ECHO Federated Cyber Range: Towards Next-Generation Scalable Cyber Ranges

Nikos Oikonomou
CERTH-ITI
Thessaloniki, Greece
nikosoik@iti.gr

Notis Mengidis
CERTH-ITI
Thessaloniki, Greece
nmengidis@iti.gr

Minas Spanopoulos - Karalexidis
CERTH-ITI
Thessaloniki, Greece
mspanopoulos@iti.gr

Antonis Voulgaridis
CERTH-ITI
Thessaloniki, Greece
antonismv@iti.gr

Matteo Merialdo
Security Services
RHEA Group
Redu, Belgium
m.merialdo
@rheagroup.com

Ivo Raisr
Security Services
RHEA Group
Prague, Czech Republic
i.raisr@rheagroup.com

Kaarel Hanson
Guardtime
Tallinn, Estonia
Kaarel.Hanson
@guardtime.com

Paloma de La Vallee
Cyber Defense Lab
Royal Military Academy
Brussels, Belgium
p.delavallee@cylab.be

Theodora Tsikrika
CERTH-ITI
Thessaloniki, Greece
theodora.tsikrika@iti.gr

Stefanos Vrochidis
CERTH-ITI
Thessaloniki, Greece
stefanos@iti.gr

Konstantinos Votis
CERTH-ITI
Thessaloniki, Greece
kvotis@iti.gr

***Abstract*—Cyber ranges are valuable assets for cybersecurity training and education, advanced prototype development, and certification testing. To address the limitations of individual cyber ranges in terms of their capabilities and capacities to simulate complex realities and multi-sector dependencies, federated cyber ranges are emerging. This work presents the ECHO Federated Cyber Range, a marketplace for cyber range services, that establishes a mechanism by which the independent cyber range capabilities can be interconnected and accessed via a convenient portal for configuration and managemement. Its features and architecture are described in detail, along with the design,validation, and deployment of a training scenario.**

***Index Terms*—cyber range, training, federated, simulation, situational awareness, cybersecurity**

I. Introduction

Recent cybersecurity incidents indicate that cyber threats are constantly increasing in complexity, with attackers becoming more organised and their arsenal continuously upgraded with more advanced tools. This necessitates the availability of cybersecurity training in realistic conditions and renders the hands-on experience using cyber ranges one of the most sought-after assets for cybersecurity professionals. Since cyber ranges are closed and controlled environments that contain all the necessary tools, networks, and user simulations required for training and education purposes, they allow trainees to use realistic scenarios that otherwise would be impossible to execute, with minimal risk of a threat getting out of hand.

Overall, cyber ranges have the potential to help strengthen the stability, security, and performance of cyber-infrastructures, e.g., information technology (IT), operations technology (OT), and industrial control systems (ICS), by facilitating high-fidelity simulations of operational conditions in a virtual environment. These virtual environments are a practice ground not only for hands-on education and training purposes, but also for advanced prototype development and cybersecurity certification testing. Cyber ranges also offer the possibility to evaluate new technologies or updates to existing technologies prior to operational deployment.

An important challenge for most cyber ranges currently in the market is their limited capabilities and capacities to simulate the complex realities and dependencies in inter-sector scenarios. While sector-specific cyber ranges are emerging, it is still extremely complex to simulate effective inter-sector scenarios; a cyber range may be well equipped in one sector, but it may lack capabilities in other sectors. Moreover, large-scale cyber defence exercises have revealed that simulating complex environments with hundreds or even thousands of virtual machines cannot be realistically achieved by using only one cyber range provider. Besides, a multi-domain cyber range is not something easily sustained by a single organisation since it is cost-prohibitive to own and manage all the required cyber ranges, and also difficult to have the expertise to perform research and development on these heterogeneous ranges.

It is thus important to have the capability to combine multi-domain cyber ranges from different providers to create elaborate scenarios. It is also conceivable that multiple cyber ranges, each with its area of expertise, could work together to offer end users the ability to train on multiple use cases and different scenarios. To this end, the concept of *federation* has been developed as a solution to meet such growing demands. In this context, this work presents the Federated Cyber Range developed by the ECHO pilot project (https://echonetwork.eu/) which aims to address the problem of fragmented capabilities by establishing a mechanism by which the independent cyber range capabilities can be interconnected and accessed via a convenient portal for configuration and management.

Section II overviews the state-of-the-art on cyber ranges. Section III presents the ECHO Federated Cyber Range, its features, and architecture. Section IV presents the design, validation, and deployment of a scenario which is the primary driver of the system. Section V concludes this work.

II. Related Work

This section overviews the current state-of-the-art cyber ranges so as to identify capabilities and functionalities served within modern cyber ranges and also evaluate the technology stack they utilise. In a survey by Holm et al. [1], information from 30 ICS testbeds was collected and several characteristics were covered including the main methods that can be used for the implementation of ICS in cyber ranges, namely virtualisation, simulation, and hardware. The survey also classified the objectives of these cyber ranges into 11 categories. The survey, although thorough, was mostly focused on industrial ranges and their vulnerability assessment.

A systematic review by Kucek et al. [2] focused on assessing functionality and configuration in capture-the-flag (CTF) environments. They examined eight open source CTF environments and concluded that most of the platforms can be installed upon an arbitrary operating system and almost all platforms are recommended to be installed inside Vagrant or Docker. They also highlighted some generic features that these environments shared such as a scoring system, scheduling options, and graphical statistics per user and challenge.

Yamin et al. [3] performed the most recent and arguably most comprehensive survey on cyber ranges and security testbeds. They identified a gap in the literature which, according to them, is either sectorial or outdated, and proceeded with their own analysis, while also proposing a cyber range specific taxonomy. Their findings show that most modern cyber ranges use a hybrid environment which combines emulation, simulation, and real equipment, in order to produce a more realistic exercise experience. Even though they determine that most cyber ranges are focused on educational aspects, there is also an increased interest to use cyber ranges for testing of systems or products. Finally, scalability and federation are identified as the main future research trends and directions.

III. ECHO - Federated Cyber Range

The ECHO - Federated Cyber Range (E-FCR) provides the infrastructure needed to enable security roadmaps research, experimentation, test, and certification of new security technologies, as well as to support advanced cybersecurity training (including distributed computer-assisted exercises with specific scenarios) and preparation of qualified cybersecurity experts.

A. Overview

The E-FCR aims to interconnect existing cyber range capabilities through a convenient portal operating as a "broker" between user requirements and a pool of available cyber range capabilities. Within ECHO, a cyber range is defined as a multi-purpose virtualisation environment supporting three ”security-by-design” needs: (i) knowledge and skills development; (ii) improved system assurance during development; and (ii) improved system assurance through security test and certification evaluation. Overall, the objective of the E-FCR is to solve the problem of fragmented capabilities among cyber ranges by establishing a mechanism by which the independent cyber ranges can be interconnected and accessed via a convenient portal for configuration and management.

The E-FCR main concept centres on a portal/dashboard where users can develop their single and multi-sector cyber scenarios and then request the portal to configure the intended scenario from a pool of interconnected cyber ranges operated by different providers. Under this process, the portal also serves as a means to validate whether the scenario can be simulated, or highlights the case where some aspects of the scenario may require additional simulation capabilities, whether due to missing availability of virtual images or otherwise.

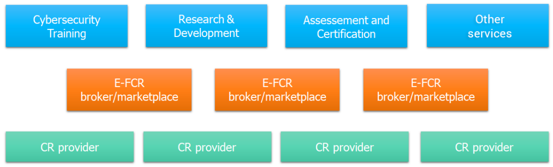


Figure 1. Cyber range providers and E-FCR

B. Vision

One of the main goals of the ECHO project is to establish the E-FCR as a significant **marketplace for cyber range services** in Europe. As such, the vision is to incorporate several aspects: the marketplace, the business space, and the innovation aspect. In general, the marketplace will focus on commercial factors, linking supply and demand, thus enabling reciprocal value exchange. In addition, the E-FCR will perform as a *virtual space*, bringing experts, customers, requirements and capabilities together in one environment (business space), and also as an *innovation driver*, by promoting open innovation and providing access to a potentially unlimited pool of innovators. These elements will be ideally guided and supported by the future EU Network of Competence Centres[1].

The approach towards the development of a strategy for the E-FCR needs to be guided primarily by the following principles: (i) **Sustainability** (with main aim to cover incurring costs on a long-term basis and potentially generate profit); (ii) **Value Creation**; (iii) **Growth** (E-FCR aims at providing to its participants a broad base enabling growth and scaling); (iv) **Visibility** (E-FCR has been designed to enhance each of its participants' visibility, extending their reach and networking power thus removing geographic boundaries and language barriers, fostering the Digital Single Market; and (iv) **Community building** (a fundamental objective is to attract, grow, and feed a vibrant and active community around the E-FCR whereby the business strategy for the E-FCR marketplace needs to be strictly linked to the E-FCR (or ECHO) innovation strategy; the creation of innovation and services within the marketplace fosters its Visibility, Value Creation, and Growth).

C. Features

The design and development of the E-FCR system has been driven by and aims to fulfill the overall ECHO vision described

[1] https://cybercompetencenetwork.eu/ & https://digital-strategy.ec.europa.eu/en/policies/european-cybersecurity-competence-network-and-centre/

above. In particular, the E-FCR is envisioned as a super-system connecting different cyber range *Providers* and acting as a concentrator of capacities and capabilities. *Customers* can request cyber range *Services* from multiple cyber ranges using the E-FCR. The system then acts as a concentrator connecting Customers and Providers. The E-FCR requires cyber range Providers to provide the up-to-date capability/capacity of each of the networked *Cyber Ranges*; this feature requires E-FCR *Agents* deployed on the federated ranges.

The Customers can select existing Services from the *Marketplace* or express their need for a custom Service via the E-FCR GUI and send the Request to the Providers. The E-FCR GUI provides the Customer with a set of information and a dashboard to submit the *Service Request*. An expert Customer can define technical details of the desired Service. In contrast, a non-technical Customer leverages standard contents in the Marketplace to simplify the Service Requests' creation. The aim is to allow the E-FCR to be accessible to a broader market, including non-technical Customers.

The E-FCR acts as a middleman between the Customer and the cyber range Provider(s) and Content Providers. This simplifies the Customer's interactions, who only has to deal with a single entity (the E-FCR) for the Request and the Services' definition. Providers forming a federation choose a *Prime Provider*.

The E-FCR offers a GUI to the cyber range Providers or Content Providers to design and propose pre-defined cyber range Services (e.g. pre-defined training scenarios) and expose them to the Customers (via the Marketplace). The same GUI is also used for negotiation to find a suitable solution when Service validation fails. The GUI also allows the Providers to manage a Federation of providers and manage the customers' Service Requests. Besides, the E-FCR will be used by the cyber range Providers to search for potential partnerships with other cyber range or Content Providers.

The E-FCR concentrates valuable information from the individual Cyber Ranges and provides a single, simple interface to validate Service Requests. The complexity of the Service's instantiation and management will remain at the single cyber range site; full automation is not foreseen and thus manual activities will be needed at each cyber range Provider side.

If the Service Request instantiation is successful, then the Customer (and their related *End Users*) interacts with the requested cyber range Service directly using the cyber range Provider tools/facilities, since it is not envisioned that the E-FCR would offer direct access to the cyber range instantiated Services; each cyber range Provider provides its own remote access system to the Services. Suppose a cyber range is provided with sector-specific capabilities; in that case, they become part of the cyber range description (capability information) within the E-FCR (e.g., from IoT devices to ICS systems, to satellite simulators or other physical appliances).

The E-FCR is not bounded only to training Services, but also leverages simulations, testing environments, emulation environments, digital twins: this allows the E-FCR to provide Services to a vast range of customers.

D. Architecture

E-FCR platform is divided in four major tiers: (i) **Client Tier**, (ii) **Front Tier**, (iii) **Mid Tier**, and (iv) **Back Tier**. Each tier comprises several core E-FCR components and provides specific access points and interconnections to adjacent tiers.

Starting from the top layer, the core component of the Client Tier is the **E-FCR Dashboard** which is mainly a container of different subcomponents which all together compose the actual user interface of the E-FCR platform. Client Tier is directly connected to the immediate lower tier, the Front Tier.

The Front Tier is actually an intermediate component, namely **ReverseProxy**, which is responsible for establishing connectivity between the Client and Mid tiers. Notably, this component is a single point of entry to the system.

At Mid Tier, the number of core components increases and there is a clear distinction into two sub-layers. The first layer, corresponds to the interconnection point of Front and Mid tiers respectively, being the main entry point of all requests entering the current tier. This component is called **Access Portal** and is basically responsible for routing incoming requests to the correct micro-service, or recipient subcomponent, residing in the Mid Tier, while also ensuring that only authorised requests are allowed to proceed. The second layer, the inner Mid Tier, contains the following core components.

Billing Manager is the component that defines the whole billing process, i.e., it determines service provisioning costs to customers in regards to service selection. There are two significant categories, the standard service and the custom service offering. In the former an automatic preparation of a standard invoice is triggered for a predefined service, while in the latter there is plenty of room for configuration and negotiation between the individuals, whereas a custom, and thus a manual, preparation of an invoice needs to be configured.

Capacity & Capability Map is a structure denoting the available capacities and capabilities of the enlisted Cyber Ranges of the providers. It provides information in respect to what each Cyber Range is capable of providing and in what extent, meaning how much of its capacities are in numbers, while also depicting a snapshot of its current reservations.

Cyber Range Gateway is another communication entry level point, which connects the E-FCR platform from the Mid-Tier to the Cyber Range Tier which resides outside of the platform. This interconnection is achieved through the Cyber Range Gateway and the components called *Agents* which reside on top of each connected Cyber Range. This works as a shield for the E-FCR components as it "hides" the actual complexity of Cyber Ranges' topology.

Quality of Service (QoS) gathers information on metrics from Cyber Ranges regarding potential scenarios running on them. It gathers all available information from their Agents in batches and creates records for each corresponding scenario.

Service Catalogue is responsible for storing and making available any services provided in the Marketplace (part of the aforementioned Dashboard in the Client Tier).

Service Request Repository is, similarly to the Service Catalogue, responsible for storing and making available all the

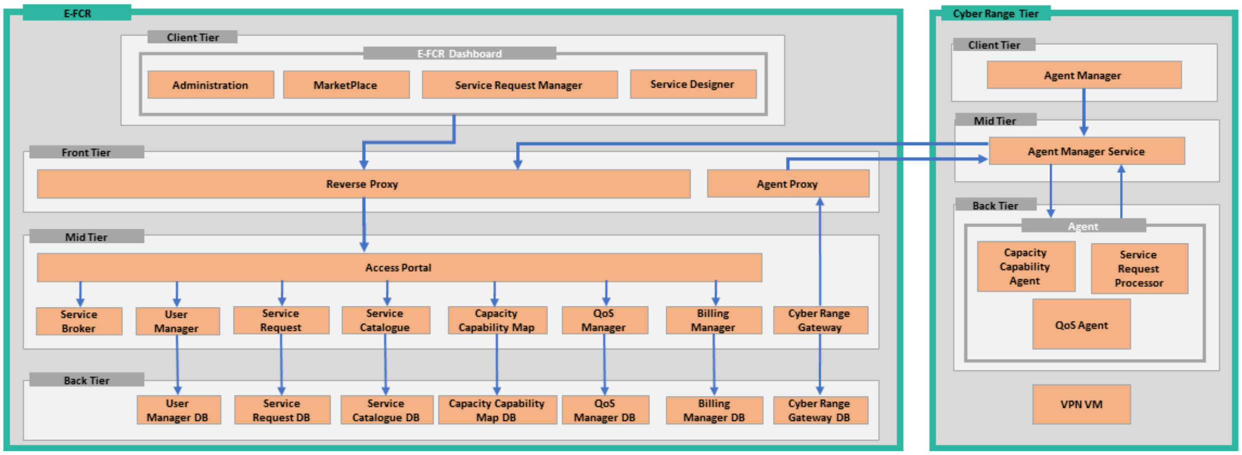


Figure 2. E-FCR architecture

information regarding service requests, such as negotiations between Customer and Provider, Service Level Agreements (SLAs), contracts with past and current statuses etc.

Service Broker handles the processing of a request and defines its distinct stages during its lifecycle in the platform. These steps consist of the initial receipt of the request from the Service Request Repository, followed by a validation process where the Capacity and Capability Map is interrogated in order to find the optimal Cyber Range to assign the service request to, and finally sending the request to the Cyber Range provider(s) for the final validation, refinement, deployment, instantiation, and start of the service.

User Manager manages the user repository of the system, providing user information (e.g., organisation, profile, and contact) and also provider information (e.g., content and cyber range providers and associated Cyber Ranges). It is also responsible for providing insight into users' roles and permissions about the authorisation of a user in the system.

There is also a MongoDB instance and a DelayedMessageQueue component which could be distinguished as the Back Tier of the system. Many of the aforementioned components communicate directly with these, especially components that need to store and keep collections of their resources; for instance the Service Request Repository holds a collection of the active Service Requests and the Capacity Capability Map a collection with all the available Cyber Range data.

IV. Scenarios

E-FCR has been designed with some specific user scenarios as primary drivers for the system, see Table I. It is essential to distinguish between a *Service* (generally selected by a Customer from the Marketplace) and *Custom Service* (a Service designed by the Customer and proposed to the E-FCR, which will match the connected cyber range's capacities and capabilities Providers to fulfill the Request). A Custom Service match-making is a complex activity that has been implemented via the Service Broker component, the core of the E-FCR.

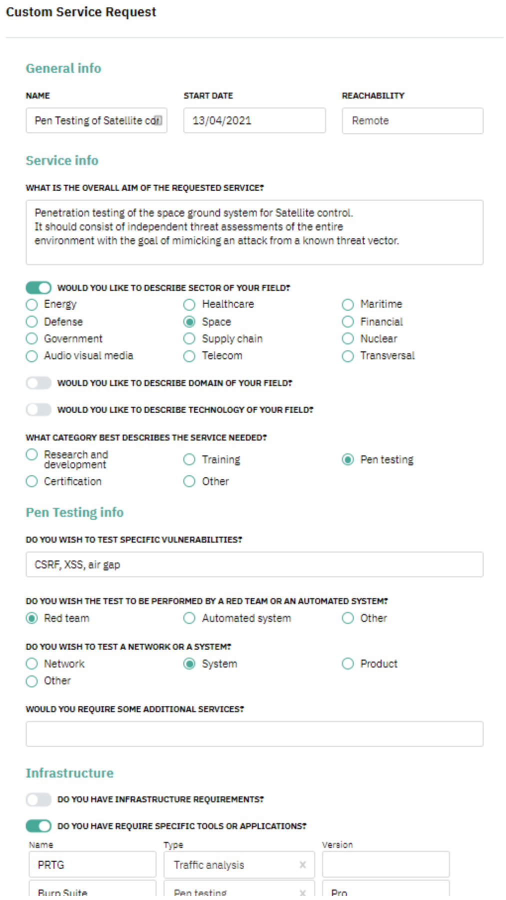
Table I
Prominent high-level Use Cases elicited for the E-FCR

Scenario	Description
Service provided by a **single Cyber Range Provider**	A listed Service proposed in the Marketplace by a federation of Content and Cyber Range Providers is delivered to a registered Customer at the requested date. The Service is provided as-is, without any customisation.
Service provided by a **federation of a Content Provider** and a Cyber Range Provider	A listed Service proposed by a single Cyber Range Provider in the Marketplace is provided to a registered Customer at the requested date. The Service is provided as-is, without any customisation.
Service provided by a **federation of Cyber Range Providers**	A listed Service proposed by a federation of Cyber Range Providers is delivered to a registered Customer at the requested date. The Service is provided as-is without any customisation.
Custom Service provided by a single Provider or a federation	The Customer submits the Request for a custom Service (or for a customized existing Service) to the E-FCR. The Service is provided by a Federation of Cyber Range Providers suggested by the E-FCR.

A. Custom Services Design and Match-making

Allowing the Customer to design his/her Service is one of the most complex tasks for the E-FCR, since it implies the translation of the Request into a set of capacities and capabilities to be matched with the collection of capacities and capabilities of the federated cyber ranges. While the match-making process is performed by the Service Broker, the design of a Customer Service leverages the **Service Designer** on the main E-FCR GUI (Figure 3) which aims to bridge the gap between high-level Service description (generally what is needed by Customers) and low-level capability/capacity world (understood and required by Cyber Range operators).

The complexity of this task stems from the need to interface with both humans and machines. Customers would define the Requested service in natural language (i.e., unstructured text), the parsing of which is notoriously challenging for machines.



Custom Service Request

General info

NAME	START DATE	REACHABILITY
Pen Testing of Satellite co	13/04/2021	Remote

Service info

WHAT IS THE OVERALL AIM OF THE REQUESTED SERVICE?

Penetration testing of the space ground system for Satellite control.
It should consist of independent threat assessments of the entire
environment with the goal of mimicking an attack from a known threat vector.

● WOULD YOU LIKE TO DESCRIBE SECTOR OF YOUR FIELD?

○ Energy ○ Healthcare ○ Maritime
○ Defense ● Space ○ Financial
○ Government ○ Supply chain ○ Nuclear
○ Audio visual media ○ Telecom ○ Transversal

○ WOULD YOU LIKE TO DESCRIBE DOMAIN OF YOUR FIELD?

○ WOULD YOU LIKE TO DESCRIBE TECHNOLOGY OF YOUR FIELD?

WHAT CATEGORY BEST DESCRIBES THE SERVICE NEEDED?

○ Research and development ○ Training ● Pen testing
○ Certification ○ Other

Pen Testing info

DO YOU WISH TO TEST SPECIFIC VULNERABILITIES?

CSRF, XSS, air gap

DO YOU WISH THE TEST TO BE PERFORMED BY A RED TEAM OR AN AUTOMATED SYSTEM?

● Red team ○ Automated system ○ Other

DO YOU WISH TO TEST A NETWORK OR A SYSTEM?

○ Network ● System ○ Product
○ Other

WOULD YOU REQUIRE SOME ADDITIONAL SERVICES?

Infrastructure

○ DO YOU HAVE INFRASTRUCTURE REQUIREMENTS?

● DO YOU HAVE REQUIRE SPECIFIC TOOLS OR APPLICATIONS?

Name	Type	Version
PRTG	Traffic analysis ×	
Burp Suite	Pen testing ×	Pro

Figure 3. Service Designer captured information from the customer

1) ESDL: The ECHO Service Description Language (ESDL) aims to find a balance between the need to fix a textual framework that is manageable by a machine, but still feels natural for humans. ESDL is used to describe E-FCR Services from the Customer's point of view, but the description can still be sufficiently detailed to serve as a basis for a contract between Customer and Provider. ESDL has its associated grammar, so it can be machine parsed. An ESDL file serves as a common ground to discuss and negotiate the Service between the parties and evolves during the Services negotiations. Given the versatility of ESDL, this file can be a central point to articulate different subsets of a Service (Figure 4).

2) Using ESDL: Customers and Providers are not required to learn ESDL. The Service Designer includes a wizard to guide mainly the Customer through the designing process via a series of questions, sort of a decision tree. The wizard is intended mostly for the first Service design, to capture as much as possible from the Customer in a structured form. However, it can be used also later, for developing an additional part of the Service, for example. The designed Service is displayed in a tree-like form, with the possibility to change or add any part of the Service, within the allowed limits of the ESDL grammar. In later stages of development, it is planned to include a graphical tool to aid with the network and timeline topologies.

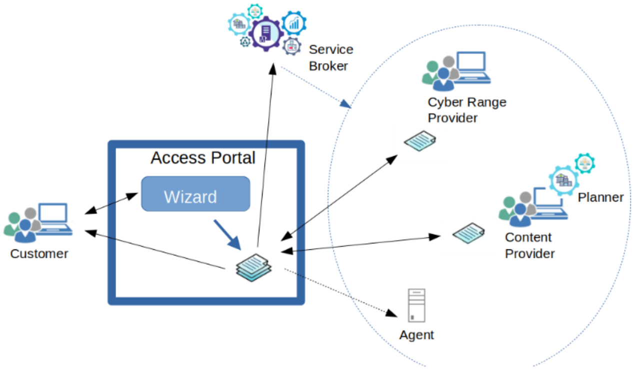


Figure 4. An instance of collaboration articulated around an ESDL service description file

The Service Designer automatically checks the designed Service for semantic correctness, thanks to the ESDL grammar. The Cyber Range and Content Providers (not Customers) have also the possibility to assign their capabilities to the designed Service. This way the Service is complete from the system point of view and can be scheduled via Service Broker.

B. Validation, approval and suggestions

At its core, the E-FCR platform is designed to process a Customer's Service Request in regards to the availability of resources on the side of the Cyber Range Providers and validate the existence of availability - in which case the reservation of required resources and the deployment of the requested Service is carried out - or provide suggestions in the case of a custom designed Service Request.

The task of validating and deploying a Service Request is mainly reserved for the **Service Broker** which needs to work in concert with other integral backend components like the Service Request Repository, Capacity & Capability Map, User Manager, Billing Manager, and Broker Gateway.

In the first stage, following the submission of an off-the-shelf Service Request to the Service Broker, the validation process is executed. During that process, Service Broker fetches relevant Cyber Range data from **Capacity & Capability Map** and **User Manager** and validates the availability of the Service-requested Resources for either a single Provider or an existing Federation of Providers. Resource availability is determined at runtime by utilising the Capacity & Capability Map resource and reservation data. Several constraints are taken into account like schedule availability, and Capability availability for each Service-designated Cyber Range.

In case of a successful Service Request validation, Service Broker creates a Proposal that is then submitted to the Service Request Repository and is updated by the **Billing Manager** with necessary financial data. Service Request status is also updated by the Service Broker to reflect the successful validation. The created Proposal can be queried and viewed by both the Customer and the Service Provider on the E-FCR Dashboard where it is negotiated. Following an unsuccessful Service Request validation due to resource unavailability, Service Broker creates an empty Proposal and updates the Service Request status accordingly to initiate a Service Request customisation process or a cancellation.

In case of Customer-designed Service Request (designed from scratch), Service Broker utilises several methods like template-capability matching and semantic string matching against Cyber Range Capability data in order to best fulfil the Customer's request and create a list of Proposals for each Provider/Federation. Since the Service in this case is system-designed, it needs to be carried out in phases for: (i) Single Providers; (ii) Existing Federations; and (iii) possible creation of new Federations. If a Proposal is accepted by a Provider or a Federation, the aforementioned actions are executed to proceed with resource reservation and Service deployment. If none of the Proposals is accepted, the Service Request is updated to a DRAFT status and Customer intervention is required.

After successful validation, negotiation, and approval of an off-the-shelf or a designed-from-scratch Service Request, the Service deployment process is executed. During that process, Service Broker first reserves the Cyber Range resources, defined in the accepted Proposal, by notifying the Capacity & Capability Map component. Following resource reservation, Service Broker initiates service deployment by notifying each involved Cyber Range through **Broker Gateway** with relevant data. The described process is executed in the backend where every component utilises authorisation for data access and modification to ensure data safety and user-data privacy.

C. Deployment

Once the start date of the cyber-service is reached, Provider can deploy the service on cyber ranges by leveraging E-FCR. This is especially helpful considering a federated service running on multiple cyber ranges. E-FCR sends an activation request to every involved cyber range, to a special cyber range agent which receives the request and translates it to the cyber range specific API calls, thus instantiating the corresponding part of the federated scenario. The federated scenarios running on different cyber ranges are interconnected via VPN VM.

VPN VM allows to interconnect two cyber ranges with client to server Layer 3 virtual private network (VPN). The VPN software and its configuration are contained within a virtual machine on both client and server side of this point-to-point connection. VPN VM technology is agnostic to the virtualisation technology used by the cyber range itself. A VPN tunnel is established between two scenarios running on different cyber ranges. VPN VM acts as a server in one cyber range scenario and as a client in the other cyber range scenario. If a scenario is federated across N cyber ranges, the number of VPN VM tunnels can grow up to [N*(N-1) / 2] (full-mesh).

D. Training Exercise

We now consider an actual training scenario based on a cyber exercise for energy sector, consisting of power generation operators each with a corporate network, physical security, and ICS. Within this scenario, an Advanced Persistent Threat is intent on disrupting power generation to cause political destabilisation. The attacker's objective is not destruction, but untraceable disruptions at various energy suppliers that cause cascading effects and result in outages. Different electricity generation plants are targeted, and they must work together to detect, identify, contain, and recover from the cyber-attacks.

The scenario uses capabilities from three cyber ranges available at VisionSpace (VS), RHEA (RG), and Guardtime (GT), respectively. The three cyber ranges easily integrate their capabilities to bring specialty knowledge to play in the delivery of more complex and realistic simulations. Thanks to the scenario structure, only 4 VPN VM machines are necessary for the scenario interconnection; see Figure 5.

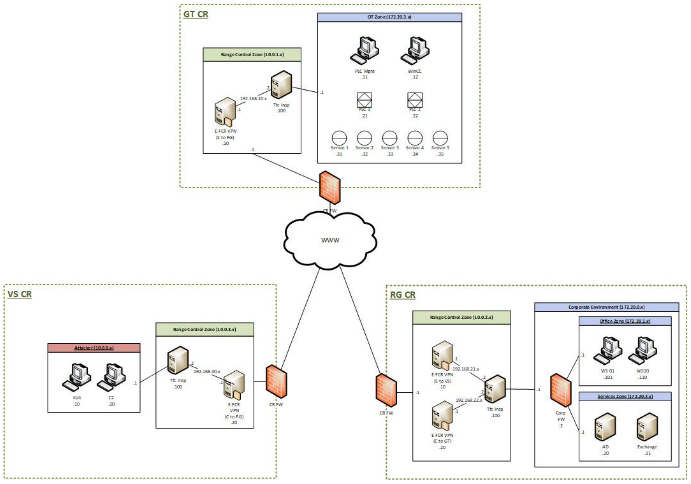


Figure 5. Network diagram of the training scenario

V. Conclusions

Motivated by the increasing importance of cyber ranges for a multitude of purposes and the need for the federation of individual cyber ranges, this work presented the ECHO - Federated Cyber Range that aims to interconnect existing cyber range capabilities through a convenient portal operating as a "broker" between user requirements and a pool of available cyber range capabilities. We presented the main features of the E-FCR, an in-depth view of its architecture, and finally the complete life-cycle of a scenario within E-FCR, starting from its design, validation, and approval, until its deployment.

Acknowledgment

This work was supported by the ECHO project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830943.

References

[1] Holm, H., Karresand, M., Vidström, A., & Westring, E. (2015, October). A survey of industrial control system testbeds. In Nordic Conference on Secure IT Systems (pp. 11-26). Springer, Cham.

[2] Kucek, S., & Leitner, M. (2020). An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. Journal of Network and Computer Applications, 151, 102470.

[3] Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636.