
DIEM - University of salerno
Master's degree in Computer Engineering
Situation Awareness

---

# Report
# Project 3: E-learning

Lecturers:
*Giuseppe D'Aniello,*
*Matteo Gaeta*

Group 6 Members:

| **Surname** | **Name** | **Number** | **E-mail** |
|---|---|---|---|
| Galasso | Gianluca | 622702000 | g.galasso33@studenti.unisa.it |
| Iovaro | Damiana | 622702017 | d.iovaro@studenti.unisa.it |
| Murati | Camilla | 622702126 | c.murati@studenti.unisa.it |
| Sellitto | Marco | 622702105 | m.sellitto13@studenti.unisa.it |

2023/2024

# Contents

# Chapter 1

# Introduction

The objective of this project is to implement a comprehensive e-learning system designed to assist users in tailoring their learning pathways and enhancing their skill sets. Developed with a strong emphasis on situational awareness, this project is structured into two primary components: the first involves *Goal-Driven Task Analysis* (GDTA), and the second focuses on the implementation of an integrated dashboard.

This system is meticulously crafted with a **User-Centric Approach**, ensuring that users can effectively monitor their competencies and track their learning progress. In developing the GDTA, we delineated operational concepts through detailed personas and scenario analysis, ensuring that the system is attuned to the diverse needs and contexts of its users.

For the dashboard implementation, we leveraged *ElasticSearch* as the underlying database and *Kibana* as the visualization tool. The data presented on the dashboard were specifically curated for this project and are stored in multiple .csv files.

Initially, our goal was to conduct a comprehensive data analysis using an extensive dataset found online. However, we faced significant challenges in locating suitable data that aligned perfectly with our needs. Consequently, we chose to create our own .csv files containing the essential data required to populate our dashboard.

This decision granted us full control over the data, enabling precise customization according to the specific requirements of our project. By curating our own dataset, we ensured the accuracy and relevance of the information presented, thereby facilitating a more insightful and effective implementation of our e-learning system.

# Chapter 2

# Data Analysis

# Chapter 3

# Operational Concept

We questioned which requirement could be critical for a Situational Awareness System. This phase involved identifying and understanding the essential needs that the system must fulfill to be effective and user-friendly.

To achieve this, we conducted a detailed analysis of the *Operational Concept*, which involved the development of detailed personas and scenario analysis.

The Operational Concept is a critical phase in the design of complex systems, translating system requirements into actionable plans. It provides a comprehensive understanding of the system's operational environment, including the roles and responsibilities of the users, the tasks they perform, and the context in which they operate.

Since we are developing an e-learning dashboard intended for users who may access it from various locations, we have not defined specific environmental constriants. The flexibility of online learning environments means that users could be utilizing the system in diverse settings, such as homes, offices, or public spaces, each with varying levels of connectivity and hardware capabilities. Additionally, given the global reach of e-learning platforms, environmental conditions can differ widely among users, making it impractical to impose rigid environmental constraints.

## 3.1 Scenario

The company requires all employees to pursue upskilling or reskilling opportunities based on their previous studies and work experiences. Marta and Matteo are two employees whose skills and knowledge will be monitored to ensure they can effectively contribute to projects in the Offensive Cybersecurity field. The company's e-learning platform provides courses that enable employees to obtain the *OSCP* (Offensive Security Certified Professional) certification.

The platform is accessible both on-site at the company and remotely, offering flexible learning options that accommodate diverse schedules. Each employee receives a personalized dashboard where they can track their progress and access a wide range of educational resources, including video courses (concept pills), slide decks, and practical exercises. At the end of each module, employees can take assessments to reinforce their understanding and ensure they meet the learning objectives.

Additionally, the platform includes analytics and trend reports that help employees understand their learning journey, estimate the time required for course completion, and measure their engagement levels. The course design features a tailored approach, continuously monitoring each employee's performance and adapting to their specific learning needs. This customization

enhances the overall learning experience, ensuring employees are well-prepared for the OSCP certification.

## 3.2 Supported Figure: Matteo

Matteo is a student from the University of Salerno, with a bachelor's degree in Computer Engineering. His passion for cybersecurity has led him to specialize in this field, acquiring basic skills ranging from understanding the fundamentals of cybersecurity to networking and network protocols, from vulnerability analysis to familiarity with essential security tools. Now, Matteo faces a new challenge: a project in collaboration with Marta concerning Offensive Cybersecurity. However, to best address this task, Matteo needs to broaden his skills and knowledge.

| **Characteristic** | **Description** |
|---|---|
| Age Range | 20-25 |
| Gender | Male |
| Culture | Italian |
| Education | Bachelor's degree in Computer Engineering |
| Language | Italian, English (proficient for technical literature) |
| Frequency of Use | Several times a week |
| Experience | Familiar with basic cybersecurity tools and platforms, intermediate programming skills |
| Personality | Curious, analytical, detail-oriented, enjoys problem-solving, goal-oriented, collaborative |
| Acquired Skills | Fundamentals of cybersecurity, networking, vulnerability analysis, basic scripting/programming, offensive cybersecurity |
| Learning Style | Visual and hands-on learner |

## 3.3 Supported Figure: Marta

Marta is a student from the University of Naples Federico II. She completed a bachelor's degree in Computer Engineering and has now specialized in machine learning, acquiring basic skills in the field of artificial intelligence, including the structure and applications of neural networks and deep neural networks, their applications in robotics, and autonomous driving. Marta wants to collaborate with Matteo on a new project in the field of Offensive Cybersecurity. Since Marta has followed a different academic path from Matteo's, which does not involve cybersecurity, she needs to upskill her competencies.

| **Characteristic** | **Description** |
|---|---|
| Age Range | 20-25 |
| Gender | Female |
| Culture | Italian |
| Education | Bachelor's degree in Computer Engineering, specializing in Machine Learning |
| Language | Italian, English (proficient for technical literature) |
| Frequency of Use | A few times a week |
| Experience | Skilled in AI and Machine Learning platforms, novice in cybersecurity |
| Personality | Innovative, inquisitive, enjoys learning new skills, collaborative, adaptable |
| Acquired Skills | Basics of AI, neural networks, deep learning, robotics, autonomous driving, basic programming, willingness to learn cybersecurity |
| Learning Style | Visual and auditory learner, prefers structured guidance |

# Chapter 4

# Goal-Directed Task Analysis

We applied the *Cognitive Task Analysis* (CTA) methodology to explore individuals' knowledge and thought processes. Among the various CTA methodologies available, we selected *Goal-Directed Task Analysis* (GDTA), specifically focusing on Situation Awareness (SA) and the goals inherent in SA processes.

GDTA is tailored to identify user goals, the decisions they make, and the critical information needed to achieve these goals. This methodology not only maps out user objectives but also provides insights into their decision-making strategies and information requirements.

By employing GDTA, our aim is to deepen our understanding of how users perceive and interact with information. This understanding informs our design process, ensuring that our solutions align closely with user needs and preferences. Ultimately, this approach enhances the usability and effectiveness of our project outcomes by prioritizing User-Centric design principles.

## 4.1 Intial GDTA Goal Tree

The initial GDTA Goal Tree, shown in Figure 3.1, identified three Major-Goals. However, after an in-depth review and analysis, we concluded that the Major-Goal 1 **"Identify prior knowledge in the field of Cybersecurity"** can be integrated into the Major-Goal 2 **"Define and evaluate the knowledge required for Offensive Cybersecurity by monitoring students' progress"**. This conclusion was drawn from a comprehensive analysis of the sub-goals associated with Major-Goal 1.

Upon examining the sub-goals of Major-Goal 1, it became evident that both the sub-goals and the Major-Goal itself address topics that students need to master throughout their learning journey in cybersecurity. Given that Major-Goal 2 aims to delineate the specific topics and skills students must acquire, we decided to incorporate Major-Goal 1 as a sub-goal within Major-Goal 2. This integration ensures a more cohesive framework for evaluating and defining the necessary knowledge for Offensive Cybersecurity.

Furthermore, the sub-goals of Major-Goal 1 have been reclassified as Level 2 elements, signifying their importance in the comprehension phase of the learning process.

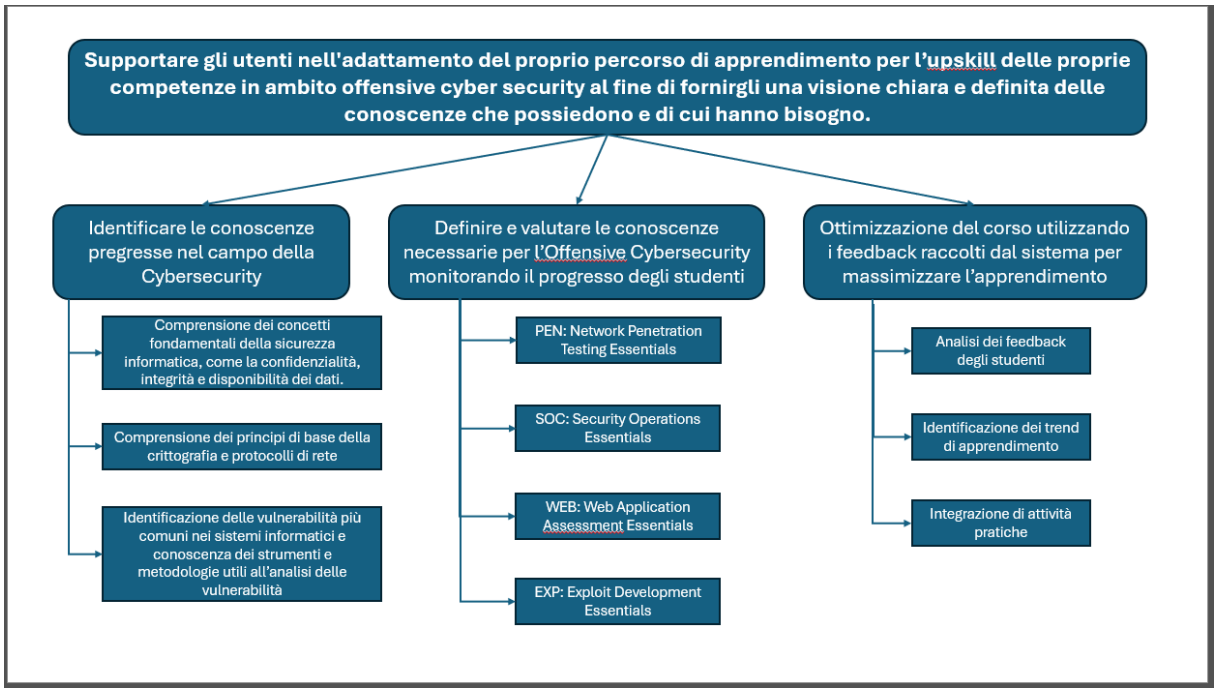


Figure 4.1: Initial GDTA Goal Tree

## 4.2 Final GDTA Goal Tree

In Figure 3.2, we present our Final GDTA Goal Tree, which outlines the primary goals of the system and the sub-goals that contribute to their achievement. In particular, our GDTA Goal Tree supports users in adapting their learning paths to enhance their expertise in Offensive Cybersecurity. The *Overall Operator Goal* is broken down into two primary *Major-Goals* as shown in the picture below. Each Major-Goal is further divided into *Sub-Goals* that are essential for achieving the Major-Goals.

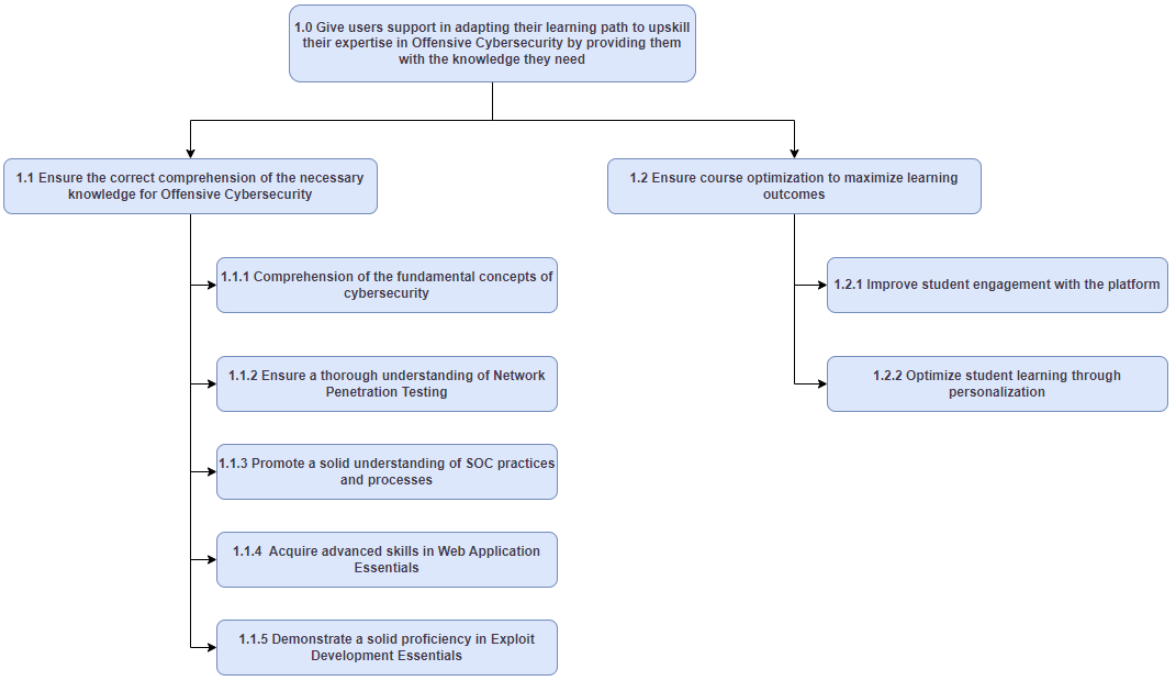


Figure 4.2: Final GDTA Goal Tree

The following sections will delve into the details of each sub-goal, providing a comprehensive understanding of the cognitive processes involved in achieving these objectives, rather than focusing on the methods or actions needed. Achieving these goals necessitates more complex cognitive processes than simply searching for a single piece of information.

Subsequently, we defined the *Informational Requirements* for each goal, which are crucial for users to make informed decisions and achieve their objectives. While these requirements might be mistakenly viewed as lower-level goals within the hierarchy, they actually serve as supportive elements that facilitate the achievement of primary goals.

In order to fulfill a goal, a decision must be made based on the available information. We are not interested in trivial yes-or-no questions: instead, we are focusing on decisions that enable the fulfillment of high-level goals. Moreover, these decisions require complex cognitive processes and a deep understanding of the situation.

## 4.3 Major-Goal 1.1: Ensure the correct comprehension of the necessary knowledge for Offensive Cybersecurity

This Major-Goal ensures that users build a solid foundation and understanding of essential cybersecurity concepts and practices. It is divided into five sub-goals.

### 4.3.1 Sub-Goal 1.1.1: Comprehension of the fundamental concepts of cybersecurity

Users need to grasp the basic principles of cybersecurity, including understanding types of threats, attack vectors, defense mechanisms, and the importance of cybersecurity in protecting information and infrastructure. The decision associated with subgoal 1.1.1 and its SA requirements are shown in the following figures.

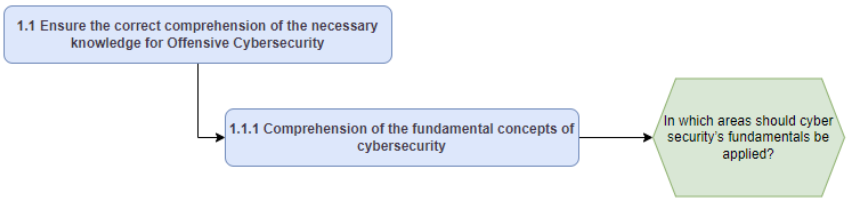


Figure 4.3: SA Requirements for Sub-Goal 1.1.1

| **Level 1 SA requirements** | **Level 2 SA requirements** | **Level 3 SA requirements** |
|---|---|---|
| OTP | Confidentiality | Capability to critically evaluate emerging technologies in relation to IT security, current laws and regulations |
| SHA256 | Integrity | |
| MAC | Confidentiality | |
| Digital Signature | Availability | |
| Blockchain | Threat Models | |
| TLS Protocol | Algorithms for Cybersecurity | |

Table 4.1: SA requirements for subgoal 1.1.1

### 4.3.2 Sub-Goal 1.1.2: Ensure a thorough understanding of Network Penetration Testing

This involves training users to conduct network penetration tests, which include identifying vulnerabilities within a network, exploiting those vulnerabilities, and providing recommendations to mitigate risks. Users learn about various tools and techniques used in network penetration testing. The decision associated with subgoal 1.1.2 and its SA requirements are shown in the following figures.

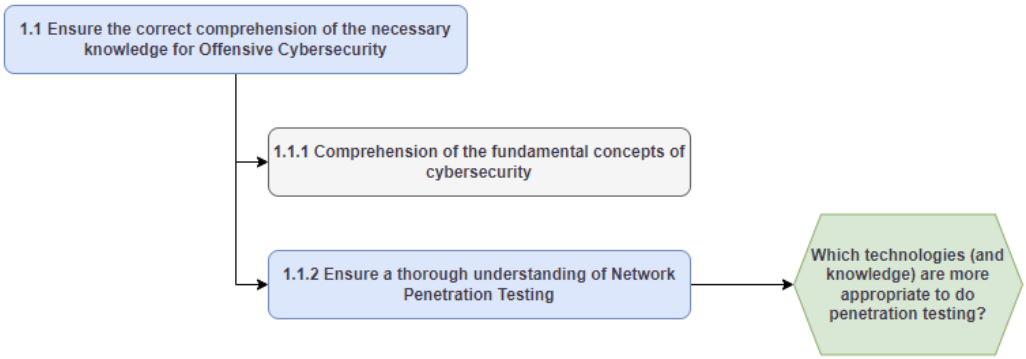


Figure 4.4: SA Requirements for Sub-Goal 1.1.2

| **Level 1 SA requirements** | **Level 2 SA requirements** | **Level 3 SA requirements** |
|---|---|---|
| Python operators | Cryptography techniques and hashing | Capability to choose the best penetration testing strategies based on the situation |
| Python syntax | Windows networking knowledge | |
| Powershell Scripting | Usage of variables | |
| Internet Protocol | Loops and functions in Python and Powershell | |
| Domain Name System | | |

Table 4.2: SA requirements for subgoal 1.1.2

# Chapter 5

# Dashboard

# Chapter 6

# Conclusions

# Contents

# List of Figures

# List of Tables