

**TOBB ETU**

**Economy & Technology University**

**BIL 495 / YAP 495**

**Project Management Plan (PMP)**

**Reference:** IEEE 1058 / ISO/IEC 12207

**Project Name:** PAPILLON - AI-Driven Cybersecurity Framework for Intelligent Threat Detection and Analysis **Version:** 1.0 **Date:** October 31, 2025

**Team Members:**

* Kerem ELMA
* Mete Cem TURAN
* Sabri Mert PİŞKİN
* Mehmet ESKİ

### **1. Project Overview**

**1.1. Project Definition** This project is being developed by the PAPILLON team for the BİL495 Graduation Project. The primary goal is to develop an integrated, AI-powered Cyber Threat Intelligence (CTI) platform that automates various elements of cyber defense, including malware classification, phishing detection, and intrusion detection. The platform aims to enhance the situational awareness and decision-making capabilities of Security Operations Centers (SOCs).

**1.2. Project Objectives**

* To develop an AI-driven CTI platform integrating multiple cybersecurity components.
* To implement a centralized threat intelligence and honeypot system to collect and analyze real-time attack data.
* To create a SOC assistant to summarize and visualize security alerts.
* To evaluate the system's effectiveness against benchmark datasets using metrics such as accuracy and detection rate.

**1.3. Scope Management (In/Out)**

* **In Scope:**
  + AI Models: Building models for malware detection, phishing detection, intrusion detection, and password strength estimation.
  + Data Processing: Gathering and preprocessing cybersecurity data such as network traffic logs, phishing emails, and CVE records.
  + Centralized Dashboard: Designing a dashboard to visualize, report, and monitor detected threats in real-time.
  + Simulation Environment: Creating a cyber-attack simulation lab to conduct controlled tests.
  + SOC Assistant: Developing an intelligent assistant to process alerts and facilitate decision-making.
* **Out of Scope:**
  + Developing automated remediation actions (e.g., blocking, deleting) for detected threats.
  + Deployment and performance testing of the tools in live, large-scale corporate networks.
  + Development of cybersecurity solutions requiring specialized hardware (e.g., FPGA).
  + Commercialization of the developed platform.

### **2. Organization and Roles**

**2.1. Team Roles and Responsibilities**

* **Mete Cem TURAN:**Genel mimari kararları, modül entegrasyonu
* **Kerem ELMA:** Proje Yöneticisi/Scrum Master: (Sprint takibi, plan güncellemeleri, toplantı yönetimi)
* **Sabri Mert PİŞKİN:** API geliştirme, veritabanı yönetimi, CTI entegrasyonu.
* **Mehmet ESKİ:** Test planı uygulama, metrik takibi.
* **Team (Joint Responsibility):** Core analysis and design tasks, Sprint review meetings.

**2.2. Communication Plan**

* **Meetings:** Each sprint will begin with planning and end with a review. Weekly progress meetings will be held as required, and short issue check-ins will occur every 3–4 days throughout the sprint.
* **Documentation:** All project documents (Reports, diagrams, this plan, etc.) will be stored in the GitHub repository.
* **Task Tracking:** The current status of tasks and overall progress will be tracked via Google Sheets (Gantt Chart and Task Tracking).

### **3. Project Schedule**

**3.1. Timeline and Sprints** The project is managed through a schedule of two-week Sprints.

* **Sprint 1 (4 Ekim - 18 Ekim):** Proje konusunu araştırma ve Proje Teklif Dokümanını tamamlama. (Tamamlandı)
* **Sprint 2 (18 Ekim - 1 Kasım):** Proje kapsamını netleştirme ve temel gereksinim diyagramlarını (Use Case) oluşturma. (Devam Ediyor)
* **Sprint 3 (1 Kasım - 10 Kasım):** Karşılaştırmalı Teknoloji Analizi yapma ve Yüksek Seviye Sistem Tasarımını (HLD) çizme.
* **Sprint 4 (15 Kasım - 30 Kasım):** Detaylı sistem tasarımı, Test Planı ve başarı metriklerini belirleme.
* **Sprint 5 (1 Aralık - 12 Aralık):** Kalite Güvence Planını sonlandırma ve dönem sonu teslimatlarını (Rapor, Sunum) hazırlama.**Dec 12, 2025):** Quality Model, Final Checklists, and Delivery Preparation.

### **4. Budget and Resources**

**4.1. Tools and Technologies**

The tools and technologies to be used will be determined at the end of the comparisons to be made in Sprint 3, and the following are available for those currently in use:

* **Project Management:** Google Sheets (for Gantt Chart and Task Tracking), Google Documents (for Documentation), Google Meets, WhatsApp
* **Version Control:** GitHub
* **Datasets:** Publicly available datasets such as CICIDS2017, NSL-KDD, Enron Fraud Dataset, etc.

**4.2 Budget Planning**

Budget planning cannot be fully defined because a technology has not yet been determined and this is an academic project. However, budget planning will be conducted in cases where a potential domain purchase is necessary, taking into account the requirements written so far.

### **5. Risk Management**

The following are potential risks and their mitigation strategies:

**5.1. Technical Risks**

* **Risk:** Difficulty in finding high-quality and well-balanced datasets.
* **Mitigation Strategy:** Multiple public datasets will be used, and synthetic data will be generated in a controlled environment.
* **Risk:** Potential compatibility issues when integrating different modules.
* **Mitigation Strategy:** The project architecture will be designed to be modular from the start.

**5.2. Resource Risks**

* **Risk:** The limited timeframe of an academic semester.
* **Mitigation Strategy:** The project scope has been clearly defined, and time will be managed by dividing tasks into Sprints.

**5.3. Ethical and Legal Risks**

* **Risk:** Sensitivity of cybersecurity data.
* **Mitigation Strategy:** Only anonymized or publicly available datasets will be used. No unauthorized penetration activities will be conducted.

### 

### **6. Quality Assurance**

* **Economic/Financial:** The project is academic, so a full budget is not defined. A potential constraint is the need for a domain purchase, which will be planned for if necessary.
* **Environmental:** (No information available in the provided documents).
* **Socio-cultural:** The platform is designed for a specific user profile: a SOC analyst or IT professional who can understand and analyze the data presented. This defines the required level of usability and data presentation.
* **Manufacturability:** (This constraint is not applicable to this software project).
* **Health:** (No information available in the provided documents).
* **Legal:** The project carries legal constraints related to cybersecurity data. To mitigate this, no unauthorized penetration activities will be conducted. The attack simulation platform is restricted to the user's own domain.
* **Ethical:** Similar to legal constraints, the project will adhere to ethical standards by using only anonymized or publicly available datasets.
* **Temporal (Time):** The project is constrained by the "limited timeframe of an academic semester". This is managed by a clear scope definition and a strict, two-week Sprint schedule.
* **Technological:**
  + **Data:** A primary risk is the "difficulty in finding high-quality and well-balanced datasets". This will be mitigated by using multiple public datasets and generating synthetic data.
  + **Integration:** A risk of "compatibility issues when integrating different modules" exists. The mitigation strategy is to design a modular architecture from the start.
  + **Stack:** The backend framework is defined (Python Django) , but final tool selection will occur in Sprint 3.
* **Safety (Security):**
  + **Project Goal:** The project's core purpose is to enhance security for a SOC analyst.
  + **Platform Security:** The application itself will incorporate security measures, including 2FA (via email initially) , session time-to-live (TTL) limits , and hashed, non-reversible passwords in the database.
* **Sustainability:** (No information available in the provided documents).

### **7. Appendix**

*The following supplementary documents, diagrams, and trackers are used for project management and documentation and are stored in the team's shared repositories:*

* *Project Management Plan (PMP)*
* *Software Requirements Specification (IEEE\_SRS)*
* *Gantt Chart*
* *Task Tracking Sheet & TRELLO*
* *Use Case Diagram*
* *Context Diagram*
* *Activity Diagram*
* *Sprint Meeting Notes*

### **8. References**

#### ***Standards***

* *IEEE 1058 (Standard for Software Project Management Plans)*
* *ISO/IEC 12207 (Systems and software engineering — Software life cycle processes)*
* *ISO 9001 (Quality management principles)*

#### ***Datasets and Data Sources***

* *CICIDS2017*
* *NSL-KDD*
* *Enron Fraud Dataset*
* *ExploitDB (API for IP scanning)*
* *NVD (National Vulnerability Database) (for CVE parsing)*

#### ***Tools and Technologies***

* ***Project Management:***
  + *Google Sheets (for Gantt and Task Tracking)*
  + *Google Documents*
  + *Google Meets*
  + *WhatsApp*
* ***Version Control:***
  + *GitHub*
* ***Development:***
  + *Python Django*
  + *MySQL (proposed)*
  + *Python Scapy (proposed)*