

DIGITAL-ECCC-2022-CYBER-B-03-
CYBER-RESILIENCE



This project has received funding from the European Union's DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE programme under grant agreement No 101145872.

Connected 5G-IoT Cyber Range for Training and Secure Operations



WP2 – Requirements Analysis and Architecture Definition

Deliverable D2.3

“Technical, legal, policy requirements and use case scenarios - second version”

Editor(s): UBI

Author(s): Christos Xenakis (UPRC), Nikitas Marinos Sgouros (UPRC), George Eftymoglou (UPRC), Kantikyan Araksya (UNILU), Anastasios Tzoumpas (UBI), Konstantinos Poulakakis (UBI), Ioannis Siachos (UBI), Christoforos Ntantogian (IURC), Stylianos Karagiannis (IURC), Emmanouil Magkos (IURC), Konstantinos Oikonomou (IURC), Tsitsoula Styliani (HCSI), Antony Vamvakaris (HCSI), George Mylonas (HCSI)

Dissemination Level: PU - Public

Type: R — Document, report

Version: 1.0

Project Profile

Contract Number	101145872
Acronym	NITRO
Title	Connected 5G-IoT Cyber Range for Training and Secure Operations
Start Date	Jan 1 st , 2024
Duration	36 Months

Partners

1	 UNIVERSITY OF PIRAEUS	University of Piraeus Research Center	Greece
2		UNISYSTEMS LUXEMBOURG SARL	Luxembourg
2.1		UNI SYSTEMS SYSTIMATA PLIROFORIKIS MONOPROSOPI ANONYMI EMPORIKI ETAIRIA	Greece
3		IONIAN UNIVERSITY	Greece
4	 HCSI HELLENIC CYBERSECURITY INSTITUTE	HELLENIC CYBERSECURITY INSTITUTE	Greece
5		UBITECH LIMITED	Cyprus

Document History

VERSIONS

Table 1: Document history

Version	Date	Author	Remarks
0.1	22/10/2024	UBI	Initial ToC and assignments
0.2	27/11/2024	UBI	Alignment with D2.1, additional content to various sections and updated structure
0.3	29/11/2024	UBI	Additional content to various sections.
0.4	4/12/2024	UBI, UPRC, UNI LU, IURC, HCSI	Additional content to various sections.
0.5	11/12/2024	UBI	Additional content to various sections.
0.6	12/12/2024	UBI, UPRC, UNI LU, IURC, HCSI	Additional content to various sections. Draft ready for review.
0.7	19/12/2024	UBI	Content refinement based on partners' feedback.
0.8	20/12/2024	UBI	Content refinement based on partners' feedback.
0.9	23/12/2024	UBI	Content refinement based on partners' feedback.
1.0	31/12/2024	UBI	Final version.

Table of Contents

Table of Tables	6
Table of Abbreviations	7
Executive Summary	9
1 Introduction	10
1.1 Overview of Deliverable Scope	10
1.2 Methodology followed in the document	11
1.3 Structure of the document	12
1.4 Relation with other WPs	13
1.5 Updates from the First Version	14
2 Vision of NITRO towards a Cyber-Range Ecosystem	15
3 5G Threat Landscape	17
3.1 Security challenges of 5G mobile networks	17
3.2 Attacks in 5G Networks	18
3.2.1 Distributed Denial of Service (DDoS) Attacks	19
3.2.2 Rogue Base Stations	19
3.2.3 Network Slicing Attacks	19
3.2.4 IoT Device Compromises	20
3.2.5 Virtualization Layer Attacks	20
3.2.6 Advanced Persistent Threats (APTs)	21
3.3 Adversarial & Robust AI	21
3.3.1 Adversarial AI in 5G Networks	21
3.3.2 Robust AI for 5G Networks	23
3.4 Incident Response in 5G Networks	24
3.4.1 Incident Response Steps	24
3.4.2 5G-Tailored Incident Response Playbooks	26
4 Gamification and Learning	28
4.1 Gamification in Cybersecurity Education	28
4.2 Learning Analytics	29
4.2.1 Privacy issues in learning analytics	29
5 Legal and Policy Aspects	31
5.1 Relevant Legal and Policy Frameworks and Compliance	31
5.1.1 Compliance with EU and international laws	31
5.1.2 Data protection and privacy laws	34
5.1.3 Industry-specific regulations	35
5.1.4 Intellectual property and licensing	35
6 Requirements for NITRO Cyber-Range Ecosystem	37
6.1 Final Methodology for Requirements Elicitation	37

6.2	Functional & Technical Requirements.....	37
6.2.1	NITRO Cyber-Range Requirements	37
6.3	Engineering Stories	39
6.3.1	5G Attack Scenarios of NITRO Cyber-Range platform	40
6.3.2	5G Incident Response of the NITRO Cyber Range.....	45
6.3.3	Adversarial & Robust AI Training Scenarios of NITRO Cyber-Range	48
6.3.4	Privacy Preserving Learning Analytics in NITRO Cyber Range.....	49
6.3.5	Gamification and Scoring System of NITRO Cyber-Range	50
6.3.6	NITRO Cyber Range Implementation.....	52
6.3.7	Legal and Policy framework for NITRO Cyber Range.....	54
6.4	Mapping Requirements to Engineering stories and NITRO's System Architecture	55
7	NITRO 5G Cyber Range Implementation Aspects	58
7.1	Building Blocks for the NITRO Cyber-Range	58
7.1.1	Virtualization with containers	58
7.1.2	Emulation of 5G Core network.....	59
7.1.3	Emulation of devices and radio network.....	59
7.1.4	5G Traffic generator and Attack Simulation.....	60
7.1.5	NITRO data repository of 5G and IoT attacks	60
7.1.6	Security Tools for Incident Detection	60
7.2	NITRO Cyber Range Platform	62
7.2.1	KPIs Discussion	62
8	Use Case Scenarios.....	64
8.1	Use Scenario 1: Cybersecurity Testing of 5G and IoT Applications and Network Services.....	64
8.2	Scenario 2: Security Training for ECSC.....	66
9	Conclusions	70
	References	72



Table of Tables

Table 1: Document history.....	3
Table 2: Identified Requirements	38
Table 3: Requirements to Engineering Stories Mapping	55
Table 4: Identified NITRO KPIs	62
Table 5: Use case description template	64
Table 6: Use Case Scenario UC1.1 (Cybersecurity Fundamentals and Incident Response)	65
Table 7: Use Case Scenario UC1.2 (Threat Detection and Mitigation)	65
Table 8: Use Case Scenario UC1.3 (Critical Infrastructure and Emerging Threats).....	66
Table 9: Use Case Scenario UC2.1 (Familiarize with the 5G Technology).....	67
Table 10: Use Case Scenario UC2.2 (Interact with the 5G Core)	68
Table 11: Use Case Scenario UC2.3 (Perform an Attack on the 5G Core)	68

Table of Abbreviations

Abbreviation	Explanation
5G	5 th Generation
6G	6 th Generation
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
API	Application Programming Interface
APTs	Advanced Persistent Threats
C&C	Command and Control
CSIRT	Computer Security Incident Response Team
CU	Centralised Unit
DDoS	Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
ES	Engineering Story
EU	European Union
EUCC	European Cybersecurity Certification Scheme
FAIR	Findable, Accessible, Interoperable, and Reusable
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IDS	Intrusion Detection Systems
ISO	International Organization for Standardization
IMSI	International Mobile Subscriber Identity
IOC	Indicators Of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention Systems

LMS	Learning Management Systems
MANO	Management orchestration
MitM	Man-in-the-Middle
ML	Machine Learning
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output
MVP	Minimum Viable Product
NF	Network Function
NIS2	Network and Information Security Directive 2
NFV	Network Function Virtualization
NFVO	NFV Orchestration
NWDAF	NetWork Data Analytics Function
OSM	Open Source MANO
PII	Personally Identifiable Information
QoS	Quality of Services
RAN	Radio Access Network
RCE	Remote Code Execution
ROs	Research Objectives
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SOC	Security Operations Centre
TTPs	Tactics, Techniques, and Procedures
UPF	User Plane Function
VNFs	Virtual Network Functions

Executive Summary

Deliverable D2.3, titled "Technical, Legal, Policy Requirements and Use Case Scenarios – Second Version," sets the stage for the NITRO project by laying down a comprehensive framework essential for the development of a Cyber-Range ecosystem tailored to 5G networks. This deliverable consolidates the technical, legal, and policy requirements while outlining potential use case scenarios that will drive the project's progression. The document begins with an overview of the NITRO project's vision for a Cyber-Range ecosystem, emphasising the need for innovative approaches to address the unique challenges posed by 5G technology.

A significant portion of the deliverable is dedicated to exploring the role of adversarial AI within the 5G ecosystem. This section assesses the potential threats posed by AI-driven attacks and proposes strategies for mitigating these risks, thereby ensuring the resilience of 5G networks against sophisticated cyber threats. In constructing a privacy-preserving Cyber-Range platform, the deliverable outlines key mechanisms to ensure data protection and compliance with relevant privacy laws. This platform will provide a secure environment for conducting cybersecurity training and evaluations, without compromising on data privacy. Additionally, NITRO will provide 5G incident response playbooks, detailing procedures and best practices for managing and mitigating security incidents within 5G networks, thus enhancing the preparedness and responsiveness of cybersecurity teams. The enhancement of the Cyber-Range ecosystem with evaluation metrics for both offensive and defensive strategies is another critical aspect covered in this document. These metrics will provide meaningful insights into the effectiveness of various cybersecurity practices, facilitating continuous improvement.

Legal and policy requirements are thoroughly addressed, ensuring that the Cyber-Range ecosystem complies with EU and international laws, as well as industry-specific regulations. This section underscores the importance of legal compliance and data protection, which are vital for the credibility and acceptance of the Cyber-Range platform. The deliverable also outlines the requirements for creating a proof-of-concept environmental testbed, which will be used to validate the effectiveness and practicality of the Cyber-Range ecosystem. This testbed will play a crucial role in demonstrating the feasibility and robustness of the proposed solutions. Finally, the document details the NITRO methodology for defining use cases and developing a Minimum Viable Product (MVP) within the project framework. This methodology ensures a structured and iterative approach to development, aligning with the overall project goals.

In conclusion, Deliverable D2.3 provides a detailed and holistic framework that will guide the subsequent phases of the NITRO project. By addressing technical, legal, and policy requirements and by proposing realistic use case scenarios, the deliverable provides a strong foundation for the successful development and implementation of a 5G tailored Cyber-Range ecosystem.

1 Introduction

1.1 Overview of Deliverable Scope

The primary objective of Deliverable D2.3, titled "Technical, Legal, Policy Requirements and Use Case Scenarios - Second Version," is to establish a comprehensive foundation for the development and implementation of a robust Cyber-Range ecosystem tailored to 5G networks. This deliverable is an integral component of the NITRO project, which aims to enhance cybersecurity capabilities through the creation of advanced tools and methodologies.

This deliverable encompasses technical, legal, and policy aspects crucial to the successful implementation of the NITRO project. It provides a comprehensive roadmap for developing a secure, resilient, and legally compliant Cyber-Range ecosystem tailored to the specific needs of 5G technology. By addressing these multifaceted requirements, the deliverable aims to lay a strong foundation for subsequent project phases and ensure the achievement of NITRO's strategic objectives.

As the second version of the NITRO functional specifications and technical requirements, this document will guide all subsequent implementation activities. It is important to note that the dynamic nature of the project necessitates a flexible approach, allowing for refinements and updates as new insights and advancements emerge.

The core outcome of this deliverable is the requirements and accompanying functional specifications described through engineering stories (ES). These stories, framed from the perspective of various stakeholders, provide clear and actionable requirements for the development team. For instance, an engineering story might be articulated as follows: "As a stakeholder, I want to ensure that the Cyber-Range can simulate complex 5G attack scenarios to test and enhance our security protocols." These stories are essential for translating high-level objectives into specific, measurable tasks that drive the project's progress.

Engineering stories are a fundamental component of the NITRO project's deliverables, providing a structured approach to defining and capturing the technical requirements and functional specifications necessary for the successful implementation of the Cyber-Range ecosystem. These stories are articulated from the perspective of various stakeholders, ensuring that their needs and objectives are clearly understood and addressed. By framing requirements in this user-centric manner, the NITRO project can translate high-level goals into actionable tasks that guide the development process.

Each engineering story is designed to convey specific functionalities or capabilities that the Cyber-Range must possess. They typically follow a standard format: "As a [stakeholder], I want [functionality] so that [goal]." This format helps to clarify the purpose and importance of each requirement, making it easier for the development team to prioritize and implement them effectively.

In the context of the NITRO project, engineering stories play a crucial role in ensuring that the Cyber-Range ecosystem is not only technically robust but also aligned with the practical needs of its users. By continuously refining these stories through ongoing discussions and feedback, the project remains

adaptable and responsive to new insights and emerging challenges in the 5G landscape. The following section outlines the core engineering stories that form the foundation of the NITRO project's functional specifications.

By incorporating technical, legal, and policy considerations, this deliverable ensures that the NITRO project not only meets its technical goals but also adheres to regulatory standards and aligns with best practices in cybersecurity. The detailed roadmap included in this document outlines the necessary steps for creating a robust Cyber-Range ecosystem, addressing potential challenges, and proposing solutions to mitigate risks.

In summary, this deliverable sets the stage for the NITRO project's success by providing a clear and detailed plan that integrates technical requirements with legal and policy considerations. It establishes a framework for ongoing development, ensuring that the project remains adaptable and responsive to new challenges and opportunities in the rapidly evolving landscape of 5G technology.

1.2 Methodology followed in the document

Considering the evolving landscape in Cybersecurity and the project's objectives, we tried to clarify the vision and requirements for the development of a state-of-the-art Cyber-Range ecosystem. We structured the vision along three main pillars; a) the relevant threat landscape, b) the legal and privacy legislation, c) the gamification aspects for cyber range. We provided an analysis based on those pillars and then continued with the collection of requirements.

The requirements collection exercise and the relevant engineering stories presented in this document have evolved in alignment with the key principles identified through this analysis and the needs of the use cases. Finally, we tried to elaborate on a prioritization plan that can assist us in the timely design and implementation of NITRO MVP.

In essence the following are the main points of the deliverable:

Step 1: Define the Vision for a Cyber-Range Ecosystem:

- Present the overarching vision of NITRO for developing a state-of-the-art Cyber-Range ecosystem that can address the unique challenges and requirements of 5G and IoT technology.
- Detail the innovative approaches and strategic goals that will guide the development and deployment of this ecosystem.

Step 2: Analyse Cybersecurity Aspects

- **Build a 5G Tailored Attack Scenarios:**
 - Identify and analyse potential cyber threats specific to the 5G core and far edge networks.
 - Develop comprehensive attack scenarios to simulate these threats, providing a realistic training and testing environment.
- **Develop a 5G Incident Response Playbook:**

- Create a tailored incident response framework for addressing security incidents within 5G networks.
- Outline procedures and best practices for effective incident management and mitigation.
- **Explore Adversarial AI in 5G Context:**
 - Investigate the role and impact of adversarial AI within the 5G ecosystem.
 - Assess the threats posed by AI-driven attacks and propose defensive strategies to mitigate these risks.

Step 3: Analysis of Legal and Privacy Aspects

- **Address Legal and Policy Requirements:**
 - Ensure compliance with EU and international laws, as well as data protection and privacy regulations.
 - Review industry-specific regulations and integrate them into the Cyber-Range framework.
- **Construct a Privacy-Preserving Mechanism for Learning Analytics:**
 - Design a mechanism that ensures privacy and data protection of learning analytics.
 - Comply with relevant data protection and privacy laws.

Step 4: Gamification Aspects

- **Enhance Cyber-Range Ecosystem with Gamification and Scoring Metrics:**
 - Establish metrics for evaluating both offensive and defensive cybersecurity strategies within the Cyber-Range environment.
 - Introduce gamification elements tailored to a 5G cyber range.

Step 5: Steps for Proof of Concept and MVP development

- **Define Proof of Concept Environmental Testbed Requirements:**
 - Outline the requirements for creating a testbed environment that can validate the Cyber-Range ecosystem's effectiveness and practicality.
- **Detail NITRO Methodology for Minimum Viable Product (MVP):**
 - Describe the methodology for defining use cases and developing an MVP within the NITRO framework.
 - Ensure the methodology aligns with project goals and facilitates efficient, iterative development.

1.3 Structure of the document

The structure of deliverable D2.3 is organized in the following structure:

- Chapter 2 presents the overall vision,
- Chapter 3 presents the threat landscape with focus on 5G domain,
- Chapter 4 focuses on the gamification aspects,
- Chapter 5 presents an analysis on the legal and privacy landscape,
- Chapter 6 presents the aggregated view of the requirements, the user stories and also how

they align to the architecture as outlined in D2.2,

- Chapter 7 presents an initial version of the platform concept and candidate technologies,
- Chapter 8 presents the use case scenarios that will be further elaborated in WP5 and will be used for the evaluation of the NITRO platform,
- Chapter 9 concludes the document.

1.4 Relation with other WPs

Deliverable D2.3, plays a pivotal role in providing essential inputs to several other work packages (WPs) within the NITRO project. Its comprehensive analysis and detailed framework serve as the foundational bedrock upon which other WPs will build and refine their specific contributions to the overall project objectives.

Contribution to WP3: Cyber Security Training Exercises

The detailed attack scenarios and the 5G tailored threat playbook provided in D2.3 are crucial for WP3, which focuses on designing and implementing cyber security training exercises. These scenarios will enable WP3 to create training modules that accurately reflect potential real-world threats to 5G networks. The in-depth analysis of threats to the 5G core and far edge networks outlined in D2.1 and D2.3 will guide the development of realistic and effective training exercises, ensuring that participants are well-prepared to handle a variety of cyber incidents.

Contribution to WP4: Scoring System and Gamification

For WP4, which is centred on the development of a scoring system and the incorporation of gamification elements into the Cyber-Range ecosystem, D2.3 offers invaluable insights. The evaluation metrics for both offensive and defensive strategies detailed in this deliverable will serve as the foundation for creating a robust scoring system. Additionally, the threat playbook and attack scenarios will provide context for gamification, helping to design challenges and scoring criteria that are engaging, educational, and reflective of actual cyber security challenges in a 5G environment.

Contribution to WP5: Demonstration and Evaluation

WP5, which focuses on the demonstration and evaluation of the Cyber-Range platform, will significantly benefit from the groundwork laid out in D2.3. The deliverable's comprehensive methodology for use case definition and the creation of an MVP within the NITRO framework will guide WP5 in setting up effective demonstration scenarios. Furthermore, the privacy-preserving mechanisms and compliance strategies detailed in D2.3 will ensure that the demonstration environments adhere to relevant legal and policy requirements, enhancing the credibility and reliability of the evaluation processes.

In summary, D2.3 is integral to the success of WP3, WP4, and WP5, providing essential information and frameworks that these work packages will leverage to achieve their specific goals within the

NITRO project.

1.5 Updates from the First Version

Since the publication of **Deliverable D2.1**, several key updates have been made to enhance the framework and scope of the NITRO Cyber-Range ecosystem:

1. Refinement on the landscape analysis on threats, gamification and legal aspects.
2. Updates on the engineering stories:
 - Added advanced scenarios focusing on cascading IoT-5G attack interdependencies and adversarial AI, which were less detailed in D2.1.
 - Strengthened alignment with WP3 and WP4 through updated engineering stories that now explicitly detail the integration of these scenarios.
3. Collection of Requirements and mappings to engineering stories and preliminary architecture from D2.2.
4. Definition of Use Case Scenarios for the demonstrations (section 8).
5. Updates on the identified implementation aspects:
 - Refined the architecture of the proof-of-concept testbed, incorporating additional tools for attack emulation, advanced data analytics, and network traffic simulation.
 - Added components for simulating privacy and security policies in training exercises.
6. Updates on document structure for improved readability after receiving feedback on D2.1.

These updates ensure that the second version of the deliverable provides a more robust and comprehensive foundation for the subsequent phases of the NITRO project.

2 Vision of NITRO towards a Cyber-Range Ecosystem

NITRO aims to increase the knowledge and capacity of the EU to cope with the complex security challenges posed by the convergence of 5G and IoT technologies. This is a key motivation behind the project, as evidenced by the growing number of cybersecurity threats targeting 5G systems [1]. The convergence of 5G and IoT creates a complex environment that requires enhanced knowledge and capabilities within the EU to effectively secure these interconnected systems. Aligned with the European Commission's strategic goals, particularly the NIS and NIS 2 Directives¹, NITRO will deliver a state-of-the-art 5G cyber range. This enhances security for 5G and other critical infrastructures through training on complex and cascading attacks.

Most cyber ranges in the market focus on cybersecurity for computer networks targeting OS vulnerabilities (Windows, Linux) since these OS are used by most users while cyber ranges for critical infrastructures are in infancy [2]. One exception is SPIDER², a cyber range for 5G security [10]. While it is considered one of the first 5G cyber ranges, the functionality of the SPIDER cyber range is rather limited as it considers 5G networks mainly as the access medium and not the target. NITRO goes well beyond the existing state-of-the-art maintaining a holistic security approach of 5G environments across multiple layers. The added value from NITRO lies on the delivery of a novel cyber range that can simulate and evaluate the security of 5G systems. This includes educational scenarios for identifying and mitigating potential cascading attacks that can exploit the interdependencies between devices, systems, and network elements in 5G networks and with external networks such as IoT.

NITRO provides a platform for researchers and security professionals to simulate real-world scenarios, assess vulnerabilities, and validate security measures. Not only it focuses on cybersecurity attacks, but also includes adversarial AI exercises on 5G networks to highlight AI vulnerabilities and defences. In particular, NITRO focus on adversarial AI attacks and their mitigation techniques (also known as robust AI), contributing to the emerging field of AI and cybersecurity [4]. The NITRO project focuses on creating realistic training scenarios that simulate both AI adversarial attacks and defensive strategies within 5G environments. By doing so, it provides a comprehensive platform for cybersecurity professionals to develop and test robust AI strategies, ensuring the security and reliability of AI applications in these advanced networks. The overarching goal is to enhance the security of AI as applied in 5G networks and help develop new cyber ranges that will focus exclusively on AI security. In this way, NITRO aligns with the AI Act's objectives of promoting safe and transparent AI use and promotes ENISA guidelines on the security of AI models as documented in various reports:

- Cybersecurity of AI and Standardisation³

¹ <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

² <https://spider-h2020.eu/>

³ <https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation>

- Artificial Intelligence and Cybersecurity Research⁴

Moreover, cyber ranges in the market have a strong focus on the offensive side of cybersecurity, giving a second priority on the defence [2]. This contributes to the identified skills gap in cybersecurity, a well-studied issue. NITRO will provide contributions to the defensive side of cybersecurity by defining incident response playbooks specifically designed for 5G networks. These playbooks provide structured procedures for managing cybersecurity incidents, addressing the complexities of 5G technology, such as network slicing and virtualization. They ensure effective responses to minimize security impact, enhancing the preparedness and coordination of cybersecurity blue teams. By utilizing the NITRO cyber range for realistic defensive scenarios, professionals can practice and refine their skills in incident handling, improving the resilience and security of 5G networks.

Another innovative feature of the NITRO project focuses on implementing privacy-preserving techniques for learning analytics [5]. This approach ensures that the benefits of learning analytics can be fully realized while protecting the privacy of all users involved, thereby enhancing the overall effectiveness and ethical standards of cybersecurity education. By prioritizing data privacy, NITRO not only complies with regulatory standards but also fosters a culture of security and respect for personal information within the training ecosystem. NITRO aims to build trust among participants and data sharing procedures creating a secure environment for conducting cybersecurity training.

Finally, the scarcity of 5G data repositories poses a significant challenge for cybersecurity training and research, as comprehensive datasets are essential for understanding and mitigating emerging threats. NITRO project addresses this gap by compiling detailed information on various attack types and scenarios. In this way, NITRO not only facilitates the development of realistic training environments but also supports ongoing cybersecurity research strengthening the overall security posture of 5G networks. Utilizing open standards like XML and JSON, the NITRO knowledge repository will facilitate knowledge transfer and big data analytics through an open-data access policy. The repository will be shared with existing European ISACs⁵ and specifically with the Cyber Information and Intelligence Sharing Initiative (CIISI-EU).

⁴ <https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research>

⁵ <https://www.isacs.eu/european-isacs>

3 5G Threat Landscape

In this section we provide an overview of the threat landscape in the 5G domain, in order to understand the cybersecurity needs and the capabilities that the NITRO cyber range should offer.

3.1 Security challenges of 5G mobile networks

5G mobile networks offer several new services that enhance speed, connectivity and reliability, enabling innovative and data-centric applications such as real-time data processing and analysis [6]. 5G technology represents a significant evolution in mobile network architecture, transitioning from hardware-dependent systems to a more flexible and scalable software-centric approach. Previous generations of mobile networks relied heavily on dedicated hardware to support core network functions. In contrast, 5G introduces a software-defined architecture that leverages virtualisation and cloud computing technologies to achieve these functionalities.

At the heart of 5G's architectural transformation are Software-Defined Networking (SDN) and Network Function Virtualization (NFV) [7]. SDN technology decouples the control plane from the data plane, thereby simplifying network management and administration. It achieves this by separating the routing and forwarding decisions of networking elements, such as routers and switches, from the actual data transmission. NFV complements SDN by virtualising network functions that traditionally run on dedicated hardware. This virtualisation allows network services to run on standard server hardware, decoupling capacity (processing, storage, data transport) from functionality (filtering, analysing, forwarding, balancing). NFV Orchestration (NFVO) plays a critical role in coordinating these virtualised resources, ensuring efficient and scalable network operations. The combination of SDN and NFV provides the foundation for 5G networks, enabling dynamic and flexible service deployment.

However, new technologies introduced in 5G can lead to opportunities for new attack vectors which are not well studied [1]. As a matter of fact, this software-centric approach introduces new security challenges across all layers of the network. By decomposing applications into different layers within the compute continuum, we expose additional potential attack surfaces that must be diligently protected. The increased complexity of virtualised environments means that cyber attackers can exploit vulnerabilities not just at the application level but throughout the entire infrastructure.

By enabling multi-tenancy and support for multiple services and in a dynamic manner, network slicing has evolved into a fundamental concept in 5G. At the same time, it constitutes an opportunity for new types of threats, such as time impersonation attacks against the network slice manager or network slice instances. The provision of different security protocols and policies in different slices may also produce new challenges, accentuated by the multi-tenant nature of 5G. Apart from network slicing, another important feature of 5G networks is related to the fact that the 5G Core functions are meant to be largely composed of applications running on general purpose hardware that communicate through application programming interfaces (APIs). The integrity of the software, especially from open-source locations and the overall software supply chain, is an area of vulnerability. As services can be created, destroyed, and communicate with each other dynamically, systems must be properly authenticated, and communications protected in order to prevent unauthorized execution of

functions or access to data.

Attacks on 5G Far edge are of particular interest, since they can lead to cascading effects where a single breach can compromise multiple layers, significantly increasing the complexity and impact of the attack [8]. Far edge refers to the outermost boundary of the network where data processing and analytics occur close to the source of data generation. This proximity to data sources enables low-latency processing and real-time decision-making, making it ideal for applications such as Internet of Things (IoT), industrial automation, and autonomous vehicles. At the far edge, computing resources are deployed in close proximity to end devices, such as IoT sensors and actuators. This infrastructure includes edge servers, gateways, and network appliances capable of processing and analysing data locally. 5G networks provide ultra-low latency connectivity to devices at the far edge, enabling real-time data transmission and response.

Usually far-edge devices are the target of attacks since they are outside the control of an administrative domain which means that the Orchestrator might not know a priori which security mechanisms are deployed. Hence, it is crucial to also add this as part of the cyber-range activities – especially with the current trend of deploying service resources closer to the edge through MEC deployments [8]. By providing connectivity to an unprecedented number of small and insecure IoT devices, 5G networks may experience high occurrence of security breaches either originating from these devices or targeting them to cause adverse effects. The potential large-scale impact caused by remotely controlling or passively monitoring a large number of IoT devices will be very attractive to escalating cyber threats.

Therefore, it is crucial to implement robust security measures at every layer of the virtualised network infrastructure. This includes strong authentication to verify identities, stringent access controls to limit permissions, and continuous monitoring to detect and respond to suspicious activities promptly. Additionally, providing mechanisms to enhance the understanding of these attacks is vital. By educating security practitioners about the intricacies of these complex attack vectors and the potential cascading effects, we can better prepare them to defend against and mitigate these threats effectively. Robust security layers, combined with comprehensive training and awareness, form the foundation of a resilient 5G network infrastructure. Based on the above, it becomes clear that better training techniques are needed covering all layers of the 5G/6G ecosystem. Because currently we have mechanisms focusing on specific layers.

3.2 Attacks in 5G Networks

The unique architecture and advanced capabilities of 5G networks introduce new types of attacks and expand the potential impact of cyber threats. Understanding them in detail is crucial for developing effective incident response strategies. The following scenarios provide examples of potential attacks that illustrate the diverse range of threats 5G networks may face. Please note that this is not an exhaustive list; a more specific and detailed enumeration of incidents will be provided in version 2 of this document.

3.2.1 Distributed Denial of Service (DDoS) Attacks

DDoS attacks involve overwhelming a network, service, or server with a massive amount of traffic to render it unavailable to legitimate users. In the context of 5G, the increased number of connected devices amplifies the potential scale and impact of these attacks.

Specific Attack Vectors:

- **IoT Botnets:** Compromised IoT devices can be hijacked to form large botnets that launch coordinated DDoS attacks.
- **Amplification Attacks:** Attackers exploit vulnerable network services to amplify the volume of traffic directed at the target.
- **Resource Exhaustion:** Targeting specific network functions or slices to exhaust their resources, causing service disruptions.

Impact: DDoS attacks can cause significant service outages, affecting millions of users and critical applications, leading to substantial financial and reputational damage.

3.2.2 Rogue Base Stations

Rogue base stations, also known as fake base stations or IMSI catchers, are unauthorised devices that mimic legitimate cellular towers. They can intercept, eavesdrop, and manipulate communications between mobile devices and the network.

Specific Attack Vectors:

- **IMSI Catching:** Capturing International Mobile Subscriber Identity (IMSI) numbers to track and monitor users.
- **Man-in-the-Middle (MitM) Attacks:** Intercepting and altering communication between the user device and the network.
- **Denial of Service:** Disrupting communication by forcing devices to connect to the rogue station instead of legitimate ones.

Impact: Rogue base stations can compromise user privacy, steal sensitive information, and disrupt communication services. They pose a significant threat to both personal and enterprise security.

3.2.3 Network Slicing Attacks

Network slicing allows 5G networks to create multiple virtual networks on a single physical infrastructure, each tailored to specific requirements. Attacks on network slices can target the isolation and resource allocation mechanisms, compromising the security and performance of individual slices.

Specific Attack Vectors:

- **Isolation Breach:** Exploiting vulnerabilities to move laterally across slices, accessing data and services meant for other slices.
- **Resource Hijacking:** Manipulating resource allocation to deprive legitimate slices of necessary bandwidth and processing power.
- **Service Disruption:** Targeting critical slices dedicated to essential services (e.g., emergency services, industrial IoT) to cause significant disruptions.

Impact: Network slicing attacks can lead to data breaches, service outages, and degraded performance for critical applications, undermining the reliability and security of 5G networks.

3.2.4 IoT Device Compromises

The proliferation of IoT devices in 5G networks increases the attack surface, as these devices often have limited security measures and can be easily compromised. Once compromised, they can be used as entry points for broader network attacks.

Specific Attack Vectors:

- **Firmware Exploits:** Exploiting vulnerabilities in IoT device firmware to gain control over the device.
- **Weak Authentication:** Taking advantage of weak or default passwords to access devices.
- **Malware Infection:** Deploying malware to IoT devices to create botnets or launch targeted attacks within the network.

Impact: Compromised IoT devices can be used to launch DDoS attacks, facilitate data breaches, or disrupt network services. They pose a significant risk due to their sheer number and widespread deployment.

3.2.5 Virtualization Layer Attacks

5G relies heavily on Network Function Virtualization (NFV) to deliver flexible and scalable network services. Attacks targeting the virtualisation layer can compromise multiple virtual network functions (VNFs) and disrupt service delivery.

Specific Attack Vectors:

- **Orchestrator Exploits:** Exploiting vulnerabilities in the orchestrator to gain control over multiple VNFs.
- **VNF Misconfiguration:** Exploiting misconfigurations to manipulate or disrupt virtual network functions.
- **Resource Contention:** Causing resource contention issues by overloading the virtualization infrastructure, leading to degraded performance or service outages.

Impact: Virtualization layer attacks can lead to widespread service disruptions, data breaches, and loss of control over network functions, severely impacting network reliability and security.

3.2.6 Advanced Persistent Threats (APTs)

APTs are sophisticated, long-term attacks conducted by well-resourced and skilled adversaries. These attacks aim to gain persistent access to networks and exfiltrate sensitive data or disrupt critical infrastructure over time.

Specific Attack Vectors:

- **Spear Phishing:** Targeting individuals within an organisation with carefully crafted phishing emails to gain initial access.
- **Exploiting Zero-Day Vulnerabilities:** Using unknown vulnerabilities to infiltrate and move laterally within the network.
- **Command and Control (C&C):** Establishing covert communication channels with compromised systems to maintain persistent control.

Impact: APTs can cause significant and long-lasting damage, including intellectual property theft, espionage, and disruption of critical infrastructure. They are particularly concerning for sectors such as defence, finance, and critical services.

3.3 Adversarial & Robust AI

In this section we present how AI affects cybersecurity through two distinct approaches; Adversarial AI and Robust AI.

3.3.1 Adversarial AI in 5G Networks

AI (and consequently adversarial AI) plays a crucial role in 5G networks serving different purposes. In 5G networks, AI (and adversarial AI) has been applied to various networking and operational functions of these networks. As mentioned in [9], AI can be utilised in 5G for:

- Channel estimation (e.g., AI estimates CSI of the whole time-frequency using the transmitted pilots),
- symbol detection (e.g., AI estimates the signal transmitted given the signal received and the CSI matrix),
- automatic modulation classification (e.g., AI performs classification based on sequences of the received signals and SNR),
- channel coding (e.g., AI searches for an optimal decoding strategy for binary linear codes or solves the decoding problem for convolutional and LDPC codes),
- beamforming (e.g., AI predicts the best beam based on a subset of RSS measurements or calculates optimal antenna diagrams for massive MIMO),
- activation control (AI searches for an optimal SBS activation strategy or selects sensor power mode for indoor localization),

- power allocation (e.g., AI develops a distributively executed dynamic power allocation scheme or learns to optimise interference management),
- scheduling (e.g., infers free slots in MF-TDMA networks or formulates the cooperative localization problem as multi-agent RL),
- routing (e.g., optimizing routing),
- caching (AI learns content cache priorities or finds optimal caching policy),
- slicing (e.g., AI proposes proactive dynamic network slicing scheme or resource allocation),
- security (classifies attack symptoms in jamming attacks).

In all the above AI applications, the adversarial counterpart can be executed to cause underperforming issues in the QoS of 5G networks [3]. Adversarial AI can be executed either in training or inference stage. Training stage attacks require access to datasets and/or model in order to modify the training procedure of AI models. This type of attack is hard to be mounted in 5G networks as threat actors typically do not have access to the AI training stage and related resources (e.g., datasets). As such, NITRO will focus on adversarial inference attacks. This type of attack is a more realistic threat to the AI models deployed in a 5G network since it takes place in the inference stage and, therefore, requires having access to neither the target model nor the datasets during the training. During such an adversarial example generation attack, the adversary aims to supply such input features to the target model that it outputs some wrong result. Adversarial examples in mobile networks are usually generated via adding carefully crafted radio signal perturbations. In this case, the adversary, as a rule, perturbs the samples on the decision boundary. This allows the attacker to increase the chance of the target model making an error. The algorithms for adversarial example generation usually fall into one of two main categories: white-box or black-box. In the former scenario, the adversary has access to the target model and, in some cases, even the data used for its training. In the latter case, the attacker is only capable of observing the labels returned by the model for the inputs provided, making the attack algorithms from this category more applicable in real-world use case scenarios.

In a 5G network system, white-box attacks during the inference stage would necessitate access to critical and internal network components, such as the centralised unit in the RAN, the network data analytics function, the management data analytics function and data storage centres. To achieve this, an adversary would need to initiate an eavesdropping or man-in-the-middle attack beforehand. These attack vectors are significantly harder to execute due to the defence mechanisms defined by 3GPP SA3. Therefore, we argue that in 5G networks, adversaries typically lack direct access to the target model, its input feature space, or its output labels. **Thus, black-box attack scenarios are more feasible in a 5G system**, as they are easier to be carried out by utilizing end users' equipment to send crafted signals.

IoT networks have their own specialized use of AI depending on the IoT system [11]. For instance, AI can be utilized for smart homes (optimize ventilation, heating, lighting and air conditioning systems based on occupancy patterns and external weather conditions to reduce energy consumption). Another example is in agriculture IoT, where machine learning models can predict optimal planting times and irrigation schedules based on weather and soil data. NITRO cyber range platform will utilise

a generic IoT network that utilizes AI for security purposes. That is, AI has been applied to an IoT-specific Intrusion Detection System, where the adversarial AI's goal is to attack the network in such a way as to avoid detection. Both training and inference attacks are feasible for the IoT use case (as opposed to 5G networks, which, as we mentioned above, only inferences are considered realistic).

3.3.2 Robust AI for 5G Networks

While adversarial AI focuses on creating and defending against intentionally crafted inputs designed to deceive AI models, robust AI aims to strengthen these models against a wide range of unpredictable and potentially harmful scenarios [12]. Robust AI techniques have become a critical focus in the literature to ensure that AI systems can perform reliably and securely in diverse and unpredictable conditions, especially in 5G and IoT networks. One prominent technique is adversarial training, which involves exposing AI models to adversarial examples during the training process. This method enhances the model's ability to recognize and defend against maliciously crafted inputs designed to cause errors. Ensemble learning is another technique where multiple AI models are combined to improve overall decision-making accuracy and robustness. By leveraging the strengths of various models, ensemble methods can better handle outliers and reduce the impact of any single model's weaknesses.

On the other hand, robust optimization techniques aim to improve the model's performance under worst-case scenarios. This involves optimizing the model to not just perform well on average but also to withstand the most challenging and unexpected inputs. Moreover, dropout and noise injection methods are used during training to prevent overfitting and to improve the model's ability to generalize from the training data to real-world scenarios. By randomly dropping units or adding noise to the input data, these techniques make the model less sensitive to specific features of the training data and more robust overall. Defensive distillation is another technique used in which a model is trained to predict the soft outputs (probabilities) of a more complex model rather than the hard labels. This can make the final model less sensitive to small perturbations in the input data. Finally, transfer learning can also enhance robustness by allowing models to leverage knowledge gained from one domain to improve performance in another, thus making them more adaptable to new and unseen environments.

In summary, robust AI techniques from the literature focus on making AI systems more resilient, adaptable, and secure. These techniques are essential for maintaining high performance and reliability in the complex and dynamic environments of 5G and IoT networks.

3.4 Incident Response in 5G Networks

Incident response in 5G networks requires a specialized approach due to the advanced capabilities and complexities introduced by 5G technology. Traditional incident response methodologies must be adapted to address the unique challenges of 5G, such as operation around the world, interconnection with service providers, increased connectivity with IoT devices. Below, we present a methodology based on five distinct steps and how the concept of incident response can be utilized in scenarios utilizing 5G networks.

3.4.1 Incident Response Steps

This chapter provides a comprehensive overview of the steps involved in incident response within 5G networks, emphasizing the specific requirements and best practices.

3.4.1.1 Identification and Detection

The identification and detection phases are critical for recognising potential cybersecurity incidents before they can cause significant harm. In 5G networks, this phase involves continuous monitoring and the use of advanced tools and techniques to detect anomalies and suspicious activities.

- **Real-time Monitoring:** Employ tools like SIEM for real-time monitoring and analysis of network traffic. These tools collect and correlate data from various sources across the network, providing a comprehensive view of network activity.
- **Anomaly Detection:** Implement Machine Learning algorithms to detect deviations from normal traffic patterns. Machine Learning algorithms can analyse large volumes of data in real-time, identifying unusual behaviours that may indicate a security incident. Anomaly detection can be used to combine predictions from multiple models to detect inconsistencies, enhancing the overall resilience against adversarial attacks. Special care should be taken for adversarial AI based attacks that can avoid detection. To this end, the robustness of the models should be considered to mitigate this class of AI attacks.
- **Threat Intelligence Integration:** Utilize threat intelligence feeds to stay updated on the latest threats and vulnerabilities. Integrating these feeds with monitoring tools can enhance the detection of known attack patterns and indicators of compromise (IOCs).
- **Automated Alerts:** Set up automated alerts to notify the incident response team of potential security incidents. These alerts should be based on predefined thresholds and rules that trigger when suspicious activities are detected.

3.4.1.2 Containment

The containment phase involves isolating the affected parts of the network to prevent the spread of the incident. In 5G networks, containment strategies must consider the dynamic and virtualised nature of the network.

- **Network Segmentation:** Implement network segmentation to isolate affected segments and prevent lateral movement of attackers. This involves creating secure zones and enforcing strict access controls between them.

- **Quarantine Devices:** Use automated systems to quarantine compromised devices, particularly IoT devices that may have been hijacked. Quarantining prevents these devices from communicating with the rest of the network.
- **Isolate Slicing:** Leverage the dynamic slicing capabilities of 5G networks to create isolated slices for affected services. This can help contain the incident within a specific slice, minimizing the impact on other services.
- **Traffic Filtering:** Deploy traffic filtering mechanisms to block malicious traffic. This includes setting up firewalls, intrusion prevention systems (IPS), and other filtering tools to block traffic from known malicious sources.

3.4.1.3 Eradication

The eradication phase focuses on removing the root cause of the incident. This involves eliminating malware, closing vulnerabilities, and ensuring that the threat is fully eradicated from the environment.

1. **Patch Management:** Ensure all virtualized network functions (VNFs) and IoT devices are updated with the latest security patches. Regular patching helps close vulnerabilities that attackers may exploit.
2. **Malware Removal:** Deploy advanced anti-malware tools to clean infected systems. This includes scanning for and removing malware from affected devices and network components.
3. **Vulnerability Remediation:** Identify and remediate vulnerabilities that were exploited during the incident. This involves conducting thorough vulnerability assessments and applying necessary fixes.
4. **Reconfiguration:** Reconfigure network slices and virtualised functions to close vulnerabilities exploited by the attack. This includes updating configurations, access controls, and security policies.

3.4.1.4 Recovery

The recovery phase involves restoring normal operations and ensuring that systems are secure and functional. In 5G networks, recovery must be swift and comprehensive to minimise downtime and impact.

- **Restore Services:** Utilise backup systems and redundancy to restore normal operations quickly. This includes restoring data from backups, rebuilding systems, and ensuring that services are operational.
- **System Validation:** Conduct thorough testing to validate the integrity and security of restored systems. This involves running security checks, performance tests, and functional tests to ensure that systems are operating correctly.
- **Phased Recovery:** Implement a phased recovery approach to gradually restore services. This helps identify and address any issues that may arise during the recovery process, ensuring a smooth transition back to normal operations.
- **Post-Recovery Monitoring:** Continue monitoring systems and network traffic for any signs of residual threats or new incidents. This helps ensure that the recovery is complete and that

systems remain secure.

3.4.1.5 *Lessons Learned Phase*

The lessons learned phase is crucial for understanding the root cause of the incident and improving future responses. This involves conducting a post-incident analysis and updating incident response playbooks based on insights gained.

- **Post-Incident Analysis:** Conduct a thorough post-incident review to understand the root cause, the effectiveness of the response, and areas for improvement. This involves analysing logs, attack patterns, and the actions taken during the incident.
- **Updating Playbooks:** Regularly update the incident response playbooks based on lessons learned from past incidents. This ensures that the playbooks remain relevant and effective, incorporating new insights and best practices.
- **Training and Awareness:** Conduct training sessions and awareness programs for the incident response team and other stakeholders. This helps ensure that everyone is prepared and knowledgeable about the latest threats and response strategies.
- **Documentation:** Document all findings, actions taken, and lessons learned in detail. This helps create a comprehensive record that can be referenced in future incidents and used to improve incident response processes.

3.4.2 **5G-Tailored Incident Response Playbooks**

An incident response playbook is a comprehensive and detailed guide designed to assist cybersecurity teams in managing and responding to various types of cybersecurity incidents effectively. These playbooks provide a structured, step-by-step approach to handling incidents, ensuring that all necessary actions are taken promptly to mitigate the impact, recover from the incident, and implement measures to prevent future occurrences. The primary purpose of an incident response playbook is to standardise the response process, ensuring consistency and efficiency across the organisation. By having predefined procedures, organisations can minimise the chaos and confusion that often accompany cyber incidents, enabling quicker and more effective responses.

The deployment of 5G networks introduces new challenges and complexities in cybersecurity [1]. With higher speeds, lower latency, and increased connectivity, 5G networks expand the attack surface and potential vectors for cyber-attacks. Incident response playbooks tailored for 5G environments are crucial for several reasons:

- **Complexity of 5G Architecture:** 5G networks utilise a combination of new technologies, including Network Function Virtualization (NFV), Software-Defined Networking (SDN), and network slicing. These technologies require specialised knowledge and procedures for effective incident response. Playbooks tailored to 5G can address these unique aspects and provide clear guidance for managing incidents in this complex environment.
- **Increased Attack Surface:** The proliferation of IoT devices and the extensive use of virtualisation in 5G networks increase the potential entry points for attackers. Incident

response playbooks can help mobile operators quickly identify and mitigate threats to IoT devices and virtualised network functions.

- **Real-time Response:** 5G networks support critical applications that require real-time data processing and communication. Any disruption can have significant consequences. A challenge for 5G tailored Incident response playbooks is to ensure that response actions are timely and effective, minimising downtime and impact.
- **Coordination and Communication:** Effective incident response requires seamless coordination among various stakeholders, including network operators, service providers, and security teams. 5G playbooks can provide a clear communication framework, ensuring that all parties are informed and engaged during an incident.

Playbooks are essential tools for incident responders as they outline roles and responsibilities, communication protocols, technical procedures, and post-incident activities. Especially in the complex and dynamic environment of 5G networks, an incident response playbook is an essential tool for managing and responding to cybersecurity incidents. By providing structured procedures and leveraging advanced simulation and detection capabilities, NITRO will enhance the ability of mobile operators to respond effectively to incidents, ensuring the security and resilience of 5G networks. NITRO's cyber range offers a realistic, emulated 5G environment where various types of incidents can be simulated, providing a safe space for testing and refining response procedures. Through NITRO's advanced simulation capabilities, cybersecurity professionals can practice responding to simulated incidents, enhancing their skills and readiness.

4 Gamification and Learning

4.1 Gamification in Cybersecurity Education

The industry and literature support using engaging methods such as Gamification, Games for Learning (G4L), and Game-Based Learning (GBL) to achieve high information retention rates for trainees. Due to budget constraints, organizations may find it hard to implement extensive programs to enhance employee awareness of information security and privacy, resulting in a lack of suitable exercises. Typically, the training topics focus solely on advanced concepts, leading to programs that do not effectively address the specific learning objectives of beginners or non-IT professionals. Consequently, not all available programs in the market offer the necessary flexibility for deployment. Therefore, modern educational tools need to be expanded to be adaptive, catering to individual needs by incorporating gamification elements.

Previous research has demonstrated that creative teaching methods and approaches to course delivery play a crucial part in increasing student motivation [15]. Gamification tools assist in delivering courses by applying established game design principles to improve skill building, regular practice, and self-assessment. There are numerous studies on the effects of gamification on learning impact. The result of these studies is almost unanimous, drawing all of them to the same conclusion that the integration of gamified elements into cybersecurity education can significantly enhance learning outcomes. A recent research in 2024 [16] evaluated the impact of integrating gamification into cybersecurity education with a focus on increasing university students' awareness of email phishing. The study compared the effectiveness of gamified learning methods with traditional video-based instruction in improving participants' ability to detect phishing attempts. The findings revealed substantial enhancement in phishing detection skills for both groups, with the gamified group exhibiting a higher improvement rate (59%) compared to the traditional group (41%). However, there are a few articles (such as [17]) that have identified gamification failures that is negative impacts on user engagement stemming from user maladapting due to design issues of gamified systems.

Moreover, a well-designed scoring system further enriches this experience by providing immediate, quantifiable feedback on trainee performance. This feedback is essential for learning, as it helps individuals identify their skills, strengths and weaknesses. There are some studies in this field that propose scoring algorithms for achieving fairness (to evaluate all participants equally regardless of their defensive or attacker role) and generality (to apply in all cyber ranges). NITRO will investigate strategies for scoring systems not only for the attackers using the traditional Capture the Flag but also for defenders, introducing metrics for Defend the Flag exercises. This is a significant challenge for NITRO cyber range as existing solutions emphasize on the offensive part of cybersecurity education. Focusing on the offensive capabilities without equally stressing defensive strategies can create an imbalance and contribute to the skills gap. Defensive cybersecurity is critical because it involves protecting systems, detecting breaches, and responding to incidents—skills that are essential for maintaining the security and integrity of information. To this end, NITRO will define novel metrics to follow the progress of a trainee focusing on defensive exercises.

4.2 Learning Analytics

Publishing and sharing research findings from the learning analytics can have multiple benefits on the educational landscape of cybersecurity. By disseminating relevant data, cybersecurity educators can gain insights into students' learning patterns and preferences, identifying knowledge gaps, common weaknesses and correlations between personal characteristics (e.g., age, sex). On the other hand, the design and effectiveness of cyber ranges are greatly enhanced through learning analytics, and this is done by creating personalised training environments that suit the particular skill levels and progress of the participants. Teachers and designers can, therefore, make custom scenarios that give learners a good challenge for better acquisition and retention of skills since data on user performance, learning styles, and engagement are analysed. Moreover, this data-driven method facilitates real-time feedback as well as changing scenarios to recover weak areas or introduce new challenges where necessary. Therefore, cyber ranges cease to be mere training grounds as they become intelligent adaptive learning systems which improve cybersecurity skills against changing threats and technologies.

In summary, learning analytics can offer several benefits to the educational landscape: 1) Enhance educational strategies allowing other educators to adapt and implement these strategies in their own contexts, potentially improving learning outcomes. 2) Data-driven insights can lead to the creation of adaptive learning platforms that are more responsive to individual learner needs and learning styles. 3) Fostering collaboration, 4) Publicly available research sets benchmarks for what can be achieved in educational settings for measuring their own efforts and can inspire them to reach or surpass existing standards, 5) Influencing educational practices and policies as published data and findings can pinpoint inefficiencies and pave the way for reforms or introducing new policies that enhance learning environments. Overall, the act of publishing in the field of learning analytics not only advances the academic discipline but also has practical implications for improving education globally.

4.2.1 Privacy issues in learning analytics

Learning analytics requires privacy, particularly in sensitive environments such as cyber ranges where data collected includes detailed user interactions and possibly identifiable information. Participant confidentiality is a matter of ethics and trust between learners and their respective platforms. Strict observation of robust privacy protocols helps ensure that learning analytics is done within legal boundaries such as GDPR, which emphasizes consent and data minimisation. As a result, including strong privacy measures in the learning analytics framework provides an avenue for safeguarding people's personal information while utilising advantages associated with personalised learning environments. By doing so, it will not only protect participants but also improve the integrity and reliability of the cyber range (and in general any e-learning platform), leading to wider adoption and participation.

Unfortunately, privacy is often neglected in learning analytics. A recent study found that less than 6% of the papers focused on learning analytics have also covered privacy issues [13]. In particular, only four papers of the 2919 ones indexed by Scopus mentioned or discussed the data anonymization

subject without achieving a real application. Institutions rarely inform their students about learning analytics practices, and there exist significant privacy concerns. Without incorporating a clear student voice in the design of learning analytics, institutions risk placing themselves in an ethical gray area. As mentioned in [14], *"institutions must balance their desire to implement LA with their obligation to educate students about their analytic practices and treat them as partners in the design of analytic strategies reliant on student data in order to protect their intellectual privacy"*.

In the area of privacy-preserving mechanisms, mechanisms such as k-anonymity and differential privacy are crucial. K-anonymity guarantees that individual entries appear as at least k mutually indistinguishable records so as to maintain some level of anonymity that thwarts identity disclosure. However, differential privacy appears to be more robust, especially in environments needing higher security and precision. It introduces controlled noise into the analysis data such that it hides the single contribution but still allows meaningful aggregate data analysis. This technique not only maintains statistical integrity but also ensures the privacy of each subject irrespective of how much external information a potential adversary has got. In fact, differential privacy is highly efficient because it provides an explicit measure for balancing between utility and security; hence, becoming preferable in modern data-oriented cybersecurity education or training field. NITRO will adopt the use of differential privacy as a viable solution for privacy preserving learning analytics.

5 Legal and Policy Aspects

The NITRO project must operate within a well-defined legal and policy framework. This ensures that the project adheres to legal standards and fosters trust among stakeholders. The following sections provide a detailed analysis of the legal and policy requirements relevant to the project.

5.1 Relevant Legal and Policy Frameworks and Compliance

5.1.1 Compliance with EU and international laws

EU Cybersecurity Act:

Framework: The EU Cybersecurity Act establishes a certification framework for ICT products, services, and processes. This framework enhances the security of digital products and services in the EU.

Implications for NITRO: NITRO must ensure that its platform and activities meet the certification standards outlined in the act. This involves adopting best practices for cybersecurity and potentially seeking EU certification for the cyber range.

Specific Regulations to Monitor:

- EU Certification Schemes: Monitor initiatives such as the European Cybersecurity Certification Scheme (EUCC) for IT products.
- ENISA Guidelines: Follow guidelines and updates from the European Union Agency for Cybersecurity (ENISA).

General Data Protection Regulation (GDPR):

Scope: GDPR is a comprehensive data protection law that applies to any organisation processing personal data of EU citizens. In order to adhere to the requirements of GDPR, NITRO will give priority to the implementation of differential privacy and data minimization as the main methods for ensuring privacy, as explained in section 6 mentioned earlier.

Key Requirements:

- Lawful Processing: Data processing must be based on one of the six lawful bases (e.g., consent, legitimate interests).
- Data Subject Rights: Facilitating rights such as access, rectification, erasure, and data portability.
- DPIAs: Conducting DPIAs to assess the impact of data processing activities on data subjects.
- Breach Notification: Reporting data breaches to supervisory authorities within 72 hours.

Implications for NITRO: Ensuring compliance with GDPR involves integrating these principles into the platform's design and operations. This includes secure data storage, processing, and transmission practices.

Specific Regulations to Monitor:

- GDPR Article 25: Data protection by design and by default.
- GDPR Article 32: Security of processing requirements.

Particularly in light of the engineering stories and duties that were previously mentioned, GDPR should be taken into account, as data and its protection are of paramount importance. The following tasks, objectives, and security risks serve as an indication of the necessity of incorporating GDPR into every stage of the development process in order to prevent any potential non-compliance.

1. The development of a Data Collection Toolkit, designed to collect actual data streams, highlights the importance of safeguarding and reducing the data in accordance with GDPR regulations.
2. Furthermore, it is imperative to ensure the safeguarding of the data pertaining to the industrial partners who will be summoned to evaluate the cyber-range and furnish us with their valuable input.
3. The potential for a white-box assault, as discussed earlier, highlights the ability of an attacker to gain access to a network's data and some essential data analytics services. This underscores the importance of complying with GDPR regulations.
4. The requirement for GDPR compliance and general data protection can be further demonstrated by other assaults, such as the creation of a Rogue Base Station, Network Slicing assaults, IoT Device Compromises, and Virtualisation Layer Attacks. All the aforementioned have the potential to compromise user privacy, steal crucial information, and lead to data breaches.

NIS2 Directive:

Purpose: The NIS2 Directive, adopted in January 2023 and fully transposed into national laws since October 2024, aims to establish a higher and more consistent level of cybersecurity across the European Union. It builds on the original NIS Directive by introducing more stringent requirements for cybersecurity risk management, incident reporting, and operational resilience. This directive is now the primary framework for cybersecurity within the EU, replacing the original NIS Directive, with its implementation standardising cybersecurity practices across EU's Member States. [21]

Key Requirements:

- **Enhanced Security Measures:** Implementing appropriate and stricter security measures to manage risks to network and information systems and to ensure resilience.
- **Incident Reporting:** Establishing protocols for reporting significant security incidents to national authorities, following the stricter timeline established in NIS2 Directive. To achieve that an incident should be reported within 24 hours to the national authorities. Whereas, a detailed incident report should also be provided within 72 hours of the initial notification.

Accountability & Governance: Management bodies are now directly accountable for ensuring compliance with cybersecurity obligations, including penalties for non-compliance.

Implications for NITRO: Regulatory modifications and modifications in business conduct are necessary for the NITRO project to correspond with the NIS2 Directive. One minor adjustment in the project's strategy is the integration of advanced security risk-management practices, including customised protections for the cyber range. A solid incident reporting system should be used to enforce compliance with hard and quick deadlines for 24- and 72-hour reporting since these deadlines are designed to facilitate smooth contact with each country's authorities and all stakeholders in the wake of a major incident. In addition, clear accountability needs to be integrated into the project's governance structure, which assigns specific roles and responsibilities.

Cyber Resilience Act:

Objective: The Cyber Resilience Act aims to ensure that hardware and software products placed on the EU market have fewer vulnerabilities and that manufacturers take security seriously throughout a product's lifecycle.

Key Provisions:

- Security by Design and by Default: Manufacturers must integrate security features into products from the outset.
- Vulnerability Handling: Requirements for manufacturers to manage vulnerabilities post-market.
- Conformity Assessment: Products must undergo a conformity assessment to ensure they meet security standards.

Implications for NITRO: The NITRO project must align its platform components with the Cyber Resilience Act, ensuring that all software and hardware used comply with these security requirements, from design through to end-of-life management.

AI Act:

Purpose: The AI Act seeks to regulate AI systems to ensure they are safe, respect fundamental rights, and promote trustworthy AI within the EU.

Key Requirements:

- Risk-based Classification: AI systems are classified based on their risk levels (unacceptable, high, limited, and minimal).
- Compliance Obligations for High-Risk AI: High-risk AI systems must meet stringent requirements related to data governance, transparency, robustness, accuracy, and human oversight.
- Prohibited Practices: Certain AI practices deemed to be unacceptable are outright banned.

Implications for NITRO: If the NITRO project incorporates AI components, it must ensure compliance with the AI Act. This involves assessing the risk level of AI systems used, implementing necessary

safeguards, ensuring transparency and accountability, and avoiding prohibited AI practices.

Specific Regulations to Monitor:

- **AI Risk Management:** Follow guidelines on risk management for AI systems as defined by the AI Act.
- **Transparency Obligations:** Ensure adherence to transparency and accountability standards.

International Laws and Standards:

ISO/IEC 27001: This international standard provides a framework for information security management systems (ISMS).

Implications for NITRO: Adopting ISO/IEC 27001 can help in systematically managing sensitive information and ensuring robust security controls.

5.1.2 Data protection and privacy laws

GDPR Compliance:

In order to ensure the future advancement of the NITRO cyber range, it is crucial to examine certain critical factors [20]. Firstly, it is imperative to integrate data protection principles into all systems and processes from the outset, both as a fundamental aspect of their design and as the default setting. Furthermore, it is crucial to guarantee that the handling of personal data within NITRO is grounded on a legal justification, such as getting explicit consent or proving a legitimate interest. Furthermore, it is imperative to provide systems that enable the smooth exercise of data subjects' rights, such as the provision of automated tools to handle requests for data access and deletion. Lastly, conducting Data Protection Impact Assessments (DPIAs) for high-risk data processing operations is essential to identify and reduce potential hazards to data subjects. Implementing these procedures is crucial for ensuring GDPR compliance and efficiently safeguarding personal data.

Data Anonymization and Pseudonymization:

Data anonymisation and pseudonymisation should also be implemented in NITRO's data protection efforts. Anonymisation refers to the process of eliminating personally identifying information (PII) from datasets that are utilised in cyber range exercises. Pseudonymisation is the process of substituting personally identifiable information (PII) with pseudonyms to minimise the possibility of data being linked back to individuals. These strategies are essential for mitigating the risks connected with data breaches and maintaining adherence to GDPR regulations. Adopting these measures will improve data security and safeguard personal information within NITRO.

Data Minimization and Retention:

As we advance the project, it is crucial to consider key aspects of data minimization and retention. The principle behind data minimization is to collect only the data necessary for the specified purpose and to retain it only for as long as necessary. For NITRO, this means implementing strict data minimization

and retention policies to ensure that data is not kept longer than required and is securely deleted when no longer needed. These practices are vital for safeguarding personal information and maintaining compliance with data protection regulations.

Security Measures:

Technical measures such as encryption, access controls, and secure communication protocols are crucial. Organisational measures, including staff training, regular security audits, and incident response plans, also play a significant role. For NITRO, it is imperative to ensure the implementation of both technical and organisational measures to safeguard personal data from unauthorised access, accidental loss, or destruction. These steps are essential for maintaining robust data security and compliance with regulatory requirements.

5.1.3 Industry-specific regulations

Telecommunications Regulations:

Overview: Regulations governing the telecommunications industry focus on network security, interoperability, and spectrum management.

Implications for NITRO: The cyber range must comply with these regulations to ensure that the simulated 5G environments adhere to legal standards. This includes managing spectrum usage and ensuring secure, interoperable network components.

Specific Regulations to Monitor:

- 5G Security Guidelines: Monitor the European Telecommunications Standards Institute (ETSI) guidelines for 5G security.
- Spectrum Management Rules: Stay updated on spectrum allocation and management regulations by national regulatory authorities.

5.1.4 Intellectual property and licensing

Intellectual Property Rights (IPR):

Ownership and Protection: Establishing clear policies on intellectual property ownership and protection developed within the NITRO project.

Implications for NITRO: Implementing legal agreements to protect the intellectual property of all project partners.

Specific Regulations to Monitor:

- EU Directive on Copyright in the Digital Single Market: Ensure compliance with copyright laws related to digital content.
- Patent Regulations: Monitor EU regulations on patents to protect any innovations developed during the project.



Open-Source Licensing:

Licensing Models: Choosing appropriate open-source licenses for software components to ensure compliance with legal requirements.

Implications for NITRO: Adopting licensing models that promote collaboration while protecting the intellectual property rights of contributors.

By adhering to these legal and policy requirements, the NITRO project will not only ensure compliance but also build a robust and trustworthy platform for cybersecurity training and testing. This approach will enhance the overall security and resilience of 5G-IoT networks, addressing both current and emerging threats in this rapidly evolving field.

6 Requirements for NITRO Cyber-Range Ecosystem

In this section we present the requirements for the NITRO cyber-range ecosystem, organized in different guiding forces for the design of NITRO.

6.1 Final Methodology for Requirements Elicitation

NITRO considers that the full development of the project concept and the high-level architecture that will drive the technical developments has to be based on requirements collection that are challenging current concepts and promote ground-breaking research and also align with the current legislation principles.

The engineering of the requirements stems from a number of challenges emerging from the need to define new or re-establish existing practices towards the creation of a Cyber-range usable for an evolving landscape of service and application deployment in 5G and IoT networks. These challenges were presented in the previous sections, and here, we use those challenges as a base to elaborate on the requirements in order to respond to the above challenges by analysing both functional and non-functional ones.

6.2 Functional & Technical Requirements

In this section, we present the functional requirements from different perspectives and elaborate on the objectives and motivation behind the definitions for each requirement. This will make it easier to formulate a common view of NITRO and understand the needs that the created solution should address.

Furthermore, as part of this exercise we present the way envisioned for addressing each requirement; this initial presentation of building blocks is provided by the project partners providing the requirements and serve as a starting point for the design of the architecture in D2.2.

6.2.1 NITRO Cyber-Range Requirements

In the following table, we present the aggregated requirements. We follow the MoSCoW approach to help prioritise requirements, manage resources, and ensure a focus on delivering the most critical functionalities. The MoSCoW approach is a prioritisation technique commonly used in project management and software development to classify requirements into four categories: Must-Have, Should-Have, Could-Have, and Won't-Have. Each category represents a different level of necessity: "Must-Have" items are essential for the project's success and cannot be compromised, while "Should-Have" items are important but not critical, meaning they can be deferred if necessary. "Could-Have" items are desirable but optional, often considered if resources allow, and "Won't-Have" items are deliberately excluded in the current scope, usually reserved for future consideration.

Furthermore, a more structured prioritization in the form of table parameters (Value - HIGH, MEDIUM, LOW and Complexity – HIGH, MEDIUM, LOW) can be used for the identification of the development priority, with critical features are delivered first, while lower-priority items can be tackled later or set aside for future enhancements.

Table 2: Identified Requirements

ID	Requirement	Value	Complexity	Functional / Non-Functional
REQ-01	The platform should emulate realistic 5G traffic patterns with minimal jitter	HIGH	HIGH	Functional
REQ-02	Essential cybersecurity features must be integrated to monitor threats.	HIGH	LOW	Functional
REQ-03	The system should efficiently manage high-volume subscriber and device profiles.	MEDIUM	HIGH	Non-functional
REQ-04	The system must ensure data confidentiality through encryption.	HIGH	MEDIUM	Functional
REQ-05	User Equipment (UE) should interact seamlessly with the 5G Core network.	HIGH	MEDIUM	Functional
REQ-06	The system should support the addition of multiple User Equipment (UEs) without degradation of performance.	MEDIUM	HIGH	Non-functional
REQ-07	It should be possible to retrieve and inspect the 5G network traffic for analysis and troubleshooting.	MEDIUM	LOW	Functional
REQ-08	Trainees should be capable of submitting flags or other approach to retrieve their progress.	MEDIUM	LOW	Functional
REQ-09	Metrics of the trainees' actions should be retrievable from the Cyber Range for assessment and feedback.	MEDIUM	MEDIUM	Functional
REQ-10	The system must support dynamic scaling of core 5G components to handle varying user loads and network traffic.	HIGH	MEDIUM	Non-functional
REQ-11	The cyber range must provide the capability to isolate network slices for distinct environments.	HIGH	LOW	Functional
REQ-12	The system must intelligently allocate network bandwidth and support automatic rerouting to optimize performance under variable network load and congestion.	HIGH	MEDIUM	Non-functional
REQ-13	The system must integrate with Kubernetes or similar to allow distributed deployments.	HIGH	MEDIUM	Functional
REQ-14	The platform should support capture the flag exercises for 5G networks	HIGH	LOW	Functional
REQ-15	The platform should offer tools for simulating reconnaissance attacks in 5G networks	HIGH	LOW	Functional
REQ-16	The platform should allow to use traffic generators to perform replay attacks and traffic injection	HIGH	MEDIUM	Functional
REQ-17	Platform could simulate APTs targeting 5G networks	HIGH	HIGH	Functional
REQ-18	Platform should simulate RCE attacks in a 5G environment and respond on them	HIGH	HIGH	Functional

REQ-19	The cyber range should support simulation of service disruption attacks such as DoS	HIGH	MEDIUM	Functional
REQ-20	The cyber range should support simulation of control plane disruption attacks and allow responding	HIGH	MEDIUM	Functional
REQ-21	Platform must deploy 5G NFs with deliberate misconfigurations	HIGH	MEDIUM	Functional
REQ-22	The cyber range should support simulation of cascading attacks and respond on them	HIGH	HIGH	Functional
REQ-23	Cyber range should support different types of attack scenarios and allow incident handling	HIGH	MEDIUM	Functional
REQ-24	Platform should offer predefined incident response procedures	MEDIUM	MEDIUM	Functional
REQ-25	Platform could offer the means for training the communication of incidents	MEDIUM	MEDIUM	Functional
REQ-26	Cyber range should simulate scenarios with adversarial techniques for attacking AI models	HIGH	HIGH	Functional
REQ-27	Cyber Range should provide realistic storylines	HIGH	MEDIUM	Non-functional
REQ-28	Cyber Range should include scoring system and provide motivation to trainees	HIGH	MEDIUM	Non-functional
REQ-29	Cyber Range should support trainees of different levels of knowledge	HIGH	MEDIUM	Non-functional
REQ-30	Cyber Range must be easy to install	MEDIUM	MEDIUM	Non-functional
REQ-31	The platform should provide pre-installed cybersecurity tools for training	HIGH	MEDIUM	Functional
REQ-32	Cyber Range should use only the required 5G elements	LOW	MEDIUM	Non-functional
REQ-33	Platform should gather and store interoperable attack traffic data from various sources	HIGH	MEDIUM	Non-functional
REQ-34	Platform must respect privacy of participants	HIGH	MEDIUM	Non-functional
REQ-35	Cyber Range should respect secure data retention and deletion practices	HIGH	MEDIUM	Non-functional

6.3 Engineering Stories

In this section, we define engineering stories (ES) for the NITRO Cyber range. These engineering stories are intended to outline the objectives, motivation and building blocks to implement them. Note that some stories (e.g., ES-7) provide a detailed and technical description that includes components of the 5G network. These components are analysed in the deliverable “D2.2 “NITRO cyber range architecture, testing and validation plans”.

6.3.1 5G Attack Scenarios of NITRO Cyber-Range platform

ES-1: Build A cyber range ecosystem exposing attacks on the 5G core

Description: As a user of the cybersecurity training system, I want to be exposed to the intricacies of the most prominent attack vectors in 5G/6G environments.

Objectives: To set up a testing environment and training exercises, such as capture the flag, that represent real-world operations and information which trainees can use to exploit the most prominent attack vectors.

Motivation: To enhance the knowledge and skills of users regarding 5G attack vectors as well as considering the interconnection and dependencies between attacks targeting different layers of 5G networks.

Building Blocks: The Cyber Range ecosystem infrastructure will include all necessary components for the capture the flag exercises we will create. This includes the injection of vulnerabilities into all 5G/6G components, from the control plane to the data plane, and network traffic anomalies. These elements will be wrapped in detailed write-ups that users must identify to successfully launch an attack. Based on user interactions with the write-ups, we will generate a gamification risk score to evaluate the success rate of specific attacks and the user's knowledge representation.

ES-2: Understanding 5G network structure by reconnaissance of 5G networks

Description: As a user of the cybersecurity training system, I want to utilize reconnaissance tools to infer the details of 5G networks.

Objectives: To set up a 5G network where trainees can perform network investigation exercises to enhance the trainees' ability to fingerprint topologies and assess 5G networks.

Motivation: To better understand the network structure, vulnerabilities, and potential points of attack of 5G networks. Better comprehension of 5G networks new technologies and protocols that may present novel security challenges

Building Blocks: The cyber range platform will include several reconnaissance open source tools that students can execute including Nmap for network and service discovery, traceroute for path analysis, Wireshark for traffic monitoring and protocol analysis.

ES-3: Understanding information leaks in 5G networks

Description: As a cybersecurity professional, I want to understand the risks and mechanisms of information leaks in 5G networks so that I can implement effective measures to prevent unauthorized data exposure.

Objectives: Study how information leaks can happen, including misconfigurations, protocol weaknesses, and insider threats. Analyze various components and interfaces in 5G networks to identify where information leaks are most likely to occur.

Motivation: Information leaks in 5G networks can lead to significant breaches of privacy, loss of sensitive data, and compromise of critical services.

Building Blocks: A 5G network that trainees should explore using reconnaissance tools to identify which network component is responsible for the information leak and what exactly the sensitive data is and how it can be exploited.

ES-4: Scenario specific for information leaks in 5G networks

Description: As a cybersecurity professional, I want to prevent information leaks across different 5G network slices to ensure the confidentiality and integrity of slice-specific sensitive data.

Objectives: Identify how shared NF instances between slices can lead to information leaks due to weaknesses in the NRF-based service authentication scheme.

Motivation: Ensuring the confidentiality and integrity of slice-specific sensitive data is crucial for the security and trustworthiness of 5G networks. Addressing the vulnerabilities in the NRF-based service authentication scheme to prevent unauthorized data access and protect against information leaks.

Building Blocks: In a 5G network, a Service Provider NF (Network Function) instance can be shared by multiple slices, potentially containing slice-specific sensitive data. A misbehaving NF obtains a valid OAuth access token, which subsequently conveys it to the victim NF. The latter approves the request because the access token is valid and responds with the requested sensitive data.

ES-5: Replay attacks and traffic injection in 5G networks

Description: As a cybersecurity professional, I want to understand how to perform replay attacks and traffic injection in 5G networks and what is their security impact.

Objectives: Analyze how replay attacks are conducted, including the interception and retransmission of valid data packets. Examine the methods used by attackers to inject malicious or unauthorized data packets into the network. The scenario underscores the importance of comprehensive security testing and validation tools like 5Greplay in identifying and mitigating such vulnerabilities in 5G networks.

Motivation: The primary risk is the potential for unauthorized access or impersonation of a UE. This enables attackers to manipulate the security level of the connection, either by downgrading it to a weaker encryption algorithm or disabling it entirely. Such vulnerabilities lead to a wide range of security breaches, including data interception, privacy violations, and unauthorized access to network resources

Building blocks: Configuring traffic generator (e.g., 5Greplay) to identify and replicate susceptible messages (e.g., NAS-5G SMC messages) sent by a UE post-authentication. Assessing the online forwarding capabilities of 5Greplay and the resilience of AMF against replay attacks.

ES-6: Simulation of Advanced Persistent Threats (APTs) in 5G networks

Description: As a security researcher, I want to simulate a kill chain and study Advanced Persistent Threats (APTs) targeting 5G networks in order to understand the full attack lifecycle, including initial access, exploitation, lateral movement, and persistence, so I can develop effective countermeasures and strategies.

Objectives: The objective is to simulate a full kill chain within a 5G network, covering stages from reconnaissance to impact. This includes realistic scenarios targeting network functions such as AMF, SMF, and RAN components. Researchers will focus on identifying vulnerabilities in virtualized environments, and investigate the full impact of the cyberattack.

Motivation: To improve the researcher's understanding of APT tactics, techniques, and procedures (TTPs), and to develop effective strategies for detecting and countering these threats.

Building Blocks: : The Cyber Range emulates 5G network environments and explore APT in connection to MITRE focusing on initial access, lateral movement, and privilege escalation.

ES-7: A specific scenario for simulation of attacks in 5G networks → Attacking a healthcare service

Description: As a security researcher, I want to simulate an adversary, aiming at dropping the health services customers' data traffic by gaining control of the UPF node in e-health network slice.

Objectives: Understand multi-stage attack campaigns in 5G networks. To gain initial access to a NF container, escape from it and query the NFR for the target slice by finding the correct slice identifier. Next, the attacker accesses the UPF and redirects the users' traffic, causing DoS.

Motivation: To improve the researcher's understanding of how the NF containers can be compromised and execute step by step the attack graph leading to a DoS of e-health services that rely on a 5G network slice.

Building Blocks: The cyber range will creation a set of network slices which the attacker will eventually find which one is used by the targeted network (i.e., e-health).

ES-8: Simulating Remote Code Execution (RCE) attacks

Description: As a cybersecurity researcher, I want to simulate RCE attacks in a 5G environment to understand their mechanisms and develop countermeasures.

Objectives: To create scenarios where RCE vulnerabilities are exploited, allowing researchers to study the techniques and implement effective security measures.

Motivation: To enhance the researcher's ability to detect and prevent RCE attacks, ensuring the security and stability of network functions.

Building Blocks: The Cyber Range will simulate RCE attacks by injecting malicious code into vulnerable applications and services within the 5G network. Researchers will use security tools to detect and mitigate these exploits, analyse the attack vectors, and apply patches. Performance will be measured based on the effectiveness of the detection and response strategies.

ES-9: Simulating service disruption attacks

Description: As a cybersecurity analyst, I want to simulate service disruption attacks in 5G networks so that I can evaluate the network's resilience and improve its defences against such attacks.

Objectives: Analyze the different types of service disruption attacks, including DoS and DDoS, and their mechanisms. Study the potential impact of these attacks on the availability and performance of 5G network services.

Motivation: Service disruption attacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, can significantly impact the availability and reliability of 5G networks. Simulating these attacks helps in understanding their impact, identifying vulnerabilities, and developing robust defense mechanisms.

Building Blocks: The Cyber Range will simulate various service disruption attacks, such as DDoS and targeted disruptions of critical services. Performance will be assessed based on the effectiveness of the attack to disrupt the relevant services.

ES-10: A specific scenario for service disruption attacks → IoT botnet DDoS attack for flooding data plane

Description: As a cybersecurity researcher, I want to perform data plane flood attacks in 5G networks so that I can study their impact and understand the vulnerabilities they exploit.

Objectives: Understand Data Plane Flood Attacks and how a botnet of IoT devices can have a disastrous impact on data plane VNFs (i.e., shared UPF).

Motivation: Data plane flood attacks, such as ping flood attacks, involve malicious IoTs flooding the network with excessive ping requests. This can overwhelm the links of a network slice and exhaust the resources of data plane Virtual Network Functions (VNFs).

Building blocks: Emulate IoT traffic by sending ping requests from several sources (i.e., emulated UEs). The data network will provide ping replies further flooding the network links of the shared UPF.

ES-11: A specific scenario for service disruption attacks → IoT botnet DDoS attack for flooding control plane

Description: As a cybersecurity researcher, I want to carry out control plane flood attacks in 5G networks so that I can evaluate the network's vulnerabilities and stress-test its control plane VNFs (i.e., the AMF).

Objectives: Analyze how registration request flood attacks are initiated by malicious UEs (i.e., compromised IoT devices) and their impact on the control plane VNFs (i.e., the AMF) as well as connectivity delays for legitimate UEs, negatively impacting data transmission speed and overall network efficiency.

Motivation: Control plane flood attacks, specifically registration request flood attacks, involve IoT botnets sending a high volume of registration requests to the core network. These requests aim to maliciously register with a network slice that the attacker is not authorized to join. Although the malicious registration requests do not succeed due to failed authentication, the persistent high-rate requests cause a flood situation, overloading the core VNFs and consuming their resources.

Building blocks: The attacker UE is configured to simulate a large number of UEs, creating an excessive load on network resources. This configuration leads to continuous connection attempts to the AMF by all simulated UEs, effectively emulating a DDoS attack. Legitimate UE shall experience connectivity delays.

ES-12: Identifying and exploiting misconfigurations in 5G components

Description: As a cybersecurity professional, I want to understand the types of attacks that can occur due to misconfigurations in 5G networks so that I can implement effective security measures to prevent such vulnerabilities.

Objectives: To create scenarios to first pinpoint typical misconfigurations in components of 5G networks and subsequently exploit them.

Motivation: Misconfigurations in 5G networks can lead to vulnerabilities that have severe consequences, including unauthorized access to network resources of the 5G core network, data theft, and service disruptions. By understanding and addressing these issues, cybersecurity professionals can significantly enhance the security and reliability of 5G networks.

Building Blocks: The Cyber Range will automatically deploy 5G NFs with deliberate misconfigurations. A trainee should perform reconnaissance and vulnerability scanning to identify them and select a proper attack path.

ES-13: Identifying and exploiting cascading attacks in 5G networks

Description: As a cybersecurity professional, I want to understand cascading attacks in 5G networks so that I can implement comprehensive defence strategies to prevent widespread network disruptions.

Objectives: Identify how initial attacks can propagate through different layers and components of a 5G network. Recognize critical components and interdependencies that are susceptible to cascading failures. Assess the potential impact of cascading attacks on network services and overall performance.

Motivation: Cascading attacks pose a significant threat to the integrity and reliability of 5G networks. Due to the interconnected nature of network components and services, an attack on a single point can lead to widespread disruptions. Understanding these attacks is crucial for developing strategies to protect against them, ensuring continuous and secure network operation.

Building Blocks: Initiation of an attack scenario that covers the interconnection of 5G networks with another system. Attack simulation on the 5G network will lead to negative consequences to an interconnected system from service disruption to data theft.

ES-14: A specific scenario for identifying and exploiting cascading attacks in 5G networks → Attacking 5G to disrupt 5G drone swarm

Description: As a cybersecurity professional, I want to understand the cascading effects of exploiting Packet Forwarding Control Protocol (PFCP) in the 5G core to block communications of a UAV swarm (Unmanned Aerial Vehicle) so that I can develop strategies to mitigate widespread disruptions.

Objectives: Same as ES-13, but specific in drone swarm scenario

Motivation: The deployment of 5G networks is crucial for supporting advanced IoT applications such as drone swarms. However, exploiting 5G vulnerabilities can lead to cascading effects by blocking or disrupting UAV communication which are served by the 5G network. This user story aims to investigate these cascading effects and their impact.

Building blocks: Set up a controlled environment to safely develop and implement PFCP attacks. Establish a testbed that simulates a drone-based scenario with 5G tunnelling between swarms. The emulated attacks perform DoS attack at N4 interface disrupting established 5G tunnels of drone swarms and blocking in this way their communication.

6.3.2 5G Incident Response of the NITRO Cyber Range

ES-15: Exposure to incident handling for different types of attacks

Description: As a security analyst, I want to be exposed to incident handling for different types of attacks to develop a comprehensive understanding of the necessary responses and mitigation strategies.

Objectives: To create scenarios involving various attack vectors, allowing security analysts to practice detection, containment, eradication, and recovery procedures for each type of attack.

Motivation: To improve the security analyst's ability to handle diverse cyber threats effectively, ensuring they are well-prepared to protect the 5G network infrastructure against multiple forms of attacks.

Building Blocks: Simulation of a wide range of attack scenarios, including DDoS attacks, network slicing attacks, far edge attacks, RCE attacks to VNFs, etc. Analysts will be guided through the incident handling lifecycle.

ES-16: Responding to service disruptions in 5G networks

Description: As an incident responder, I want to respond to service disruption incidents in 5G networks to ensure quick recovery and minimal impact.

Objectives: To create scenarios of service disruption incidents, allowing SOC analysts to practice detection, response, and recovery procedures.

Motivation: To enhance the analyst's ability to manage service disruptions effectively, ensuring rapid recovery and minimal impact on users.

Building Blocks: Scenarios for service disruption incidents, including detection through SIEM systems and response actions such as isolating affected services and rerouting traffic. Performance will be assessed based on the speed and effectiveness of the response and recovery efforts.

ES-17: Responding to misconfiguration originated attack

Description: As an incident responder, I want to train in responding to misconfiguration incidents in a 5G network to ensure effective incident management and recovery.

Objectives: To understand the security impact of misconfigurations and propose corrections to close the security loophole.

Motivation: Response to misconfigurations attacks require a deep understanding of the erroneous configuration so that a correct course of actions is followed that ends with changing the relevant configuration.

Building Blocks: Develop scenarios for misconfigurations-based attack that the trainee should be able to respond as quickly as possible. Inclusion of correct configuration to eradicate the root cause of the attack.

ES-18: Responding to RCE attacks in VNFs

Description: As a network engineer, I want to defend against RCE attacks targeting Virtual Network Functions (VNFs) to ensure the reliability and security of network services.

Objectives: To develop comprehensive incident response training scenarios specifically tailored for RCE attacks on VNFs.

Motivation: Given the critical role of VNFs in 5G networks, protecting these functions is essential for maintaining network security and reliability. A dedicated response strategy enhances the resilience of the network and ensures that any disruptions caused by RCE attacks are minimized.

Building Blocks A set of predefined incident response procedures will be developed, considering the specifics of VNFs and the types of RCE attacks that can occur. Recovery processes will be also taken into account.

ES-19: Responding to attacks on network slicing mechanisms

Description: As an incident responder, I want to efficiently respond to attacks targeting the network slicing mechanism so that I can mitigate threats and ensure the integrity and security of the 5G network.

Objectives: To develop a comprehensive incident response framework specifically tailored for attacks on network slicing mechanisms.

Motivation: Given the importance of network slicing in 5G networks, protecting these mechanisms is crucial for maintaining service quality and security.

Building Blocks: A set of predefined incident response procedures will be developed, outlining the steps to take when the Network Slicing Mechanisms is detected. Slice isolation mechanisms will be offered to the responder.

ES-20: Responding to Information leak incidents

Description: As an incident responder, I want to respond to information leak incidents in a 5G network to minimise the impact and ensure data confidentiality.

Objectives: To provide hands-on training scenarios where incident responders must detect, contain, and mitigate information leak incidents.

Motivation: To improve the responder's ability to manage and recover from information leak incidents, ensuring minimal impact on data confidentiality.

Building Blocks: A set of predefined incident response procedures will be developed, outlining the steps to take when an information leak is detected. Mitigation strategies to minimize the impact of the information leak.

ES-21: Communicative tasks for responding to 5G Cyberattacks

Description: As an incident responder, I want to manage communicative tasks within the NITRO Cyber Range to effectively handle targeted cyberattacks and ensure coordination with national and/or cross-border authorities.

Objectives: To equip incident responders with the ability to manage and respond to targeted cyberattacks within the NITRO Cyber Range. This includes handling communicative aspects of the attack and ensuring effective communication with national and cross-border authorities.

Motivation: Incident response does not cover only technical activities but also communications tasks. That is, proper coordination and communication are crucial for a timely and effective response, minimizing the disruption to business operations and ensuring the security and integrity of the network.

Building Blocks: A scenario of a cross-border attack will be designed identifying also the communication protocols and channels to manage effective coordination with national and cross-border authorities.

ES-22: Responding to cascading attacks in 5G networks

Description: As an incident responder, I want to efficiently respond to cascading attacks in 5G networks so that I can mitigate the impact and prevent widespread disruptions.

Objectives: Develop a comprehensive incident response playbook specifically tailored for cascading attacks in 5G networks for training purposes.

Motivation: Given the interconnectedness of 5G components, an incident response may require the communication and coordination with organizations not related with the mobile operation, fact that increase the complexity of the incident response.

Building Blocks: A set of predefined incident response procedures targeted for training on managing cascading attacks.

6.3.3 Adversarial & Robust AI Training Scenarios of NITRO Cyber-Range

This section provides engineering stories as starting points to describe the requirements of designing exercises to train adversarial and robust AI techniques. Please note that in the second version of this deliverable, more specific stories will be developed to reflect concrete usages of AI in 5G / IoT networks. Specific AI models will be also selected from the list of functionalities described above.

ES-23: Attacking AI models for 5G and IoT Networks with adversarial examples

Description: As a cybersecurity trainee, I want to learn how to attack AI models as they are applied to 5G and IoT networks using adversarial techniques as applied either at the training or testing phase.

Objectives: To simulate real-world scenarios where the performance of AI models is undermined due to the presence of adversarial samples targeting 5G and IoT operations.

Motivation: To increase the trainee's understanding of the vulnerabilities associated with AI models devices and raise awareness of the dangers lurking due to the adversarial techniques.

Building Blocks: The Cyber Range will simulate various AI models to be applied for optimizing 5G network operations (e.g., slicing) as well as for an IDS in IoT networks. Trainees will be tasked with identifying and attacking these AI models with different adversarial techniques including poisoning attack, backdoor attack and evasion attacks. The exercises will include step-by-step guides, and trainees' performance will be evaluated based on their ability to deteriorate as much as possible the performance of AI models and studying the impact of them on 5G and IoT networks.

ES-24: Securing AI models for 5G and IoT Networks

Description: As a cybersecurity trainee, I want to learn how to secure AI models as they are applied to 5G and IoT networks to prevent adversarial AI attacks against them.

Objectives: To simulate real-world scenarios where the performance of AI models is not undermined even in the presence of adversarial samples targeting 5G and IoT operations.

Motivation: To increase the trainee's understanding of AI robustness techniques to improve their ability to secure AI models.

Building Blocks: NITRO will simulate various AI models to be applied for optimizing 5G network operations (e.g., slicing) as well as for an IDS in IoT networks. Trainees will be tasked with securing the AI models using a set of robustness techniques. The exercises will include step-by-step guides, and trainees' performance will be evaluated based on their ability to understand which robustness technique is suitable for each AI model to be secured.

6.3.4 Privacy Preserving Learning Analytics in NITRO Cyber Range

ES-25: Privacy-Preserving mechanisms for learning analytics

Description: As a system administrator, I want to implement robust privacy-preserving measures in the NITRO Cyber Range to ensure the protection of participant data and compliance with data protection regulations, while enabling realistic and effective cybersecurity training scenarios.

Objectives: Privacy preserving collection and processing of learning data during the cyber range exercises. To implement data anonymization techniques to protect the privacy of participants and their associated data based on differential privacy. To ensure that the cyber range scenarios and data processing activities do not pose undue privacy risks to the participants.

Motivation: By implementing these privacy-preserving measures, the NITRO Cyber Range will create

a secure and compliant training environment that gives the opportunity of learning analytics with a controlled loss of information.

Building Blocks: Implementation of a differential privacy algorithm for learning analytics. Configuration and parameter selection such as the value privacy budget ϵ and noise distribution (e.g., Laplace). The aim will be to minimize loss of information without sacrificing data privacy.

ES-26: Secure data retention and deletion

Description: As a system administrator, I want to ensure that the NITRO Cyber Range adheres to secure data retention and deletion practices, minimizing the storage of personal data and securely disposing of it when it is no longer needed.

Objectives: To establish clear data retention periods and procedures for the secure deletion of personal data generated within the NITRO Cyber Range. To implement technical and organizational measures to ensure the proper disposal of data and prevent unauthorized access or recovery.

Motivation: By implementing these secure data retention and deletion practices, the NITRO Cyber Range will demonstrate its commitment to responsible data stewardship and minimize the risk of unauthorized access, misuse, or breach of personal data. This approach will also help to ensure compliance with relevant data protection regulations and build trust among the platform's user community.

Building Blocks: Determine the minimum necessary retention periods for personal data generated within the NITRO Cyber Range, based on the training objectives and legal requirements. Establish clear policies and procedures for the secure deletion of personal data upon the expiration of the retention periods. Regularly review and update data retention periods to ensure their continued relevance and compliance with data protection regulations. Ensure that deleted data cannot be recovered through forensic analysis or other means. Ensure that the logging mechanisms do not record any real MAC addresses or other personally identifiable information (PII) that could compromise the privacy of participants.

6.3.5 Gamification and Scoring System of NITRO Cyber-Range

ES-27: Gamification elements

Description: As a cybersecurity trainee I want gamification elements integrated into my training program to make learning more engaging and motivating.

Objectives: To enhance the training experience through gamification, making it more interactive and motivating. By incorporating various game-like elements, trainees will be more engaged, leading to better retention of knowledge and skills.

Motivation: By integrating gamification, trainees can benefit from increased motivation, higher

engagement levels, and a sense of accomplishment, all of which contribute to more effective learning and skill development.

Building Blocks: Integrate gamification elements (e.g., leaderboards, rankings, badges, certificates, progress bar, avatars, rewards, virtual currency, and access privileges).

ES-28: Scoring system for attackers and defenders

Description: As a cybersecurity trainee, I want a scoring system to keep track of my progress, whether I am playing the role of an attacker or a defender, so that I can gauge my skills and improvement over time.

Objectives: To develop a scoring system that accurately reflects the trainees' performance in both attacker and defender roles. This system will record successes, failures, and skill enhancements, offering detailed feedback and progress reports.

Motivation: Scoring system is neglected by current cybersecurity training programs. Especially for the defenders, there are no specific metrics to evaluate the progress of a cybersecurity defender. On the other hand, attackers utilize only capture the flag systems for scoring which is not appropriate for all cases (e.g., denial of service attack).

Building Blocks: A set of metrics and criteria will be defined for both attacker and defender activities. This includes measuring the success rate of attacks, the effectiveness of defense strategies, the speed and efficiency of responses, and the ability to identify and mitigate threats. The scoring system should include features for setting personal goals, tracking achievements, and receiving badges or certifications upon reaching certain milestones.

ES-29: Storytelling and scenario walkthroughs

Description: As a cybersecurity trainee, I want storytelling and scenario walkthroughs to be part of my training so that I can better understand real-world applications of security concepts and improve my problem-solving skills.

Objectives: To create engaging and realistic storylines that provide context and motivation for the training scenarios. To develop detailed walkthroughs and guides that help participants navigate the training exercises and understand the expected outcomes.

Motivation: By providing trainees with a compelling narrative and clear guidance, they will be better equipped to understand the context and objectives of each training exercise.

Building Blocks: Development of engaging storylines that provide context and motivation for the training scenarios. Incorporation of realistic characters, settings, and events to create an immersive learning experience. Creation of detailed walkthroughs and guides that explain the objectives, tasks, and expected outcomes of each training exercise as well as hints and tips to assist participants in overcoming troubling challenges.

ES-30: Difficulty levels

Description: As a cybersecurity trainee, I want an adaptive difficulty system to ensure that the training exercises and scenarios match my skill levels.

Objectives: To create a comprehensive user profiling system that assesses the skill levels and learning preferences of each participant. To guide participants through increasing levels of difficulty, unlocking new challenges and opportunities as they demonstrate mastery.

Motivation: Personalized approaches ensure that participants of all skill levels can participate and progress at a pace that is suitable for their individual needs.

Building Blocks: Continuous monitoring of participant performance and progress throughout the training exercises. Detailed user profiles that capture the strengths, weaknesses, and learning patterns of each participant. Dynamic modification of exercise complexity, including the introduction of new challenges, the adjustment of time constraints, and the variation of task requirements.

6.3.6 NITRO Cyber Range Implementation

ES-31: Automated platform deployment and management

Description: As a system administrator, I want an automated way to deploy, configure, and manage the NITRO platform and all its components to ensure efficient and consistent 5G network setup and maintenance.

Objectives: To develop an automated system for the deployment, configuration, and management of the NITRO Cyber-Range platform, ensuring that all 5G components are consistently set up and maintained without manual intervention.

Motivation: To streamline the setup and maintenance processes, reduce the potential for human error, and ensure that the platform is always configured correctly and up-to-date.

Building Blocks: The automation system will utilize Infrastructure as Code (IaC) tools such as Terraform or Ansible for defining and provisioning all necessary infrastructure components like servers, networking, and storage, ensuring consistent and reliable setup. Container orchestration will manage containerized applications, maintaining uniform deployment across environments.

ES-32: Exercises in the cyber range without running the complete 5G stack

Description: As a cybersecurity trainee, I want the cyber range to offer exercises that do not require running the complete 5G stack because memory resources may not be adequate at a particular moment.

Objective: To guarantee continuous availability of exercises even in the most resource demanding situations (e.g., several trainees connected, memory issues, etc.).

Motivation: Comprehensive 5G network simulations are valuable for learning, but they can also be complex and resource-intensive. For certain training exercises, it's beneficial to have the option to focus on specific security skills and scenarios without the need to run the entire 5G stack.

Building Blocks: Design and development of targeted exercises that are lightweight in the sense that there is no need to run 5G core network to simulate attacks and defense scenarios.

ES-33: Access to preinstalled and diverse cybersecurity tools for training

Description: As a cybersecurity trainee, I want easy access to a variety of tools including 5G traffic generators and network fingerprinting tools so that I can gain practical experience and enhance my skills in network security.

Objective: To provide a training environment where key 5G security tools are pre-installed and readily available. This includes specialized tools for 5G traffic generation and network fingerprinting, among others. By achieving this, trainees will have immediate access to the resources they need, facilitating a smoother and more productive learning process.

Motivation: Cybersecurity trainees can fully concentrate on learning and practicing their skills without being impeded by the difficulty of finding and installing specialized 5G security tools.

Building Blocks: Selection of a comprehensive set of 5G security tools and installation. Detailed tutorials and practical exercises to guide trainees on how to use these tools effectively.

ES-34: Collecting attack traffic to create the NITRO data repository

Description: As a cybersecurity researcher, I want to collect attack traffic to create the NITRO data repository so that I can analyze various threat patterns and improve security measures.

Objective: The primary objective is to gather diverse attack traffic data from multiple sources, ensuring it is captured, stored, and organized within the NITRO data repository. This repository will provide a rich dataset for analyzing threat behaviours and improving overall network defences.

Motivation: To create a centralized and comprehensive repository of attack traffic data that can be used to enhance our understanding of 5G cyber threats. The datasets of the repository can be utilized to build robust AI models for intrusion detection in 5G networks.

Building Blocks: Establish a reliable method for capturing attack traffic of the cyber range platform. The data must be securely transmitted and stored in the NITRO data repository, ensuring data integrity and confidentiality. Third, the repository's architecture must be designed to handle large volumes of data, with capabilities for indexing, querying, and analyzing the collected attack traffic. Additionally, comprehensive documentation and guidelines will be developed to facilitate the use of the repository by researchers and analysts.

ES-35: Ensuring interoperability of the NITRO data repository

Description: As a system administrator, I want the NITRO data repository to support interoperability by accommodating different data formats like JSON and XML so that it can be seamlessly integrated with various systems and applications.

Objective: The primary objective is to develop and test the NITRO data repository's capability to store, retrieve, and manage data in multiple formats. By achieving this, the repository will become a versatile tool, capable of supporting different data interchange standards.

Motivation: In the field of cybersecurity, it is crucial to collect, store, and analyze network traffic data from various sources to detect and respond to potential threats. The NITRO data repository must be capable of handling multiple data formats, including JSON and XML, to ensure it can effectively manage and integrate attack network traffic data.

Building blocks: The repository's architecture must be designed to support multiple data formats natively, allowing seamless transitions between formats. This involves implementing parsers and serializers for JSON and XML, ensuring that attack network traffic data can be accurately converted and stored regardless of its original format.

6.3.7 Legal and Policy framework for NITRO Cyber Range

ES-36: Compliance with legal and policy frameworks

Description: As a Platform/Service Provider, I want to increase user adoption by ensuring the integration of strict data protection mechanisms (safeguarding user personal data) aligned with the EU data protection standards and regulations.

Objectives: To acquire and analyse the necessary information within the cyber range platform to verify compliance with legal and policy requirements. To identify and address any gaps in compliance to enhance overall system security.

Motivation: To improve the ability to identify system weaknesses. To strengthen protection mechanisms by ensuring all legal and policy safeguards are in place. To enhance trust and increase user adoption by demonstrating compliance with data protection standards.

Building Blocks: Auditing procedures which will take place with the creator providing access to all necessary information. The auditor will conduct interviews with key personnel and inspect system configurations while collecting data, including documentation, records, and evidence of compliance measures, from various components of the cyber range during the execution phase. Gap analysis will follow to identify gaps and areas of non-compliance and assess the potential hazards associated with these issues. The goal will be to ensure compliance with all required legislation. Re-audits will be conducted periodically to guarantee ongoing compliance and continuous improvement.

6.4 Mapping Requirements to Engineering stories and NITRO’s System Architecture

In this chapter, we aim to map NITRO’s requirements to the described user stories and also to make an initial mapping to the layers of the architecture defined in D2.2.

In addition, we performed the exercise of mapping NITRO’s functional and technical requirements to the corresponding components or layers of the system architecture. The mapping of requirements to architecture components serves several purposes:

1. **Traceability:** It allows stakeholders to trace each functional requirement back to the specific architectural element responsible for its implementation. This enhances transparency and ensures that nothing is overlooked during development.
2. **Alignment:** It ensures that the technical and functional aspects of the platform are fully aligned with NITRO’s objectives. This also helps in validating that the system architecture is appropriately designed to support the desired features and services.
3. **Optimization and Validation:** By clearly identifying which architectural components are responsible for which requirements, we can better assess whether the architecture is optimized for performance, scalability, and security. It also aids in the validation and verification processes, ensuring that all technical requirements are met by the architecture as designed.

This process will ensure that each requirement is directly associated with the architectural elements responsible for fulfilling it. By doing so, we create a clear and traceable link between the high-level objectives of the NITRO platform and the practical components that will deliver those functionalities. To facilitate this, we map each set of functional and technical requirements to their corresponding architecture components. The layers **CoreNet**, **AttackNet**, **TrafficNet**, **EduNet**, **PrivacyNet**, **SecureNet** as defined in D2.2 are logical representations of the main functionalities and cyber range components which are responsible among others to manage the core network emulation, enable threat and attack simulations, traffic simulations, user interactions, and ensure data privacy. This exercise is presented in the following table:

First, we provide an alignment of the requirements and the user stories.

Table 3: Requirements to Engineering Stories Mapping

ID	Requirement	Related User Stories	Architecture Components/ Layers
REQ-01	The platform should emulate realistic 5G traffic patterns with minimal jitter	ES-5, ES-9, ES-10, ES-11	CoreNet
REQ-02	Essential cybersecurity features must be integrated to monitor threats.	ES-15, ES-16, ES17, ES-34	SecureNet

REQ-03	The system should efficiently manage high-volume subscriber and device profiles.	ES-34, ES-11, ES-14	CoreNet, SecureNet
REQ-04	The system must ensure data confidentiality through encryption.	ES-36	All layers
REQ-05	User Equipment (UE) should interact seamlessly with the 5G Core network.	ES-1, ES-32	CoreNet
REQ-06	The system should support the addition of multiple User Equipment (UEs) without degradation of performance.	ES-34, ES-11, ES-14	CoreNet, TrafficNet, SecureNet
REQ-07	It should be possible to retrieve and inspect the 5G network traffic for analysis and troubleshooting.	ES-1, ES-15, ES-16, ES17, ES-34	CoreNet, SecureNet
REQ-08	Trainees should be capable of submitting flags or other approach to retrieve their progress.	ES-28, ES-29	EduNet
REQ-09	Metrics of the trainees' actions should be retrievable from the Cyber Range for assessment and feedback.	ES-28, ES-29	EduNet
REQ-10	The system must support dynamic scaling of core 5G components to handle varying user loads and network traffic.	ES-1, ES-31, ES-32	CoreNet
REQ-11	The cyber range must provide the capability to isolate network slices for distinct environments.	ES-6, ES-7	CoreNet
REQ-12	The system must intelligently allocate network bandwidth and support automatic rerouting to optimize performance under variable network load and congestion.	ES-32	CoreNet
REQ-13	The system must integrate with Kubernetes or similar to allow distributed deployments.	ES-31, ES-33	CoreNet
REQ-14	The platform should support capture the flag exercises for 5G networks	ES-1	EduNet, CoreNet,
REQ-15	The platform should offer tools for simulating reconnaissance attacks in 5G networks	ES-2, ES-3	CoreNet, AttackNet
REQ-16	The platform should allow to use traffic generators to perform replay attacks and traffic injection	ES-5	AttackNet, TrafficNet
REQ-17	Platform could simulate attack targeting 5G networks	ES-1, ES-2, ES-3, ES-4, ES-5, ES-6, ES-7	AttackNet, TrafficNet, CoreNet
REQ-18	Platform should simulate RCE attacks in a 5G environment and respond on them	ES-8, ES-19	AttackNet,, CoreNet, SecureNet
REQ-19	The cyber range should support simulation of service disruption attacks such as DoS	ES-9, ES-10	TrafficNet, SecureNet

REQ-20	The cyber range should support simulation of control plane disruption attacks and allow responding	ES-11, ES-19	CoreNet, AttackNet
REQ-21	Platform must deploy 5G NFs with deliberate misconfigurations	ES-12, ES-17	CoreNet, EduNet
REQ-22	The cyber range should support simulation of cascading attacks and respond on them	ES-13, ES-14, ES-21	AttackNet, SecureNet
REQ-23	Cyber range should support different types of attack scenarios and allow incident handling	ES-15, ES-16	AttackNet, SecureNet
REQ-24	Platform should offer predefined incident response procedures	ES-20	SecureNet
REQ-25	Platform could offer the means for training the communication of incidents	ES-21	EduNet, PrivacyNet
REQ-26	Cyber range should simulate scenarios with adversarial techniques for attacking AI models	ES-23, ES-24	AttackNet
REQ-27	Cyber Range should provide realistic storylines	ES-29	EduNet
REQ-28	Cyber Range should include scoring system and provide motivation to trainees	ES-27, ES-28	EduNet
REQ-29	Cyber Range should support trainees of different levels of knowledge	ES-30	EduNet
REQ-30	Cyber Range must be easy to install	ES-31	All layers
REQ-31	The platform should provide pre-installed cybersecurity tools for training	ES-33	SecureNet
REQ-32	Cyber Range should use only the required 5G elements	ES-32	CoreNet
REQ-33	Platform should gather and store interoperable attack traffic data from various sources	ES-34 , ES-35, ES-26	SecureNet
REQ-34	Platform must respect privacy of participants	ES-25, ES-36	All layers
REQ-35	Cyber Range should respect secure data retention and deletion practices	ES-26, ES-33, ES-36	All layers

7 NITRO 5G Cyber Range Implementation Aspects

For cybersecurity training and preparedness, the NITRO cyber range is a platform tailored for the challenges of 5G networks and IoT. Designed to replicate realistic 5G cyber threats and scenarios, NITRO integrates cutting-edge emulation of 5G components, including user devices. NITRO provides a dynamic environment where cybersecurity professionals can hone their skills through hands-on experience with tools for traffic generation, attacker simulation, and incident response. Generally speaking, the most important components of the NITRO cyber range platform are:

- Emulation of 5G components as well as devices and the radio network using virtualisation,
- 5G Traffic generation (i.e., fuzzing) and attacker tools (e.g., Nmap),
- An interface for administration and management of the cyber range platform supporting the creation of virtual topologies, information systems, and assets,
- Incidence response playbooks,
- Creation of NITRO data repository and knowledge base.

In deliverable D2.2, "NITRO cyber range architecture, testing and validation plans", these components are elaborated, and their interconnections will be presented. In this section, we briefly describe the underlying technologies, important tools and key components.

7.1 Building Blocks for the NITRO Cyber-Range

7.1.1 Virtualization with containers

Modern cyber ranges typically cannot support many users simultaneously, usually accommodating fewer than tens of users with topologies of up to 50 components on a rack server with a Xeon Gold processor and 256 GB of RAM. Cyber range deployments also require specific network configurations based on their experimentation methods, which may include emulation or simulation. Emulation is the most widely used approach in modern cyber ranges since VM technology is stable enough. Examples of network emulation environments include Emulab⁶ and DETER⁷ in academia. The key technology that will allow NITRO to emulate 5G services is virtualization technology and particularly containers.

The architecture of NITRO will be founded on a Docker-based virtualization framework designed to create a lightweight yet efficient emulation environment for both 5G network components and cybersecurity scenarios [18]. Docker is an open-source container platform that excels in orchestrating a lightweight virtual environment conducive to code execution, application migration, and enhanced project collaboration. Docker notably surpasses Virtual Machines (VMs) in execution and startup efficiency, demonstrating at least a fifty per cent enhancement in performance. The containerization technique inherent in Docker not only streamlines scalable, on-demand service delivery but also significantly curtails IT operational expenses. In contrast, VMs, conceptualised as software constructs

⁶ <https://www.emulab.net/portal/frontpage.php>

⁷ https://deter-project.org/about_deter_project.html

within a host environment, offer extensive operating system functionalities appropriate for a broad spectrum of software applications, yet their efficiency is comparatively subdued when placed against Docker containerized approach. Thus, Docker is employed to create a virtualised environment, hosting different network elements, attack emulations, and countermeasures, offering a realistic and adaptable training environment.

7.1.2 Emulation of 5G Core network

Previous generations of mobile networks relied on dedicated hardware to support core network functions, but 5G introduces a new architecture where these functions are achieved in software. This shift from hardware to software benefits cybersecurity by preventing and containing present and future attacks and allowing for patch and update procedures. This recognition has stimulated open-source projects for the implementation of 5G radio access and core networks, such as free5GC, Open5GS, and OpenAirInterface (OAI), which allow complete network stacks to be implemented over commercial-off-the-shelf hardware. Software-based implementations facilitate the evolution of the network, allowing the development and rollout of new functionality without necessarily replacing hardware. For example, open-source software projects have become an important driver to the establishment of private 5G network deployments, which are becoming a viable alternative to operate large-scale wireless networks in industrial environments.

Open5GS⁸ is an open-source software, implements the core functionalities of the Core Network and Evolved Packet Core (EPC), enabling the creation of private and commercial network solutions. It comes with a Web application for managing UE subscription information, suitable for testing. The implementation of Open5GS is based on the 3GPP specifications Release 17 with a rich set of supported features such as IPv6 support, the capability to handle multiple PDU sessions, handover functions, and integration of Voice over LTE and Voice over 5G New Radio. Compared to other 5GC projects, Open5GS benefits from a larger contributor base, resulting in weekly commits to its repository and more frequent software releases. However, Open5GS does not offer official releases of container images for Open5GS's components; thus, users must build images if they want to deploy them in container-based environments.

Free5GC⁹ offers container image releases to facilitate its usage and provides a Docker Compose file for automated network function deployment. Additionally, the contributors of free5GC have maintained a list of articles, studies, and tutorials for those new to the platform. At the time of writing this text, the latest version of Free5GC is 3.4.1.

7.1.3 Emulation of devices and radio network

UERANSIM¹⁰ is a 5G RAN emulation tool, simulates 5G base stations (gNodeB) and UEs (i.e., mobile devices, IoT devices, etc.) for network protocol testing and scenario emulation. These components are

⁸ <https://open5gs.org>

⁹ <https://free5gc.org/>

¹⁰ <https://github.com/aligungr/UERANSIM>

crucial for providing a genuine 5G network emulation environment, essential for hands-on cybersecurity training and performing testing in 5G far edge.

Android Emulator¹¹ is a virtual machine that emulates an Android device on a computer for testing by developers. It allows testing of applications on a variety of devices and Android API levels without needing to have each physical device.

7.1.4 5G Traffic generator and Attack Simulation

5Greplay is an open-source 5G network traffic fuzzer designed to evaluate 5G components by replaying and modifying 5G network traffic and injecting network scenarios into a target, which can be a 5G core service (e.g., AMF, SMF) or a RAN network (e.g., gNodeB). NITRO will utilize 5Greplay for recreating attack scenarios such as replay attacks, enhancing the training experience with realistic cyberattack emulations [19].

7.1.5 NITRO data repository of 5G and IoT attacks

One of the objectives of NITRO is to pave the way for the creation of 5G-related intrusion/anomaly detection data repository that can be used among others for the training process of AI-based Intrusion detection and prevention systems. The data set is the backbone for the construction of an efficient AI model. However, given the lack of 5G-related cyberattacks and the sensitive nature of such data, to the time of writing this deliverable, there are no publicly available intrusion detection data sets related to 5G and 6G communications. The NITRO data repository will provide a robust and secure platform for storing, managing, and sharing 5G cybersecurity related data. Its primary function is to support interoperability, enabling seamless data exchange between different systems. This capability is crucial for facilitating collaboration and continuity in cybersecurity research and development, particularly for subsequent similar projects and cyber ranges. By ensuring that data can be shared without compromising security, the repository helps to advance the collective understanding and defence against 5G cyber threats.

In addition to its interoperability, the NITRO data repository will be designed with security measures to prevent information leakage. This includes encryption techniques for both data at rest and in transit, as well as access control mechanisms to restrict unauthorized access. By combining these security features with a comprehensive data management system, the repository ensures that sensitive information remains protected while still being accessible for legitimate and necessary use.

7.1.6 Security Tools for Incident Detection

For the needs of NITRO cyber range, we shall provide users with a set of tools to perform the incident detection and response. We won't focus on complex systems such as Security Orchestration, Automation, and Response tools (SOAR) but our focus will be to use widely available and used solutions that offer basic detection capabilities, such as IDS and SIEM and will also focus on response based on IPS and EDR/XDR offerings.

¹¹ <https://source.android.com/docs/setup/create/avd>

Intrusion Detection and Prevention Systems (**IDS/IPS**) are cybersecurity tools designed to monitor network or system activities for malicious behaviour and respond accordingly. An IDS passively observes and analyses traffic, generating alerts when it detects potential threats, but it does not take action to stop them. In contrast, an IPS actively blocks identified threats by preventing malicious traffic from reaching its destination. Both systems use techniques like signature-based detection (identifying known patterns) and anomaly-based detection (flagging unusual behaviours). Together, IDS/IPS enhance network security by identifying and mitigating risks such as unauthorized access, malware, and denial-of-service attacks.

A Security Information and Event Management (**SIEM**) solution is a virtualised software offering real-time monitoring and notification of security events in the network's topology. A SIEM provides logging, storage, and analytics, along with a dashboard view for data presentation and an interface for training SOC and/or CSIRT operators. It can be deployed on demand and adapted to various information sources and expected learning outcomes.

Finally, Endpoint Detection and Response (**EDR**) and Extended Detection and Response (**XDR**) platforms integrates data from multiple security layers—such as endpoints, networks, servers, email, and cloud environments—into a unified platform for enhanced threat detection, investigation, and response. By correlating data across these layers, XDR identifies complex attacks, reduces alert fatigue, and provides a holistic view of an organization's security posture. It streamlines incident response by offering automated workflows and actionable insights, making it a powerful tool for managing sophisticated and evolving cyber threats.

For our work in the project, we envision Wazuh¹² and Suricata as main candidates for our needs. Wazuh is an open-source security platform that provides unified threat detection, visibility, and response capabilities. It combines functionalities such as Security Information and Event Management (SIEM), endpoint detection and response (EDR), and compliance management. Wazuh collects and analyses data from endpoints, networks, and cloud environments to detect anomalies, security threats, and vulnerabilities. With its lightweight agents and scalability, Wazuh is widely used for real-time monitoring, incident response, and meeting regulatory requirements across diverse IT infrastructures.

Suricata is an open-source, high-performance network monitoring and intrusion detection/prevention system (IDS/IPS) capable of real-time traffic analysis. It inspects network packets to identify malicious activity by using signature-based and anomaly-based detection methods. Suricata supports multiple protocols, including HTTP, DNS, TLS, and SMB, and provides deep packet inspection for comprehensive threat detection. It is highly scalable and integrates well with modern security tools, offering features like multi-threading, logging, and flow-based analysis. Widely used in cybersecurity environments, Suricata helps protect networks from a variety of threats while providing detailed insights into traffic

¹² <https://github.com/wazuh/wazuh>

behaviour.

7.2 NITRO Cyber Range Platform

NITRO will deliver an innovative platform capable of addressing the evolving challenges of network security in the 5G era. This platform will be provided for extended testing to verify it cover the needs of various stakeholders, providing a foundation for future enhancements and broader implementation. The NITRO cyber range will provide a virtual environment for cyber warfare training and technology development. This will include the emulation of 5G components and IoT devices. Moreover, adversarial and robust AI training scenarios for 5G networks will be included, as well as incident response tailored for 5G. A data repository will collect attack data flows within the NITRO 5G testbed. Using methods like network sniffing, it will capture real-time network traffic and logs from virtual devices and applications. This data will be crucial for training Machine Learning algorithms and feeding into a 5G SIEM.

The evaluation, will be performed in the scope of WP5 where stakeholders will provide feedback in two phases in order to refine and improve the provided solution, as feedback from stakeholders will be incorporated to enhance the platform's capabilities.

7.2.1 KPIs Discussion

To elaborate more on the planned platform the following metrics, performance indicators, and KPIs have been identified.

Table 4: Identified NITRO KPIs

Metric	Description	Relevant KPIs
Type of Attacks	Simulated attacks on 5G components such as NFV, SDN, IoT devices, network slicing, and virtualization layers.	Must cover a variety of attack vectors, including at least 3 distinct types (e.g., DoS, DDoS, RCE).
Type of AI attacks	Adversarial and Robust AI training scenarios for 5G networks.	At least 2 different AI models to be considered. At least 2 different adversarial techniques to be included. At least 1 robust AI technique should be considered.
Simulation/Emulation	Simulation of 5G components and IoT devices; Simulation of various cyber threats and attack scenarios.	Successful simulation of at least the main building blocks of the 5G core and accurate simulation of at least 3 cyber threats.
Users Concurrently Supported	Number of concurrent users the platform can support for training and testing purposes.	Support for at least 150 concurrent users without performance degradation.
Stakeholder	Engagement and validation	Active participation and constructive



Involvement	feedback from stakeholders such as cybersecurity experts and students.	feedback.
Data Collection and Monitoring	Metrics on the volume and quality of data collected for ML training and SIEM analysis.	Successful collection and processing of data from 100% of test scenarios.
Training and Testing Environment	Evaluation of the robustness and realism of the simulated cyber range environment for training purposes.	Realistic training scenarios with at least 90% participant engagement and scenario completion.
Performance and Reliability	System uptime, reliability, and performance metrics of the NITRO platform during testing.	At least 99.5% system uptime during testing periods and no critical failures.

8 Use Case Scenarios

This section analyses and describes the use cases and scenarios that will validate the NITRO platform. Particularly, NITRO consists of two discrete use cases: i) **Cybersecurity Testing of 5G and IoT Applications and Network Services**: It ensures a safe environment without the risk of proprietary data loss or adverse impact on existing networks. The test bed infrastructure consists of high-performance and state-of-the-art equipment, including IoT physical hardware, programmable radio, computing, and networking technologies, deployed at UBI premises; and ii) **Security Training for ECSC**: Questionnaire will be prepared and disseminated to the participants -- users that comprise the members of the Hellenic Cyber Security Team, the Greek National Team that participates to the European Cyber Security Challenge (also known as ECSC) -- for feedback and evaluations consisting of questions that will assess both technical and usability aspects of the NITRO platform. The description of NITRO use cases is structured under the following format:

Table 5: Use case description template

Title: <i>Brief description of the use case</i>	
Overview	Key objectives/Outcomes
<i>Brief description of the use case</i>	<i>Enumeration of the goals/objectives of the use case.</i>
Description	
<i>Detailed description of the use case</i>	
Scenarios to be demonstrated	
<i>Brief analysis of the scenarios that comprise the corresponding use cases.</i>	

8.1 Use Scenario 1: Cybersecurity Testing of 5G and IoT Applications and Network Services

This use case involves the development of a demonstrator to validate the effectiveness of the NITRO cyber range as a testbed for conducting tests, security assessments, and emulating network-wide rudimentary and complex attacks on IoT and 5G applications, network services, and network control elements. It ensures a safe environment without the risk of proprietary data loss or adverse impact on existing networks.

We will explore various interconnection scenarios of IoT devices and demonstrate monitoring and emulation of attacker entities through a set of representative vulnerability tests. This task will cover and evaluate all functionalities of NITRO platform and specially the 5G-IoT adversarial attacks for evasion of machine learning models. Moreover, this task will give feedback for a second round of the technical tasks in WP3 and WP4.

Table 6: Use Case Scenario UC1.1 (Cybersecurity Fundamentals and Incident Response)

UC1.1: Cybersecurity Fundamentals and Incident Response	
Overview	Key Objectives/Outcomes
This use case focuses on foundational cybersecurity concepts, threat detection, and incident response processes in 5G networks. It emphasizes hands-on training in analyzing traffic, identifying malicious patterns, and implementing defensive measures.	Understand 5G architecture and protocols. Develop skills for traffic analysis and network traffic and NetFlow extraction. Train students in initial response to cyber incidents. Enhanced understanding of 5G-specific security challenges. Competence in traffic flow analysis and IoC detection. Ability to perform basic incident response tasks. Initial response to cyber incidents.
Description	
Students will explore the fundamentals of 5G and network security. They will analyze network traffic to identify malicious patterns and extract network traffic. Through interactive exercises, students will simulate reconnaissance activities and replay attacks, learning how to detect and mitigate these threats. By the end of the use case, students will gain practical skills in traffic analysis and performing initial responses to cyber incidents within 5G environments.	
Scenarios to be demonstrated	
- Fundamentals – Overview of 5G network components and security features. - Reconnaissance – Identifying reconnaissance activities and mitigating them. - Traffic/Flow Extraction – Analyzing network flows and extract to detect anomalies. 5G Replay – Simulating a replay attack to disrupt network operations and demonstrating mitigations.	

Table 7: Use Case Scenario UC1.2 (Threat Detection and Mitigation)

UC1.2: Threat Detection and Mitigation	
Overview	Key Objectives/Outcomes
This use case dives into detecting, analyzing, and mitigating complex threats, including Distributed Denial of Service (DDoS), adversarial AI, and Advanced Persistent Threats (APTs).	Learn strategies for detecting and mitigating DDoS attacks. Understand adversarial AI tactics and develop countermeasures. Analyze APT campaigns. Advanced knowledge of threat actor tactics in 5G environments. Skills to implement AI-based threat detection and mitigation systems. Proficiency in handling APTs with realistic simulation exercises.
Description	
Students will explore DDoS attacks on 5G infrastructure and apply defense strategies, explore adversarial AI tactics and defenses, and use IDS and SIEM tools to identify cyber threats. Additionally, students will simulate the entire lifecycle of an APT attack, from initial breach to data exfiltration, gaining practical experience in combating advanced persistent threats. By the end, students will develop advanced skills in threat detection and mitigation	
Scenarios to be demonstrated	

- DDoS Attack – Simulating a DDoS attack on 5G infrastructure and mitigating it.
- Adversarial AI – Demonstrating adversarial attacks on AI-based systems and applying defenses.
- Intrusion Detection and Threat Management – Usage of IDS and SIEM tools to identify and understand cyberthreats.
- Cyber Kill Chain Emulation – Emulation of an multiple techniques that correspond to APT lifecycle in a 5G environment.

Table 8: Use Case Scenario UC1.3 (Critical Infrastructure and Emerging Threats)

UC1.3: Critical Infrastructure and Emerging Threats	
Overview	Key Objectives/Outcomes
This use case focuses on securing critical infrastructure, including healthcare systems and drone communication in 5G networks. It also explores the risks of remote code execution (RCE), malware, and data leaks.	Protect healthcare systems and IoT devices operating on 5G. Understand the risks and mitigation strategies for data leaks and RCE. Learn how to secure drones and autonomous systems against cyber threats. Expertise in safeguarding critical infrastructure. Familiarity with emerging threats in 5G-enabled environments. Proficiency in applying mitigation techniques to protect IoT and drone systems.
Description	
Students will navigate and cover key concepts such as data leaks, malware, and remote code execution (RCE), providing an in-depth understanding of the risks and mitigation strategies. Through interactive exercises, students will simulate attacks on healthcare IoT devices and drone communication channels, identify vulnerabilities, and apply security measures to protect these systems from emerging cyber threats	
Scenarios to be demonstrated	
• Data Leaks – Identifying and addressing sensitive data exposure. • Malware - Explores the foundational aspects of malware analysis and incident response in a 5G environment, focusing on detecting, analyzing, and mitigating malware threats. • Remote Code Execution (RCE) – Simulating and mitigating RCE attacks. • Drone/UAV/Automotive Infrastructure – Securing drone communication channels against cyberattacks. • Healthcare Infrastructure – Simulating attacks on healthcare IoT devices and securing them.	

8.2 Scenario 2: Security Training for ECSC

This use case will engage users that comprise the members of the Hellenic Cyber Security Team, the Greek National Team that participates in the European Cyber Security Challenge (ECSC). ECSC is the biggest international cyber security contest, which is supported by many European countries and ENISA. ECSC that takes place annually, aims at engaging cybersecurity talents across Europe and competing against each other by participating in national teams. UPRC participates in the steering committee of the ECSC, leading the Greek participation. Except from the Hellenic team, UPRC will also invite the rest of the national teams that participate to the ECSC to evaluate and assess the NITRO platform. The objectives of the demonstration implementation are: (i) to install and technically

validate the NITRO Cyber range in real cases, (ii) to test and monitor its performance, and (iii) obtain baseline measurements of KPIs. Questionnaire will be prepared and disseminated to the participants for feedback and evaluations. Questions will assess both technical aspects and usability aspects of the platform. Moreover, this task will give feedback for a second round of the technical tasks in WP3 and WP4.

Table 9: Use Case Scenario UC2.1 (Familiarize with the 5G Technology)

UC2.1: Familiarize with the 5G Technology (Architecture & Network)	
Overview	Key Objectives/Outcomes
This use case introduces members of the Greek ECSC team to the foundational concepts of 5G technology, including its architecture and key components. Participants will explore the structure and operations of a 5G network in a simulated environment, gaining hands-on experience.	Understand the 5G architecture and its primary components. Explore the interconnections and communication processes within a 5G network. Build foundational knowledge for advanced scenarios like attacks or troubleshooting.
Description	
Members of the ECSC team will navigate through a guided walkthrough of 5G architecture using the NITRO platform. The walkthrough will include information on the 5G network layers, it will provide information on the role of each 5G component of the architecture. The interactive exercise will allow the members of the ECSC team to identify and understand 5G components, as well as their roles in data routing, control, and management.	
Scenarios to be demonstrated	
• Interactive learning about the 5G architecture. • Simulations showing data flow between 5G components. • Exercises on mapping real-world infrastructure to 5G models	

Table 10: Use Case Scenario UC2.2 (Interact with the 5G Core)

UC2.2: Interact with the 5G Core (Resonance, Scan Components, Interact with Components, Inspect Traffic)	
Overview	Key Objectives/Outcomes
This use case engages members of the ECSC team in a hands-on exploration of the 5G Core. Participants will learn how to scan, interact with, and inspect components within the core network, fostering deeper technical insights into its operation and the protocols used.	Perform scans of 5G Core components to identify active elements. Understand the role of individual 5G components. Analyze traffic within the 5G Core.
Description	
The ECSC team will use the NITRO platform to simulate interactions with the 5G Core. They will first perform network scans to identify active components, followed by a guided exercise to explore their configurations. Traffic analysis exercises will allow participants to inspect data packets, observe routing behaviors, and identify traffic patterns. These activities will prepare participants for advanced operational scenarios like attack simulations or troubleshooting.	
Scenarios to be demonstrated	
- Scanning and identifying active 5G Core components. - Exploring the configuration and behavior of 5G elements. - Traffic inspection and analysis of network flows in real-time.	

Table 11: Use Case Scenario UC2.3 (Perform an Attack on the 5G Core)

UC2.3: Perform an Attack on the 5G Core (Provide Information for the Attack and Have the Players Conduct It)	
Overview	Key Objectives/Outcomes
This use case challenges the members of the ECSC team to execute a simulated cyberattack on the 5G Core. The exercise involves understanding the nature of the attack, planning, and executing it while monitoring the system's response.	Learn the process of identifying vulnerabilities in a 5G network. Plan and execute a cyberattack on a simulated 5G Core. Understand the impact of such attacks on the network and its components.
Description	



The participating members of the ECSC team will receive detailed information about a specific vulnerability within the 5G Core. Using the NITRO platform, they will plan and execute an attack on designated components. Throughout the exercise, participants will monitor system responses and evaluate the effectiveness of the attack, gaining insights into how real-world attackers exploit weaknesses in 5G systems.

Scenarios to be demonstrated

- Briefing on vulnerabilities in the 5G Core.
- Planning and executing attacks on the 5G Core.
- Monitoring system responses and analyzing attack outcomes.

9 Conclusions

Deliverable D2.3 represents a crucial initial step in the NITRO project, laying a comprehensive foundation for the development of a 5G tailored Cyber-Range ecosystem. This document has addressed the multifaceted requirements necessary for creating an advanced, secure, and legally compliant Cyber-Range platform. The deliverable began by articulating the vision of the NITRO project, emphasizing the necessity of a state-of-the-art Cyber-Range ecosystem capable of addressing the unique challenges and security needs of 5G and IoT networks. This vision provided the overarching framework guiding the detailed analyses and strategic recommendations contained within this document.

A significant focus was placed on the development of a 5G tailored threat playbook. By identifying and analysing potential cyber threats to both the 5G core and far-edge networks, this deliverable has established a robust foundation for the creation of realistic and effective cyber security training scenarios. These scenarios are vital for preparing cybersecurity professionals to effectively manage and mitigate 5G-specific threats. The exploration of adversarial AI within the 5G ecosystem highlighted the emerging risks posed by AI-driven cyberattacks. This section underscored the importance of developing sophisticated defensive strategies to counteract these threats, ensuring the resilience and integrity of 5G networks.

In constructing a privacy-preserving Cyber-Range platform, the deliverable outlined essential mechanisms for data protection and compliance with relevant privacy laws. This ensures that the platform not only provides a secure environment for training and evaluation but also adheres to stringent data privacy standards. The inclusion of a 5G incident response playbook further strengthens the Cyber-Range ecosystem by providing detailed procedures and best practices for managing security incidents. This playbook enhances the readiness and effectiveness of incident response teams, contributing to a more resilient cyber defence framework.

Evaluation metrics for offensive and defensive strategies were also detailed, offering a structured approach to assess and improve cybersecurity practices within the Cyber-Range. These metrics are crucial for continuous improvement and ensuring that the Cyber-Range remains an effective tool for cybersecurity training and evaluation. Legal and policy requirements were comprehensively addressed, ensuring that the Cyber-Range ecosystem complies with EU and international laws, as well as industry-specific regulations. This compliance is essential for the legal viability and acceptance of the Cyber-Range platform. The requirements for a proof-of-concept environmental testbed were outlined, providing a clear roadmap for validating the effectiveness and practicality of the Cyber-Range ecosystem. This testbed will be instrumental in demonstrating the feasibility and robustness of the proposed solutions.

Lastly, the NITRO methodology for developing a Minimum Viable Product (MVP) was detailed, ensuring a structured and iterative approach to the project's development. This methodology aligns with the overall project goals and facilitates efficient progress towards achieving the project's



objectives.

In conclusion, deliverables D2.1 and D2.3 laid a strong and comprehensive foundation for the NITRO project. By addressing the technical, legal, and policy requirements, and by proposing detailed use case scenarios, this document sets the stage for the successful development and implementation of a 5G and IoT tailored Cyber-Range ecosystem. The insights and frameworks provided herein will guide the subsequent phases of the project, ensuring that the NITRO project meets its strategic objectives and significantly enhances cybersecurity capabilities within the 5G domain.

References

- [1] Sullivan, S., et al. "5G security challenges and solutions: a review by OSI layers." IEEE Access 9 (2021): 116294-116314.
- [2] Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." Computers & Security 88 (2020): 101636.
- [3] Zolotukhin, Mikhail, et al. On attacking future 5g networks with adversarial examples: Survey. Network 3.1 (2022): 39-90.
- [4] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 371-390). IEEE.
- [5] Chicaiza, Janneth, et al. "Application of data anonymization in Learning Analytics." Proceedings of the 3rd International Conference on Applications of Intelligent Systems. 2020.
- [6] Attaran, Mohsen. "The impact of 5G on the evolution of intelligent automation and industry digitization." Journal of ambient intelligence and humanized computing 14.5 (2023): 5977-5993.
- [7] Basu, Deborsi, Raja Datta, and Uttam Ghosh. "Softwarized network function virtualization for 5g: Challenges and opportunities." Internet of Things and Secure Smart Environments (2020): 147-192.
- [8] Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini. "5G In the internet of things era: An overview on security and privacy challenges." Computer Networks 179 (2020): 107345.
- [9] Zhang, Chuan, et al. "Artificial intelligence for 5G and beyond 5G: Implementations, algorithms, and optimizations." IEEE Journal on Emerging and Selected Topics in Circuits and Systems 10.2 (2020): 149-163.
- [10] Vakaruk, S., Mozo, A., Pastor, A., & López, D. R. (2021, July). A digital twin network for security training in 5G industrial environments. In 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI) (pp. 395-398). IEEE.
- [11] Butun, I., Österberg, P., & Song, H. (2020). Security of the internet of things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.
- [12] Benzaïd, Chafika, and Tarik Taleb. "AI for beyond 5G networks: A cyber-security defense or offense enabler?" IEEE network 34.6 (2020): 140-147.
- [13] Chicaiza, Janneth, et al. "Application of data anonymization in Learning Analytics." Proceedings of the 3rd International Conference on Applications of Intelligent Systems. 2020.
- [14] Jones, Kyle ML, et al. "'We're being tracked at all times': Student perspectives of their privacy in relation to learning analytics in higher education." Journal of the Association for Information Science and Technology 71.9 (2020): 1044-1059.
- [15] Van Steen, T., & Deeleman, J. R. (2021). Successful gamification of cybersecurity training. Cyberpsychology, Behavior, and Social Networking, 24(9), 593-598.
- [16] Khairallah, Obay, and Ma'moun Abu-Naseer. "The effectiveness of gamification teaching method in raising awareness on Email Phishing: Controlled Experiment." (2024).

- [17] Tseng, Shih-Lun "Allen, et al. "Rethinking Gamification Failure: A Model and Investigation of Gamified System Maladaptive Behaviors." *Information Systems Research* (2023).
- [18] Yadav, R.; Sousa, E.; Callou, G. Performance comparison between virtual machines and docker containers. *IEEE Lat. Am. Trans.* 2018, 16, 2282–2288
- [19] Salazar, Z.; Nguyen, H.N.; Mallouli, W.; Cavalli, A.R.; Montes de Oca, E. 5Greplay: A 5G network traffic fuzzer—application to attack injection. In *Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021*; pp. 1–8.
- [20] Glas, Magdalena, Gerhard Messmann, and Günther Pernul. "Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises." *Computers & Security* (2024): 103965.
- [21] NIS2 Directive. (n.d.). Overview of the NIS2 Directive. Available: <https://www.nis-2-directive.com/>