Phase 12](#_Toc199580131)

[2.2.1 Task 1.1: Pre-training security and risk evaluation (tool) 12](#_Toc199580136)

[2.2.2 Task 1.2: Training needs analysis (procedure) 15](#_Toc199580137)

[2.3 Phase 2: Models Population 16](#_Toc199580138)

[2.3.1 Task 2.1: CRSA Models population (procedure) 16](#_Toc199580140)

[2.3.2 Task 2.2: CRST Models population (procedure) 17](#_Toc199580141)

[2.4 Phase 3: Training 17](#_Toc199580142)

[2.4.1 Task 3.1: Real-time assessment of trainee performances (tool) 17](#_Toc199580144)

[2.5 Phase 4: Post-Training 18](#_Toc199580145)

[2.5.1 Task 4.1: Post-training security and risk evaluation (tool) 19](#_Toc199580147)

[2.5.2 Task 4.2: Production of aggregate data on trainees' activities 19](#_Toc199580148)

[2.6 Phase 5: Evaluation & Adaptation 20](#_Toc199580149)

[2.6.1 Task 5.1: Pre- and Post-training security and risk comparison (tool) 21](#_Toc199580151)

[2.6.2 Task 5.2: Adaptation Analysis of training activities 22](#_Toc199580152)

[2.6.3 Task 5.3: Alerts on training adaptation needs 23](#_Toc199580153)

[3. Application of the Cybersecurity Risk Methodology 25](#_Toc199580154)

[3.2 Preliminary Analysis 25](#_Toc199580155)

[3.3 Post-training Analysis 31](#_Toc199580156)

[3.4 Data comparison 35](#_Toc199580157)

[4. Evaluation and Adaptation 37](#_Toc199580158)

[5. Conclusions 38](#_Toc199580159)

[6. References 39](#_Toc199580160)

*List of Figures*

Figure 1: AERAS reference infrastructure. 8

Figure 2: AERAS Evaluation and Adaptation Checklist. 10

Figure 3: AERAS procedures implementing Task 1.1 12

Figure 4: CVSS metrics composition [5]. 13

Figure 5: Risk evaluation data flow. 14

Figure 6: Kolb's cycle stages of learning. 15

Figure 7: CRSA Submodels. 17

Figure 8: CRST Programme Generator module. 17

Figure 9: Performance Evaluator and Progression Engine. 18

Figure 10: Progression Engine expected communication flows. 18

Figure 11: Post-training risk evaluation flow. 19

Figure 12: Performance Evaluator tool data flow. 20

Figure 13: Training Performance Monitor tool. 21

Figure 14: : Training Performance Monitor expected communication flow. 22

Figure 15: Programme Adaptor tool. 22

Figure 16: Programme Adaptor expected communication flow. 23

*List of Tables*

Table 1: Detected vulnerabilities with CVSS score and Severity weight – Pre-Training. 25

Table 2: Detected vulnerabilities with CVSS score and Severity weight – Post-Training. 31

Table 3: RiskRate results comparison. 35

*Table of Abbreviations*

|  |  |
| --- | --- |
| **CRSA** | Cyber Range Security Assurance |
| **CRST** | Cyber Range Simulation and Training |
| **CSLA** | Cybersecurity Service Level Agreement |
| **CVSS** | Common Vulnerability Scoring System |
| **DDOS** | Distributed Denials-of-Service |
| **FSM** | Finite State Machine |
| **NIST** | National Institute of Standards and Technology |
| **NVD** | National Vulnerability Database |
| **NVT** | Network Vulnerability Test |
| **WP** | Work Package |
|  |  |

# Introduction

AERAS approach is fully equipped with tools and procedures to continuously assess adopting organizations’ cybersecurity landscape and related risk, and the effectiveness of the applied training activities. To do that, the project put in place a specific methodology to assess and adapt the training activities with respect to updated cybersecurity threads and vulnerabilities, and the intrinsic response of trainees to the activities themselves.

In fact, one of the main goal of the project is to instil in adopting organization an approach to training activities that not only fulfil common needs of improving the overall educational level of employees, but also to adapt it to the actual cybersecurity threats and needs, and to continuously assess it in function of the trainees’ response to training activities. The rationale behind it is that more the organization improve its cybersecurity landscape, the more effective the training programme has been for the organization itself.

The adaptation and evaluation methodology put forward in D4.2 and applied in this deliverable has been described as a five-step checklist. Each step is composed of tasks that drive the trainers and manager in the definition and execution of the procedure. The checklist is connected to most of the AERAS tools and procedures (Figure 1) and involves the whole lifecycle of the framework.

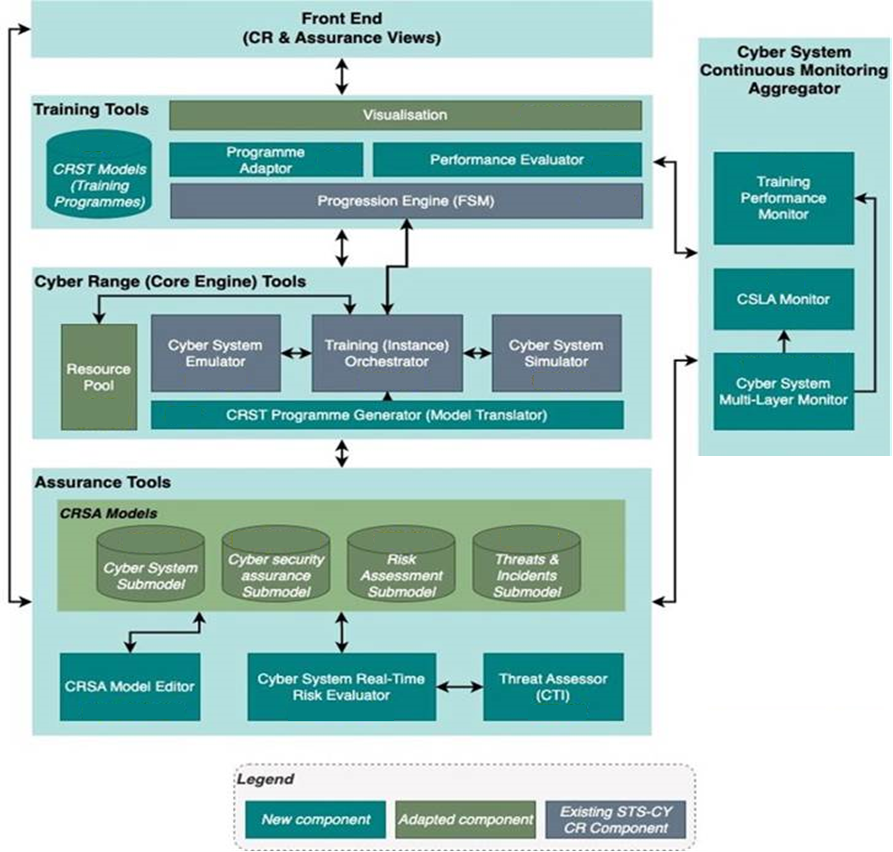


Figure 1: AERAS reference infrastructure.

## Role of the Deliverable

The role of this deliverable is to apply the methodology defined in D4.2, whose that document constitutes an update, in order to evaluate the adaptation and evaluation technique of the training programme provided within the AERAS framework.

As for D4.2, this deliverable is part of the overall Objective 3 for the aspect related to the monitoring and use of the feedback received from the various component of the framework.

**Objective 3:** *Develop mechanisms to support the adaptation of cyber range simulation and training programmes, via feedback received from multiple sources, including multi-layer system, trainee and programme performance monitoring, and CSLAs monitoring.*

This deliverable contributes also to Objective 2, that requires a mechanism for the continuous monitoring of the cyber systems and the trainees.

***Objective 2:*** *Develop novel hybrid cyber security risk analysis models, which combine traditional static cyber security risk analysis principles and standards with continuous risk estimates. These estimates are informed from simulation and the continuous real-time multi-layer monitoring of cyber-systems and trainees.*

## Relationship to other Deliverables

The Deliverable 4.4 is an update of the D4.2 is strictly related with the deliverables that are part of WP4 and WP3.

In particular, the connection with WP4 deliverables is strict in term of description of the tools and modules that compose the cyber range infrastructure and that are included in the Phase 3 of the checklist described in Section 5.

With respect to WP3, D3.2 and D3.3 are connected with the current deliverable in the work related, in particular, with Phase 2, where the CRSA and CRST models are populated, and Phase 1, where the data will be collected.

## Structure of the document

The deliverable is structured as follows.

Section 2 provides a short description of the Evaluation and Adaptation checklist, presented in D4.2, that drives the trainers and managers in the preparation and execution of the methodology.

Section 3 describes the application of the RiskRate methodology, part of the Evaluation Checklist, to a real-case scenario, discussing the results and the findings. Then, in Section 4 we depict how the RiskRate analysis can be beneficial to the adaptation of training activities.

Finally, Section 8 draws our conclusions.

# Evaluation and Adaptation Checklist

In this section we recall the Evaluation and Adaptation checklist first described in D4.2. The checklist is an integrated iterative process that involves several phases, starting from a pre-training preparation phase to the evaluation of results and adaptation of training activities and models.

Each task is supported by a specific AERAS tool or procedure, driving the trainers in the process. The schema in Figure 2, describing a checklist for the evaluation and adaptation techniques, can be considered strictly connected to WP3 “AERAS Models & Model-driven Cyber Range programmes creation” activities, since it considers the methodologies for the population of models.

The importance of the continuous monitoring and adaptation of training process to trainees results and performances has been explored in many seminal works [1] [2]. NIST, in the “Role-Based Model for Federal Information Technology/Cybersecurity Training” document [3], highlighted the importance of an evaluation process to develop information technology/cybersecurity role-based training. The primary focus of this process is to provide a comprehensive and flexible training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology/cybersecurity responsibilities.

In the following, we are going to provide a short introduction of the five phases, that will be examined in the next sections, proposing for each task the specific AERAS tool or methodology of reference and the way the task will be tackled following our approach.

Figure 2: AERAS Evaluation and Adaptation Checklist.

The five phases can be described as follows.

***Phase 1 (Pre-training)*** *include* a first analysis of the security and risk profile of the pilot’s and an analysis of its specific training needs, as a a pre-requisite for the definition of the training activities and the population of the CRSA models. The three tasks of the phase will provide inputs for the following phase. In particular, the open-source vulnerability scanner OpenVAS[[2]](#footnote-3) will be exploited to define on which aspects the trainers have to focus during the definition of the training activities. The results of this analysis will be presented in Section 3.

Then, **Phase 2** describes the models definition and population. In particular, the **Cyber Range Security Assurance (CRSA)** models specifies potential cyber-attacks, the security mechanisms used against them, and the methods for assessing their effectiveness, and the **Cyber Range Simulation and Training (CRST) models**, describes the training activities composing the training programmes and whose definition is based on the CRSA data.

D3.2 and, in particular, D3.3 provide a clear and complete description of the models, their structure, and real-case examples applied to the actual pilots. It is important to note that CRSA and CRST models has been the base for the creation and execution of training activities. They will provide the goal and target of the specific training (CRSA) and the respective activities to be fulfilled (CRST).

Following***, Phase 3*** deals with the management of the training activities, defined in the previous phase with the definition of the actual models, tailored on the architecture used for the training. The output is this phase, in terms of usage of the platform and results of trainees’ activities, have been collected and can be supplied as input for the following phase.

In fact, **Phase 4** manage the post-training analyses***.*** In this phase two aspects have been examined: the changes in the security and risk profile of the pilots after the training, and the aggregation of trainees results. This phase will be very well covered by D5.5 and D5.6, that will include the results of the training specific of a single pilot and project-wise.

Finally, **Phase 5** will drive the trainers in the adaptation actions needed to re-configure the training activities and, if needed, the training platform. Using as input the data coming from the risk evaluation, the trainers can decide whether apply or not adaptation actions. At the end of a training campaign, the adaptation alerts received are used to improve the training activities raising, or lowering, the complexity of the exercise, or focus them on the aspects that the analysis of the security and risk profile still highlights as critical.

The following sections report the description of the tasks included in each phases as there were depicted in D4.2 without any changes. They are included to give a complete view of the process and, for what concerns in particular for Phase 1 and 4, a guide on how the overall cybersecurity risk is calculated and evaluated.

# Phase 1: Pre-Training Phase

As described above, this phase is dedicated on setting the stage for the foundation models of the AERAS framework. This phase is critical for the evaluation and adaptation process, but it is also of paramount importance for the definition of AERAS training activities.

The three tasks that compose the phase cooperate to collect all the data needed for the start-up of the framework and to semi-automatically identify the goals that the organization will best benefit from the training activities. The human support will be also critical in the definition of the specific training requirements and content.

In the following section, the discussion will focus on the specific tasks and the connection with the respective AERAS tool and methodologies.



## Task 1.1: Pre-training security and risk evaluation

This task is of paramount importance for setting the stage of AERAS training framework. In fact, the AERAS approach is founded on the concept that the effectiveness of the training actions can be evaluated basing on the improvement of the overall cybersecurity profile of the Organization. This approach has already proved as valid by the experimentation within the Horizon 2020 project THREAT-ARREST and documented in its Deliverable 7.8 [4].

The task is implemented by the AERAS procedure “Cyber System Real Time Risk Evaluator” and in particular by the “Threat Assessor” (Figure 3). This procedure involves the use of the open source vulnerability scanner OpenVAS used to detect and report possible vulnerabilities and weak points in the organization’s system.



Figure 3: AERAS procedures implementing Task 1.1

The scan will produce a report containing a summary of the detected vulnerabilities, ordered by severity and based on the National Vulnerability Database[[3]](#footnote-4) (NVD) provided by the National Institute of Standards and Technology (NIST).

The set of discovered vulnerabilities, included in the OpenVAS report, as well as the information about the Common Vulnerability Scoring System (CVSS) rate and impact of these vulnerabilities, will be included in the instance of the CRSA model and used to shape and index the training activities. Details about the data to be collected and included in the instances of the CRSA models will be provided in WP3 deliverables, in particular D3.3.

In the context of the monitoring and adaption framework described in this deliverables, the analysis related to the cybersecurity posture of the organization are used to calculate the overall risk profile, whose trend during the training will be then used to evaluate the effectiveness of the actions.

In the “Cyber System Real Time Risk Evaluator”, in fact, taking in input the data provided by the OpenVAS report, an overall risk rate is calculated. In particular, the CVSS is used is reliable indicator of the cybersecurity risk rate of the pilot.

As described by Mell *et al.* in [5] , CVSS offers the following benefits:

* **Standardized vulnerability scores.** CVSS is application-neutral, enabling an organization to score all of its IT vulnerabilities using the same scoring framework.
* **Contextual scoring**. CVSS scores represent the actual risk a given vulnerability poses, helping them prioritizing remediation efforts.
* **Open framework**. CVSS provides full details regarding the parameters used to generate each score, helping to understand both the reasoning behind, and the differences among, vulnerabilities scores.

The goal is for CVSS to facilitate the generation of consistent scores that accurately represent the impact of vulnerabilities. The CVSS score is calculated composing different metrics that examine specific aspects of the vulnerabilities, such as impact, exploitability, damage potential (see Figure 4).

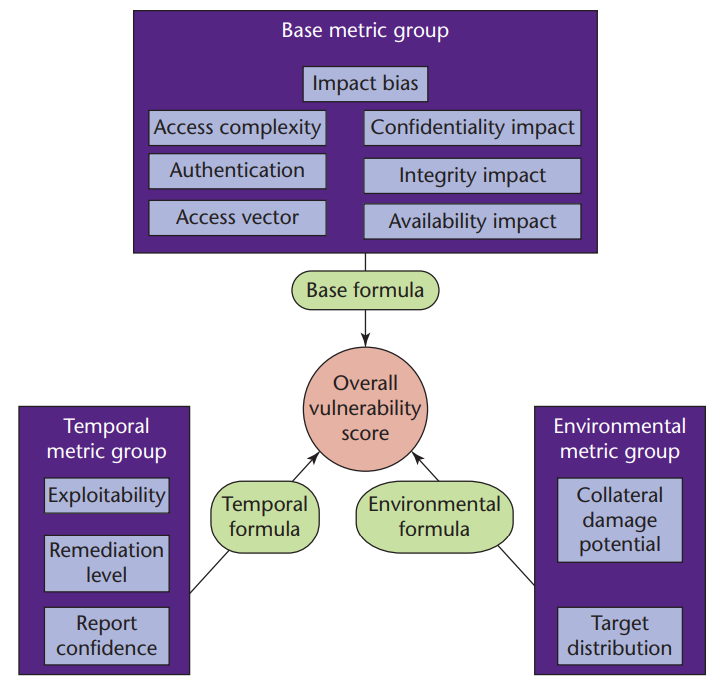


Figure 4: CVSS metrics composition [5].

One of the objectives of the AERAS project is to integrate in the proposed methodology, a mechanism for the continuous real-time monitoring of cyber-system and trainees[[4]](#footnote-5). The “Cyber System Real Time Risk Evaluator” will play the role of providing data about the actual state of the system. These data will be then proposed within the trainers interface in order to provide them the actual trend of the Organization’s security posture before, during, and after the training activities. Data shall be drilled up and down to visualize the aggregate rate, or the specific vulnerability CVSS value.

The procedure will be composed by a vulnerabilities analysis and an aggregation of the data, providing an unique indicator of the Organization’s risk rate calculate as:

Where *n* is the total number of detected vulnerabilities, *CVSS* is a function that identify and return the CVSS rate of the specific vulnerability *i* included in the OpenVas report, and *t* is the time when the rate has been calculated (*t=0* is the pre-training value). Furthermore, *severity* is a weight introduced to give more importance to vulnerabilities whose severity rate has been considered *High* (*severity=1*), other than *medium* (*severity=0.7*) or *low* (*severity=0.5*).

Data about risk level are then saved into a specific Risk Data database, that will be exploited also by Task 5.1 for post-training risk evaluation. The tool will also provide input to the Cyber System Multi-layer Monitor, that will use the provided data for CSLA continuous monitoring, and the data will be used in the population of the CRSA models. Figure 5 depicts the flow of data among the mentioned tools.

Cyber System Real Time Risk Evaluator

Cyber System Multi-layer Monitor

Visualization

CRSA models

*List of vulnerabilities with:  
- description  
- impact  
- solution*

*List of vulnerabilities  
RiskRate*

*List of vulnerabilities  
RiskRate*

Risk Data

Figure 5: Risk evaluation data flow.

## Task 1.2: Training needs analysis

The *Training Needs Analysis* procedure is aimed at providing all the needed data used to complete the CRSA models and populate the CRST with the actual information about the training programmes. This work will be better detailed in WP3, but it is also important for the sake of the adaptation process since it will provide the baseline and the ground over which any adaptation actions will be based on.

In fact, the learning process can be seen as an iterative cycle where the trainers define the programs, apply them, collect feedback and then revise the programs with respect to trainees results and comments. More in details, the learning cycle can follow the so-called “Kolb’s Four Stage of Learning” [6]. Kolb proposed that a learner moves through a cycle of actions which leads to observations and reflections on the training activity. These reflections are then absorbed and linked with previous knowledge and translated into abstract concepts or theories, which result in new actions to adjust to the training programme that can be tested and explored. The author identifies the following four experiential learning stages:

1. Concrete Experience: This stage of the learning cycle emphasizes personal involvement with people in everyday situations. The trainees can be faced with real-world problems to test their reaction and develop their skills.
2. Reflective Observation: In this stage of the learning cycle, people understand ideas and situations from different points of view. The gained experiences are examined through different perspectives, the results are processed, their significance is understood, and conclusions are drawn.
3. Abstract Conceptualization: takes the reflective process a step further by focusing on channelling those observations into a set game plan or theoretical approach. The experiences gained in the previous stage are grouped, linked to scientific data and/or theoretic approaches, general principles are drawn, and action guidelines are formed.
4. Active Experimentation: this stage deals with the process of testing existing ideas by creating new experiences. For instance, in the abstract stage, a trainee might develop theories based off of observations learned in the reflective stage, and in the active stage, the leader takes the time to then test their theories.

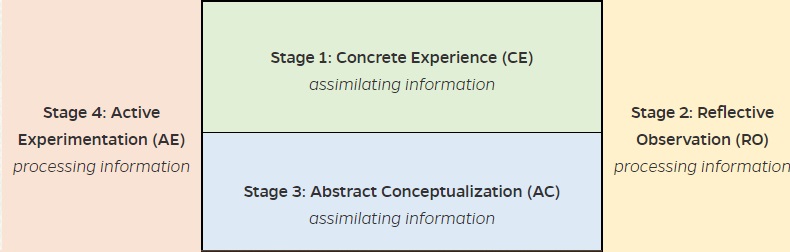


Figure 6: Kolb's cycle stages of learning.

In this iterative cycle (see Figure 6), the trainee’s evaluation has to be continuous, systematic, methodical, pedagogical, and multi-factor in terms of what has been taught, learned, and is capable of doing. Thus, an effective training procedure must be able to prepare an effective training programme that could foster the abstract conceptualization and experimentation of trainees. The programme should be also designed to adapt to each trainee’s capabilities and results, and continually contribute to their improvement.

The training needs of the Organization need to be evaluated, collected, examined and categorized in order to be included in CRST models and used as basis for the training programmes definition. Furthermore, the specific training activities identified in the analysis should be linked to the cybersecurity-specific concepts identified by the *Threat Assessor* procedure. This step will allow to link specific training activities to specific issues or weaknesses identified in the system, and will allow a monitoring of the system effectiveness based on the continuous assessment of the cybersecurity posture of the Organization.

This task has been instanced in the model population procedure described in WP3 deliverables.

# Phase 2: Models Population

The work in WP3 is also focused on the definition of the structure of CRSA and CRST models, in turn defining the cybersecurity assets and concepts related to the organization, and describing the details of the proposed training programmes. A strict link between the two is expected, to index training activity to specific vulnerabilities (e.g., DDOS attack) or assets (e.g., firewall or email clients).

The preparatory work in Task 1.1 and Task 1.2, described in Phase 1, is intended to support the work in the following tasks, providing them with specific data about the pilot’s cybersecurity landscape and training requirements.



## Task 2.1: CRSA Models population (procedure)

This task is related to the population of CRSA models. In particular, CRSA models are organized in four submodels, each describing a particular aspect of the pilot’s cybersecurity landscape and better explained in WP3 deliverables. Namely, each submodel (depicted in Figure 7) it is of interest for the following aspects:

* **Cyber System Submodels**: include data relative to the assets of the Organizations interested at the cybersecurity level. These assets could be workstations, personal laptops, routers, servers, or specific software used by employees. The identification of such assets will be done exploiting information collected in Task 3.1, but also by specific interview and analysis on site.
* **Cybersecurity Assurance Submodel**: this submodel includes data related to the assurance level of the company, investigating aspect relatives to the certification and maintaining of a predefined cybersecurity Service Level Agreements, and indicating aspects to be monitored to preserve the requested security level.
* **Risk Assessment Submodel**: contains data related to the risks detected in Task 3.1 and their current value. This submodel is of paramount importance in the continuous monitoring of the overall risk level before, during, and after the training activities.
* **Threats and Incidents Submodels**: the submodels keeps track of specific cybersecurity threats, vulnerabilities and, if available, incidents. Threats and vulnerabilities can be referred in training activities definition in other to categorize them, while the incidents tracking can be of interest in providing hints on improving in the cybersecurity management reducing the number and severity of detected incidents.



Figure 7: CRSA Submodels.

At each iteration of the Evaluation and Adaptation checklist the value in the submodels can be updated with the new data coming from Task 3.1 and 3.2. The submodels themselves include a timestamping mechanism that allows trainers to follow and examine the trend in the cybersecurity landscape during the training activities.

## Task 2.2: CRST Models population (procedure)

The procedure described in Task 2.2 is the specular of Task 2.1 described above but related to the training activities specification and linked to the CRST Programme Generator module (Figure 8).



Figure 8: CRST Programme Generator module.

The definition of the training activities, and the consequent population of CRST models, is important and linked to the monitoring process since it categorizes the activities with respect to the cybersecurity aspects listed in the CRSA models.

In fact, the goals of training activities are mainly referred to the defence against specific threats that are described in the CRSA models. At the same time, the positive (resp. negative) modification in specific risk values can be related to the effectiveness (resp. ineffectivess) of the linked training activities.

The role of trainers in this phase is of paramount importance since they have to indicate which specific training activities the programme should include with respect to the cybersecurity landscape of the Organisation. In fact, trainers can supply a training programme that is strictly related to Organization’s needs, described in the analysis of Task 3.1 and interview with pilot’s cybersecurity managers, organized on concrete objectives (i.e. active threats or vulnerability), as well as on general cybersecurity concepts. Furthermore, the lay the basis of the monitoring and evaluation approach linking activities to the respective risk factors.

The procedure described in this task will be further explained in WP3 deliverables. It is important to note that the training activities can be performed exploiting asynchronous methodologies, such as administering to the trainees *ad-hoc* questionnaires, or exploiting the facilities provided by the internal AERAS cyber range. The two modalities, or a mix of the two, will be configured in the CRST and interpreted and enacted by the CRST programme Generator Module, part of the cyber range engine.

# Phase 3: Training

The training phase is composed by a single task (Real-time Assessment of Trainee performances) and is dedicated to the execution of the training activities and on the tracking of trainee results. This phase will rely on the facilities provided by the cyber range infrastructure, and on its ability to track the actions of students.



## Task 3.1: Real-time assessment of trainee performances (tool)

This task is mainly performed by the Performance Evaluator and Progression Engine tools of the AERAS stack (Figure 9).

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Figure 9: Performance Evaluator and Progression Engine.

The Progression Engine, implemented following a Finite State Machine (FSM) architecture, is included in the Cyber range infrastructure and manage the administering of test and exercises during the execution of training activities. In fact, each programme, together with the support training material, are equipped with a set of activities (questionnaires and/or practical exercises on virtual environments) to be administered to the trainees. These activities are managed using an FSM approach by the Progression Engine.

The Progression Engine, during its execution, retrieve its inputs from the CRST Models and from the Cyber Range tools that manage the administering of the exercise to trainees. Then, the data are saved in a specific Training Results database to be accessed by the Performance Evaluator and all the tools that need to exploit trainees’ performance data (see Figure 10).

Performance Evaluator

CRST models

*Training Activity ID  
Training Programme ID  
Training-specific data*

Training Results DB

Progression Engine

Cyber Range Tools

Figure 10: Progression Engine expected communication flows.

# Phase 4: Post-Training

In this phase, the data collected during the execution of the training activities are aggregate and supplied to the other tools and procedures that need them to verify trainees progresses and evaluate possible adaptation alert on training programmes.

The phase id compose of two task, dedicated to the re-evaluation of the security landscape after the execution of the training, and the production of aggregate statistics about the trainees.



## Task 4.1: Post-training security and risk evaluation

Task 4.1 replicates the procedure describes in Task 1.1, where the cybersecurity landscape of the Organization administering the training programme is examined. The goal of the step is to understand if and in which measure the training activities helped in reducing the calculated risk level of the Organization.

The flow proposed in Figure 5 is still used, with the difference that there is a comparison between the data related to the pre-training phase, and the current data calculate in post-training. Figure 11 depicts the new scenario.

Figure 11: Post-training risk evaluation flow.

Cyber System Real Time Risk Evaluator

Visualization

CRSA models

*List of vulnerabilities with:  
- description  
- impact  
- solution*

*Updates on RiskRate*

Risk Data DB

In this task, only the vulnerabilities and risk detected in Task 1.1 are taken into consideration, and the interaction with CRSA models is related to the retrieving of input data only. Moreover. The status of the improvement (resp. deterioration) of the cybersecurity landscape of the Organization will be proposed by the Visualization in specific panels.

Since the checklist proposed in this deliverable is designed to be iterative, during each round the new risk data calculated in each iteration are saved in the Risk Data database to have the actual trend of the cybersecurity landscape. For this reason the interaction between the Cyber System Real Time Risk Evaluator and the Risk Data database are both in input and output.

The risk data will be proposed together with the data related to the trainees training activities, in order to provide the trainers with an effective tool to find and examine possible correlation among training activities and solved (resp. still active) vulnerabilities.

## Task 4.2: Production of aggregate data on trainees' activities

The Performance Evaluator tool, in cooperation with the Progression Engine, evaluates and aggregates the data saved in the Training Results Database. These data, in explicit or aggregate form, are sent to the Visualization tool for providing specific information about the performance of the trainees, or general aggregated data about the training programme (*no. executed training activities, no. active trainees, mean-min-max test results, …*).

Furthermore, data about performance are also of importance for the Programme Adaptor tool that will exploit the usage data and test results to raise alerts about the need of adaptation of training programmes. Further information about the Programme Adaptor will be provided in Section 7.

Performance Evaluator

Programme Adaptor

Visualization

CRST models

*Training Activity ID  
Training Programme ID*

*Trainee ID  
test results  
Execution time  
Training ID  
TrainingProgramme ID  
aggregatedTestResults (trainingID)  
aggregatedExecTimes(trainingID)*

*Training ID  
TrainingProgramme ID  
aggregatedTestResults (trainingID)  
aggregatedExecTimes(trainingID)*

Training Results DB

Progression Engine

Cyber Range Tools

Figure 12: Performance Evaluator tool data flow.

Figure 12 depicts at high level the communication flow cantered on the Performance Evaluator tool. In particular, the tool will exploit data saved in the Training Results database in order to produce an aggregation of data related to the execution of training activities.

On one side, the visualization tool should be able to display data in both aggregated and punctual forms. The trainer should be able to see the progress in term of *trainee* (punctual) and in term of *training programme* as a whole (aggregated).

On the other side, the Performance Evaluator will share aggregated data with the Programme Adaptor tool, that in turn will use the data to evaluate the level of accomplishment of the training programme, indicating the need (or not) to send alerts with respect to the required modifications and amendments to specific training activities.

It is important to note how the use of aggregated data in the adaptation phase will preserve the privacy of the specific trainees’ training data.

# Phase 5: Evaluation & Adaptation

This phase deals with the evaluation of the data coming from the previous phase, in order to assess possible change in the construction of the training programme and the effectiveness of the programme itself.

One of the key point of the AERAS framework is its intrinsic ability of providing an assessment *on-the-field* of the effectiveness of the training programmes. This is implemented thanks to the continuous assessment of organization’s security landscape and risk levels, and the link between training activities and detected vulnerabilities, through the CRSA models.

The following tasks describe how the comparison is made and the mechanism that will send alerts on training activities that need to be adapted.



## Task 5.1: Pre- and Post-training security and risk comparison

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamenteTask 5.1 is related to the comparison of risk data collected before in Phase 1, and the risk data as output of the Phase 4. The task goals are enacted by the Training Performance Monitor tool (Figure 13).

Figure 13: Training Performance Monitor tool.

During Phase 1 and 4, data about risk evaluation are analysed to make a comparison about the data at different time slice, highlighting the improvement (resp. deterioration) of the security landscape. Risk data are connected to the respective vulnerabilities and, thanks to CRSA models, to the assigned training activities.

Comparison data are then saved in specific monitoring tables and/or views to allow a quick visualization of data, giving the possibility to drill up and down with respect to specific training activities.

## Task 5.2: Adaptation Analysis of training activities

Immagine che contiene testo, Carattere, simbolo, segnaletica

Descrizione generata automaticamenteDuring Task 4.2, aggregate data about trainees results and usage, with respect to specific training activities, has been already made available to the Programme Adaptor tool (Fig. 15). In this task, we describe at high level how the programme adaptor is going to evaluate these data in order to identify training programs or training activities that need to be adapted.

Figure : Programme Adaptor tool.

The Programme Adaptor can detect needs of adaptation in case one or more of the following conditions are detected:

* **Change in Company assets**: during Task 2.1, CRSA model are populated with the list of detected vulnerability and the assets of the Organization that are subject of cybersecurity controls (i.e., firewalls, routers, critical workstations). Any time there is a change in the topology and a new asset is detected, the condition is met and the Programme Adaptor will trigger an *AssetChanged* alert. This condition is required since new assets present in the Organization topology could requires new skills and training to manage them.
* **New vulnerability found**: if in an iteration of the Task 1.1 a new vulnerability is found that it was not part of the original sets, the *NewVulnerability* alert is triggered in the Programme Adaptor. The alaert is an important notification, since the new detected vulnerability could raise the Company risk factor and change the overall cybersecurity landscape. New training activity should be added to the programme in order to deal with the new threat.
* **Low trainee performances**: if the Programme Adaptor detects a level in trainee performance lower than a specified threshold, the *LowPerfomance* alert will be triggered to notify trainers of that situation. Trainers can then analyze trainee data usage in order to identify if the low performance is due to a low commitment of trainees in executing training activities, or of a too-high complexity of the exercises that should be adapted.
* **High trainees scores**: if the Programme Adaptor detects that the trainees results is on average over a predefined threshold (i.e., 90% of the maximum grade), the *HighScore* alert is triggered. This alert can notify to the trainers that the overall training programme is too simple for the average level of trainee and, to optimize training outcome, the activities should be adapted to cover a highest level of complexity.
* **High (resp. Low) completion times:** this condition is met when the average time needed to complete the training activities are above (resp. below) a predefined percentage threshold of the maximum time expected to complete the training. If the condition is met, the *HighCompletionTime* (resp. *LowCompletionTime*) alert is triggered suggesting adaption to the specific training activity.

## Task 5.3: Alerts on training adaptation needs

In this task the Programme Adaptor procedure collects all the alert messages that the tools in Task 5.1 and 5.2 has sent, providing them to the visualization in order to be notified to the trainers.

The diagram in Figure 16 depicts the communication flow between the Programme Adaptor and the Visualization. In particular, the Programme Adaptor will send the collected alerts with the specification of the alert category, specific training activity involved or new vulnerability/assets (objects) detected, and the sending timestamp. For each kind of alert, a template of alert message will be included in order to provide more information to the trainee.

It is important to note that the role of the Program Adaptor will end with the sending of the alerts. The actual implementation of the adaptation action will be on the responsibilities of the trainers and managers. In the next iteration of the checklist, the tool will provide alerts only on newly detected adaptation actions, without repeating the same notification twice.

Figure : Programme Adaptor expected communication flow.

Visualization

*List of alerts with:  
- type of alert  
- object involved  
- template message  
- timestamp*

Programme Adaptor

The Programme Adaptor close the cycle of the Evaluation and Adaptation checklist, that can be iterated by the organization when the course is updated or after the termination of the training programme. Trainers and managers can decide to iterate the checklist also in case of the evidence of new threat or vulnerabilities that can involve the organization. The new iteration will update the current CRSA models and, if the training programme needs changes, the current CRST models.

# Application of the Cybersecurity Risk Methodology

In this Section, we apply the cybersecurity risk calculation methodology depicted in Section 2.2.1 to real data coming from one of the AERAS pilot, kept anonymous for privacy reasons. In fact, given the high-sensitivity of data and infrastructures involved in AERAS pilots validation, the published data are related to a subset of the organization’s systems.

However, this limitation does not invalidate the evaluation of the approach. In real case scenarios, the analysis could be applied to the whole infrastructure and data can be used by the system administrators for cybersecurity assessments.

The overall cybersecurity risk has been defined as

Where the following data sources are taken into consideration:

* The list of vulnerabilities provided in the OpenVAS report and related to the infrastructure under analysis.
* The CVSS vulnerability rate, provided using the CVSS methodology described in [7] and included in the OpenVas report.
* The specific severity of each vulnerability, indicated in the OpenVAS report, using the following weights:
  + Low: 0.3
  + Medium: 0.5
  + High: 1.0

# Preliminary Analysis

The analysis has been executed before providing any training activities using the AERAS platform. The described framework has been designed to be as flexible as possible to be exploited in any application context. The goal is to give evidence of an actual improvement of the cybersecurity posture of the organization under analysis before and after the training actions, giving to the analysts a simple but effective procedure that can be easily implemented in automatic tools.

As described above, the procedure relies on the data released by the execution of the Open Vulnerability Assessment Scanner OpenVas[[5]](#footnote-6), the state-of-the -art in terms of cybersecurity scanner available on the internet.

For privacy reason, the specific information about the node (IP address and network) of the analysed nodes have been omitted. In Table 1 the full list of the detected vulnerabilities (NVT, Network Vulnerability Test), its associated CVSS (Common Vulnerability Scoring System) score, and the related Severity, used to determine the specific weight.

It is important to note that the specific weight can be modified on request of the Organization, given that it remains constant throughout the whole training campaign.

Table 1: Detected vulnerabilities with CVSS score and Severity weight – Pre-Training.

|  |  |  |  |
| --- | --- | --- | --- |
| **Node** | **NVT** | **CVSS** | **Severity** |
| node1 | Microsoft SQL (MSSQL) Server End of Life (EOL) Detection | 10,00 | high |
| node2 | Check for discard Service (TCP) | 10,00 | high |
| node3 | Microsoft Internet Information Services (IIS) End of Life (EOL) Detection | 10,00 | high |
| node3 | Operating System (OS) End of Life (EOL) Detection | 10,00 | high |
| node4 | Microsoft SQL (MSSQL) Server End of Life (EOL) Detection | 10,00 | high |
| node4 | Operating System (OS) End of Life (EOL) Detection | 10,00 | high |
| node4 | Microsoft Internet Information Services (IIS) End of Life (EOL) Detection | 10,00 | high |
| node4 | Microsoft Internet Information Services (IIS) End of Life (EOL) Detection | 10,00 | high |
| node4 | Conficker Detection | 10,00 | high |
| node4 | Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote | 10,00 | high |
| node5 | Microsoft SQL (MSSQL) Server End of Life (EOL) Detection | 10,00 | high |
| node1 | jQuery End of Life (EOL) Detection - Windows | 9,90 | high |
| node1 | jQuery End of Life (EOL) Detection - Windows | 9,90 | high |
| node6 | jQuery End of Life (EOL) Detection - Windows | 9,90 | high |
| node7 | jQuery End of Life (EOL) Detection - Windows | 9,90 | high |
| node4 | Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active) | 9,80 | high |
| node6 | HTTP Brute Force Logins With Default Credentials Reporting | 9,80 | high |
| node4 | Microsoft Remote Desktop Protocol RCE Vulnerabilities (2671387) - Active Check | 9,30 | high |
| node4 | Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) | 8,80 | high |
| node8 | Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) | 8,80 | high |
| node3 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node3 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node3 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node3 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node1 | Eclipse Jetty Multiple Vulnerabilities (Jul 2022) - Windows | 7,50 | high |
| node1 | Eclipse Jetty DoS Vulnerability (GHSA-26vr-8j45-3r4w) - Windows | 7,50 | high |
| node1 | Eclipse Jetty DoS Vulnerability (GHSA-26vr-8j45-3r4w) - Windows | 7,50 | high |
| node1 | Eclipse Jetty Multiple Vulnerabilities (Jul 2022) - Windows | 7,50 | high |
| node4 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node5 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node6 | Eclipse Jetty Multiple Vulnerabilities (Jul 2022) - Windows | 7,50 | high |
| node6 | Eclipse Jetty DoS Vulnerability (GHSA-26vr-8j45-3r4w) - Windows | 7,50 | high |
| node7 | Eclipse Jetty DoS Vulnerability (GHSA-26vr-8j45-3r4w) - Windows | 7,50 | high |
| node7 | Eclipse Jetty Multiple Vulnerabilities (Jul 2022) - Windows | 7,50 | high |
| node9 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node10 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node11 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node12 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node13 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node14 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node15 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node11 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7,40 | high |
| node15 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7,40 | high |
| node15 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7,40 | high |
| node15 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7,40 | high |
| node4 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node4 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node4 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node4 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node5 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node11 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node15 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node15 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node15 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node15 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node15 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node15 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node16 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node16 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node17 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node17 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node18 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node8 | SSL/TLS: Report 'Anonymous' Cipher Suites | 5,40 | medium |
| node8 | SSL/TLS: Report 'Anonymous' Cipher Suites | 5,40 | medium |
| node1 | Eclipse Jetty URI Parsing Vulnerability (GHSA-qh8g-58pp-2wxh) - Windows | 5,30 | medium |
| node1 | Eclipse Jetty URI Parsing Vulnerability (GHSA-qh8g-58pp-2wxh) - Windows | 5,30 | medium |
| node1 | Eclipse Jetty Multiple Vulnerabilities (GHSA-qw69-rqj8-6qw8, GHSA-p26g-97m4-6q7c) - Windows | 5,30 | medium |
| node1 | Eclipse Jetty Multiple Vulnerabilities (GHSA-qw69-rqj8-6qw8, GHSA-p26g-97m4-6q7c) - Windows | 5,30 | medium |
| node3 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node4 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node4 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node6 | Eclipse Jetty URI Parsing Vulnerability (GHSA-qh8g-58pp-2wxh) - Windows | 5,30 | medium |
| node6 | Eclipse Jetty Multiple Vulnerabilities (GHSA-qw69-rqj8-6qw8, GHSA-p26g-97m4-6q7c) - Windows | 5,30 | medium |
| node7 | Eclipse Jetty Multiple Vulnerabilities (GHSA-qw69-rqj8-6qw8, GHSA-p26g-97m4-6q7c) - Windows | 5,30 | medium |
| node7 | Eclipse Jetty URI Parsing Vulnerability (GHSA-qh8g-58pp-2wxh) - Windows | 5,30 | medium |
| node9 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node10 | Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5,30 | medium |
| node10 | Weak Host Key Algorithm(s) (SSH) | 5,30 | medium |
| node13 | Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5,30 | medium |
| node13 | Weak Host Key Algorithm(s) (SSH) | 5,30 | medium |
| node15 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node15 | Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5,30 | medium |
| node15 | Weak Host Key Algorithm(s) (SSH) | 5,30 | medium |
| node1 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node1 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node2 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node2 | echo Service Reporting (TCP + UDP) | 5,00 | medium |
| node2 | Check for Quote of the Day (qotd) Service (TCP) | 5,00 | medium |
| node2 | Check for Chargen Service (TCP) | 5,00 | medium |
| node3 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node3 | Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability - Active Check | 5,00 | medium |
| node4 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node4 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node4 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node5 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node6 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node6 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node7 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node7 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node8 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5,00 | medium |
| node8 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5,00 | medium |
| node8 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node9 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node10 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5,00 | medium |
| node12 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node12 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node13 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5,00 | medium |
| node14 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node15 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node15 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node15 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node18 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node19 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node20 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node21 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node22 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node23 | SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection | 5,00 | medium |
| node24 | SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection | 5,00 | medium |
| node25 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node26 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node27 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node4 | Dell OpenManage Server Administrator Directory Traversal Vulnerability (Apr 2016) | 4,90 | medium |
| node1 | Cleartext Transmission of Sensitive Information via HTTP | 4,80 | medium |
| node5 | FTP Unencrypted Cleartext Login | 4,80 | medium |
| node6 | Cleartext Transmission of Sensitive Information via HTTP | 4,80 | medium |
| node7 | Cleartext Transmission of Sensitive Information via HTTP | 4,80 | medium |
| node28 | Telnet Unencrypted Cleartext Login | 4,80 | medium |
| node29 | Cleartext Transmission of Sensitive Information via HTTP | 4,80 | medium |
| node30 | FTP Unencrypted Cleartext Login | 4,80 | medium |
| node1 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node2 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node3 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node4 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node4 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node4 | SSL/TLS: RSA Temporary Key Handling 'RSA\_EXPORT' Downgrade Issue (FREAK) | 4,30 | medium |
| node5 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node6 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node7 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node8 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node8 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node8 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node8 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node8 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node8 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node9 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node9 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node10 | Weak Encryption Algorithm(s) Supported (SSH) | 4,30 | medium |
| node10 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node11 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node12 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node12 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node13 | Weak Encryption Algorithm(s) Supported (SSH) | 4,30 | medium |
| node13 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node15 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node15 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node15 | Weak Encryption Algorithm(s) Supported (SSH) | 4,30 | medium |
| node15 | Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability | 4,30 | medium |
| node15 | Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability | 4,30 | medium |
| node18 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node21 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node22 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node25 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node31 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node3 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node4 | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability | 4,00 | medium |
| node4 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node5 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node11 | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability | 4,00 | medium |
| node15 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node15 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node15 | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability | 4,00 | medium |
| node18 | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability | 4,00 | medium |
| node3 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node3 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node3 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node3 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node4 | SSL/TLS: 'DHE\_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) | 3,70 | low |
| node1 | Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Windows | 3,50 | low |
| node1 | Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Windows | 3,50 | low |
| node6 | Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Windows | 3,50 | low |
| node7 | Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Windows | 3,50 | low |
| node1 | Eclipse Jetty XXE Vulnerability (GHSA-58qw-p7qm-5rvh) - Windows | 3,40 | low |
| node1 | Eclipse Jetty XXE Vulnerability (GHSA-58qw-p7qm-5rvh) - Windows | 3,40 | low |
| node4 | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) | 3,40 | low |
| node6 | Eclipse Jetty XXE Vulnerability (GHSA-58qw-p7qm-5rvh) - Windows | 3,40 | low |
| node7 | Eclipse Jetty XXE Vulnerability (GHSA-58qw-p7qm-5rvh) - Windows | 3,40 | low |
| node15 | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) | 3,40 | low |
| node15 | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) | 3,40 | low |
| node5 | TCP Timestamps Information Disclosure | 2,60 | low |
| node6 | TCP Timestamps Information Disclosure | 2,60 | low |
| node7 | TCP Timestamps Information Disclosure | 2,60 | low |
| node8 | TCP Timestamps Information Disclosure | 2,60 | low |
| node10 | TCP Timestamps Information Disclosure | 2,60 | low |
| node11 | TCP Timestamps Information Disclosure | 2,60 | low |
| node13 | TCP Timestamps Information Disclosure | 2,60 | low |
| node15 | TCP Timestamps Information Disclosure | 2,60 | low |
| node15 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node16 | TCP Timestamps Information Disclosure | 2,60 | low |
| node16 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node16 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node17 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node17 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node17 | TCP Timestamps Information Disclosure | 2,60 | low |
| node18 | TCP Timestamps Information Disclosure | 2,60 | low |
| node19 | TCP Timestamps Information Disclosure | 2,60 | low |
| node20 | TCP Timestamps Information Disclosure | 2,60 | low |
| node22 | TCP Timestamps Information Disclosure | 2,60 | low |
| node28 | TCP Timestamps Information Disclosure | 2,60 | low |
| node29 | TCP Timestamps Information Disclosure | 2,60 | low |
| node31 | TCP Timestamps Information Disclosure | 2,60 | low |
| node32 | TCP Timestamps Information Disclosure | 2,60 | low |
| node33 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node34 | TCP Timestamps Information Disclosure | 2,60 | low |
| node35 | TCP Timestamps Information Disclosure | 2,60 | low |
| node2 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node1 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node3 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node4 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node8 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node9 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node11 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node14 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node15 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node16 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node17 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node19 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node23 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node24 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node28 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node34 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node36 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node37 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |

The analysis in Table 1 reported the following cumulative data.

* **Number of total vulnerabilities detected**: 232
* **Total nodes analysed**: 37
* **Mean number of vulnerabilities per node**: 6.27
* **Percentage of high-severity vulnerabilities:** 19%
* **Percentage of medium-severity vulnerabilities:** 55%
* **Percentage of low-severity vulnerabilities:** 26%

Using the RiskRate formula described above, the calculated risk rate for the organization under analysis, before any training activities, amounted to **3.21.** This reported risk level is an evidence of a good cybersecurity posture of the Organization, even if the level is too close to the medium-severity mean rate, indicating the need of a complete cybersecurity training to manage, in particular, the excess number of high-severity vulnerabilities found. The report can be a good guide for the trainers during the definition of training activities, focusing on the areas where the vulnerabilities are more critical. As an example, several high-severity vulnerabilities are related to the use of important software framework that are outdated and need replacement, since actually they are no longer receiving major updates.

# Post-training Analysis

The RiskRate analysis has been repeated after the execution of the training activities, giving some times to trainees, in particular IT employees, to apply specific action. It is important to note that the IT employees were aware of the AERAS RiskRate methodology and of the results of the cybersecurity analysis, giving them specific hints on which area they should operate on.

Furthemore, following the AERAS checklist, the analysis undertaken to create the CRSA models, has already included the concepts related to the vulnerabilities detected in the RiskRate analysis. In that way, the training activity could be focused on filling the gaps that have been identified.

Table 2 presents the status of the detected vulnerabilities after the execution of the training activities. As described in Section 3.2, the table presents the detected vulnerabilities (NVT), the CVSS score, the severity, and an anonymous label indicating the network node.

Table 2: Detected vulnerabilities with CVSS score and Severity weight – Post-Training.

|  |  |  |  |
| --- | --- | --- | --- |
| **Node** | **NVT** | **CVSS** | **severity** |
| node1 | Microsoft Internet Information Services (IIS) End of Life (EOL) Detection | 10,00 | high |
| node1 | Operating System (OS) End of Life (EOL) Detection | 10,00 | high |
| node1 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node1 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node1 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node1 | IBM WebSphere MQ 9.0.1 And 9.0.2 Information Disclosure | 8,10 | high |
| node10 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node10 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7,40 | high |
| node11 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node12 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node2 | Microsoft SQL (MSSQL) Server End of Life (EOL) Detection | 10,00 | high |
| node2 | jQuery End of Life (EOL) Detection - Windows | 9,90 | high |
| node2 | jQuery End of Life (EOL) Detection - Windows | 9,90 | high |
| node2 | Eclipse Jetty DoS Vulnerability (GHSA-26vr-8j45-3r4w) - Windows | 7,50 | high |
| node2 | Eclipse Jetty Multiple Vulnerabilities (Jul 2022) - Windows | 7,50 | high |
| node2 | Eclipse Jetty Multiple Vulnerabilities (Jul 2022) - Windows | 7,50 | high |
| node2 | Eclipse Jetty DoS Vulnerability (GHSA-26vr-8j45-3r4w) - Windows | 7,50 | high |
| node3 | Microsoft SQL (MSSQL) Server End of Life (EOL) Detection | 10,00 | high |
| node3 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node4 | Check for discard Service (TCP) | 10,00 | high |
| node5 | Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) | 8,80 | high |
| node6 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node7 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node8 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node9 | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 7,50 | high |
| node9 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7,40 | high |
| node9 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7,40 | high |
| node1 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node1 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node1 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node1 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node1 | IBM WebSphere MQ 8.0 And 9.0 Authentication Bypass | 3,70 | low |
| node10 | TCP Timestamps Information Disclosure | 2,60 | low |
| node10 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node11 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node12 | TCP Timestamps Information Disclosure | 2,60 | low |
| node13 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node13 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node13 | TCP Timestamps Information Disclosure | 2,60 | low |
| node13 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node14 | TCP Timestamps Information Disclosure | 2,60 | low |
| node14 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node14 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node14 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node16 | TCP Timestamps Information Disclosure | 2,60 | low |
| node17 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node18 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node19 | TCP Timestamps Information Disclosure | 2,60 | low |
| node2 | Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Windows | 3,50 | low |
| node2 | Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Windows | 3,50 | low |
| node2 | Eclipse Jetty XXE Vulnerability (GHSA-58qw-p7qm-5rvh) - Windows | 3,40 | low |
| node2 | Eclipse Jetty XXE Vulnerability (GHSA-58qw-p7qm-5rvh) - Windows | 3,40 | low |
| node2 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node21 | TCP Timestamps Information Disclosure | 2,60 | low |
| node21 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node22 | TCP Timestamps Information Disclosure | 2,60 | low |
| node23 | TCP Timestamps Information Disclosure | 2,60 | low |
| node23 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node24 | TCP Timestamps Information Disclosure | 2,60 | low |
| node25 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node26 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node3 | TCP Timestamps Information Disclosure | 2,60 | low |
| node4 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node5 | TCP Timestamps Information Disclosure | 2,60 | low |
| node5 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node6 | TCP Timestamps Information Disclosure | 2,60 | low |
| node8 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node9 | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) | 3,40 | low |
| node9 | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) | 3,40 | low |
| node9 | TCP Timestamps Information Disclosure | 2,60 | low |
| node9 | Weak MAC Algorithm(s) Supported (SSH) | 2,60 | low |
| node9 | ICMP Timestamp Reply Information Disclosure | 2,10 | low |
| node1 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024 bits | 5,30 | medium |
| node1 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node1 | Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability - Active Check | 5,00 | medium |
| node1 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node1 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node1 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node10 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node10 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node10 | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability | 4,00 | medium |
| node11 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node11 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node11 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node11 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node12 | Weak Host Key Algorithm(s) (SSH) | 5,30 | medium |
| node12 | Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5,30 | medium |
| node12 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5,00 | medium |
| node12 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node12 | Weak Encryption Algorithm(s) Supported (SSH) | 4,30 | medium |
| node13 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node13 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node14 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node14 | PKIX-SSH Prefix Truncation Attacks in SSH Specification (Terrapin Attack) | 5,90 | medium |
| node15 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node16 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node18 | SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection | 5,00 | medium |
| node19 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node19 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node2 | Eclipse Jetty URI Parsing Vulnerability (GHSA-qh8g-58pp-2wxh) - Windows | 5,30 | medium |
| node2 | Eclipse Jetty URI Parsing Vulnerability (GHSA-qh8g-58pp-2wxh) - Windows | 5,30 | medium |
| node2 | Eclipse Jetty Multiple Vulnerabilities (GHSA-qw69-rqj8-6qw8, GHSA-p26g-97m4-6q7c) - Windows | 5,30 | medium |
| node2 | Eclipse Jetty Multiple Vulnerabilities (GHSA-qw69-rqj8-6qw8, GHSA-p26g-97m4-6q7c) - Windows | 5,30 | medium |
| node2 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node2 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node2 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node2 | Cleartext Transmission of Sensitive Information via HTTP | 4,80 | medium |
| node2 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node20 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node3 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node3 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node3 | FTP Unencrypted Cleartext Login | 4,80 | medium |
| node3 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node3 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node30 |  |  | medium |
| node31 |  |  | medium |
| node4 | Check for Chargen Service (TCP) | 5,00 | medium |
| node4 | Check for Quote of the Day (qotd) Service (TCP) | 5,00 | medium |
| node4 | echo Service Reporting (TCP + UDP) | 5,00 | medium |
| node4 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node5 | SSL/TLS: Report 'Anonymous' Cipher Suites | 5,40 | medium |
| node5 | SSL/TLS: Report 'Anonymous' Cipher Suites | 5,40 | medium |
| node5 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node5 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5,00 | medium |
| node5 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 4,00 | medium |
| node5 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node5 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node5 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node5 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node5 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node5 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node6 | Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5,30 | medium |
| node6 | Weak Host Key Algorithm(s) (SSH) | 5,30 | medium |
| node6 | SSL/TLS: Renegotiation DoS Vulnerability | 5,00 | medium |
| node6 | Weak Encryption Algorithm(s) Supported (SSH) | 4,30 | medium |
| node6 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node7 | Missing 'HttpOnly' Cookie Attribute (HTTP) | 5,00 | medium |
| node7 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node7 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node7 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node8 | DCE/RPC and MSRPC Services Enumeration Reporting | 5,00 | medium |
| node9 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node9 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node9 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 5,90 | medium |
| node9 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node9 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node9 | SSL/TLS: Report Weak Cipher Suites | 5,90 | medium |
| node9 | Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5,30 | medium |
| node9 | Weak Host Key Algorithm(s) (SSH) | 5,30 | medium |
| node9 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node9 | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits | 5,30 | medium |
| node9 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node9 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node9 | SSL/TLS: Certificate Expired | 5,00 | medium |
| node9 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node9 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4,30 | medium |
| node9 | Weak Encryption Algorithm(s) Supported (SSH) | 4,30 | medium |
| node9 | Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability | 4,30 | medium |
| node9 | Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability | 4,30 | medium |
| node9 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |
| node9 | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability | 4,00 | medium |
| node9 | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4,00 | medium |

The analysis in Table 1 reported the following cumulative data.

* **Number of total vulnerabilities detected**: 170
* **Total nodes analysed**: 26
* **Mean number of vulnerabilities per node**: 6.15
* **Percentage of high-severity vulnerabilities:** 17%
* **Percentage of medium-severity vulnerabilities:** 55%
* **Percentage of low-severity vulnerabilities:** 28%

Using the RiskRate formula, the calculated risk has lowered to **3.04,** reporting a slight improvement from the pre-training level**.** The data collected in the two phases will be compared in the next section.

# Data comparison

The aim of the AERAS RiskRate methodology is to give to admin a way to effectively understand the level of the cybersecurity posture of the organization, summarizing in a rate the complex analysis behind, and to supply trainers with a efficient way to identifies gaps that could be filled in future training or adapt the actual training. The adaptation will be discussed in Section 4.

Table 3 summarizes the main results of the pre- and post-training analysis, to give a up-level view of the cybersecurity status and its evolution. It is important to note that the actual analysis is only based on the validation round we made during the AERAS validation in one pilot. The test, to be fully effective, must be run periodically during a massive training campaign, to see a complete effect on organization infrastructure. However, even if limited, the analysis can be discussed and some hints can be found out.

Table 3: RiskRate results comparison.

|  |  |  |
| --- | --- | --- |
|  | Pre-training | Post-training |
| No. vulnerabilities | 232 | 170 |
| No. nodes | 37 | 26 |
| Average vulnerabilities per node | 6.27 | 6.15 |
| High-sev. vulnerabilities | 19% | 17% |
| Med-sev. vulnerabilities | 55% | 55% |
| Low-sev. vulnerabilities | 26% | 28% |
| RiskRate | **3.21** | **3.04** |

First of all, it is clear that the overall RiskRate level has lowered from 3.21 to 3.04. Given that the grade can go from 1 to 5, this results in an improvement of the 5% of the probability to be subject to cybersecurity-related issues. The IT team worked in sorting out major issues with the highest severity level. In fact, comparing Table 1 and Table 2 we can see that all the issue related to the outdate operating systems have been resolved, reducing the impact of high-severity vulnerabilities.

However, new vulnerabilities raised out, in particular related to security protocol like SSL, mainly due to the expiration of security certificates, suggesting new areas for training (see Section 4).

The number of analysed nodes has also been reduced. This is due to the fact that the company is regularly modifying its infrastructure adding or removing nodes as needed. However, the total number of detected vulnerabilities, and the average number for nodes, has reduced. This could be related to the fact that the RiskRate analysis suggested to the IT manager to retire outdated nodes, more prone to be vulnerable to attacks, substituting them with newer system and re-organizing the service supplying.

The positive trend identified in the RiskRate can emphasize the need of training and incentive investment in it, exploiting an integrating system like the one presented by the AERAS Consortium.

# Evaluation and Adaptation

While Phases 2 and 3 are described and reported in WP3 and WP5, this section gives hints to trainers of needed adaptations of the current training activities with respect to the actual risk analysis results, after (or during) the training campaign.

In fact, the risk analysis presented in Section 3, depict a situation where the IT employees, after the trainings, decided to sort out specific vulnerabilities identified by major severity, and re-organizing the whole infrastructure in terms of a rationalising the existing infrastructure, retire old nodes and update critical ones.

The re-organization, and maybe the updating of the system, highlights new vulnerabilities the managers should manage to further improve the cybersecurity posture. In particular, such improvement should be reflected in an adaptation of the training actions that can give to IT employees the specific skills to work on them.

Specifically, vulnerabilities related to the expiration of security certificates and related, in particular, to the SSL security protocol stands out as major medium-severity vulnerabilities. This could easy raise an alert to the trainees in order to adapt the training campaign in order to encompass also this new area. Reacting to this alert, trainers and manager can go back to Phase 2 to update CRSA models to reflect the new cybersecurity status, manage the creation of new CRST and the subsequent training activities, and administer the new activities to the specific subset of employees that can should work on the new vulnerabilities (Phase 3).

This continuous approach to the adaptation of the training activities can be very beneficial to the overall quality of the educational level of the organization’s staff. It is important to note that the trainers should not base the adaptation cycles to internal problems only, but they should keep monitored the actual trend of cybersecurity n order to be ready to react to new problems.

Furthermore, the periodic RiskRate analysis, whose main tool (OpenVAS) is kept up-to date with respect to the vulnerabilities databases provided by public entities like NIST.

# Conclusions

This deliverable extended D4.2 applying the RiskRate procedure described on a real case scenario of one of the AERAS pilot, that has been kept anonymous for security reasons.

The procedure has been applied before and after the training campaign, showing the improvements we got in the cybersecurity posture and, in particular, highlighting the importance of how a continuous monitoring of the cybersecurity posture during a training campaign can be beneficial in the assessment of the training quality itself, and how it can give alerts on possible adaptation of the activities to react to new vulnerabilities or new problems found.

This deliverable, in collaboration with D4.3, complete the description of the AERAS training methodology, describing the platform (D4.3) and applying the AERAS checklist for the execution of effective and complete training campaigns.

# References

|  |  |
| --- | --- |
| [1] | G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis and H. Koshutanski, “Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees,” *Applied Sciences,* vol. 10, no. 16, 2020. |
| [2] | D. Kirkpatrick and J. Kirkpatrick, Evaluating Training Programs: The Four Levels, Berrett-Koehler Publishers, 2006. |
| [3] | P. Toth and P. Klein, “A Role-Based Model for Federal Information Technology/ Cybersecurity Training,” National Institute of Standards and Technology (NIST), 2014. |
| [4] | THREAT-ARREST Project, “D7.8: Final THREAT-ARREST evaluation report,” 2021. |
| [5] | P. Mell, K. Scarfone and S. Romanosky, “Common Vulnerability Scoring System,” *IEEE Security & Privacy,* vol. 4, no. 6, pp. 85-89, 2006. |
| [6] | D. A. Kolb, Experiential Learning: Experience as the Source of Learning and Development, Pearson FT Press, 2014. |
| [7] | Forum of Incident Response and Security Teams, “Common Vulnerability Scoring System SIG,” [Online]. Available: https://www.first.org/cvss/. [Accessed 2025]. |

1. † *The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 872735.* [↑](#footnote-ref-2)
2. <https://www.openvas.org/> [↑](#footnote-ref-3)
3. <https://nvd.nist.gov/> [↑](#footnote-ref-4)
4. **Objective 2:** Develop **novel hybrid cyber security risk analysis models**, which **combine** traditional **static cyber security risk analysis** principles and standards with **continuous risk estimates**. These estimates are informed from **simulation** and the continuous **real-time multi-layer monitoring** of cyber-systems and trainees. [↑](#footnote-ref-5)
5. <https://www.openvas.org/> [↑](#footnote-ref-6)