UNITRENTO

Cyber Security Risk Qualitative Assessment Report

Remotely piloted fleet

A.Y. 2024/2025

Work submitted in partial fulfillment for the course of Cyber Security Risk Assessment - University of Trento - a.a. 2024/2025

This work is original work, has been done by the undersigned student and has not been copied or otherwise derived from the work of others not explicitly cited and quoted. The undersigned students are aware that plagiarism is an offence which may lead to failure of the course and more severe sanctions.

NAME	SURNAME	STUDENT-ID
Simone	Rossi	257777
Matteo	Bertoldo	256131

EXECUTIVE SUMMARY (max 150 words)

This document presents the results of a qualitative cybersecurity risk assessment of the Unmanned Traffic Management (UTM) system supporting remotely piloted drones. Using the SecRAM methodology [1], we highlighted the most common [2] and high-risk scenarios as follows: **Phishing** attacks, **Denial-of-Service** (DoS) and **SQL Injection**. These scenarios could severely undermine essential system components, including secure authentication, data integrity, service availability, and confidentiality, ultimately disrupting overall operations.

Given the present cybersecurity threat landscape [3], we advise implementing robust controls, specifically enhanced **personnel training**, proper **rate limiting**, **load balancing** measures, strong user **input validation** and **Web Application Firewall** (WAF).

These measures significantly reduce system exposure while maintaining operational continuity and integrity. Further recommendations and controls are detailed in the following report sections to ensure a comprehensive risk management approach.

We also identified additional minor vulnerabilities and included recommended controls in the attached spreadsheet.

1. TARGET OF EVALUATION (max ½- page)

The target of evaluation is the Unmanned Traffic Management (UTM) system, which covers the technological infrastructure managing a remotely piloted drone fleet. This includes the physical drones, their storage facilities such as warehouses, the control center responsible for flight monitoring, the Security Operation Center (SOC) overseeing security events, and the computing infrastructure comprising data centers that handle database management and computational tasks like path prediction algorithms.

During our assessment, the following assumptions were made:

- Only authorized personnel with proper credentials have access to the control center, SOC, and related systems.
- User roles are strictly enforced, with differentiated privileges to limit access to sensitive functions (e.g., drone operation, data management, security monitoring).
- The drones communicate with the control center over encrypted channels.
- The data centers hosting critical services are located in secure environments with backup power and network redundancy.
- External access to management interfaces is limited and protected by VPN and multi-factor authentication.
- Physical security measures are in place at warehouses and data centers, reducing the likelihood of physical tampering.
- Due to the criticality of drone operation, availability is prioritized, but some secondary services may tolerate limited downtime.
- Natural disasters affecting the infrastructure are assumed to be rare given geographic location and contingency plans.
- Risk Evaluation levels range from Very low to Very High (range of 5 possible values).

2. SUMMARY OF FINDINGS (max ½ page)

The cybersecurity risk assessment of the system identified several security concerns, with the most common being [2] phishing attacks, DoS attacks, and SQL Injection. These threats predominantly target critical assets including personnel, company data centers and databases, all vital for ensuring operational continuity and maintaining data integrity. To address these risks, the following mitigation strategy is proposed:

- **Security Awareness and Training**: Implement continuous training programs to enhance employee awareness and reduce susceptibility to phishing attacks.
- **Robust DoS Attack Mitigation**: Deploy a combination of rate limiting, load balancing, and network segmentation to effectively limit the impact of DoS attacks.
- **Strong Data Protection Measures**: Enforcement of regular automated backups to ensure data recovery in the event of an incident. Additionally, enforce strong validation of user input data, and implementation of WAF.

In addition, the use of **Multi-Factor Authentication** (MFA) is strongly recommended against phishing attacks, unauthorized access and session hijacking attempts.

This combination of controls is expected to lower the overall risk level from Very High to Low/Medium, thereby safeguarding the operational integrity of the UTM system and enhancing its resilience against the most critical threats. This balanced approach integrates technical safeguards with user-focused practices to effectively mitigate both technical and human vulnerabilities.

3. RISK ANALYSIS (1 page)

The complete summary of the risk assessment results can be found in the document SecRAM.xlsx, submitted as an integral part of this report.

Step 1: We identified the primary assets and assessed their impact on the overall system (see Tables 1.1 and 1.2 in the document). Among these, the most critical assets include:

- **Internet Connectivity:** Provides essential connectivity for users and system operations, crucial for maintaining service availability.
- **System Monitoring and Auditing:** Ensures continuous oversight of system health and security, enabling prompt detection of anomalies and compliance verification.
- **Power Infrastructure:** Supports the uninterrupted operation of all system components, directly affecting reliability and availability.
- **UTM System:** Manages the coordination and safe operation of unmanned aerial vehicles (drones) within the airspace, essential for operational safety.

These primary assets are fundamental to business continuity, operational stability, and the organization's reputation.

Step 2: We then identified the supporting assets that enable and protect these primary assets (see Table 1.3). Key supporting assets include:

- **Personnel:** The human resources responsible for operating, maintaining, and securing the system.
- **Drone:** The physical air vehicle asset that supports core services.
- **Network Infrastructure:** The backbone that connects all components, ensuring reliable and secure communication across the system.
- **Services APIs:** Interfaces that enable interaction between different system modules and external services, essential for functionality.

Step 3: We analyzed threats and vulnerabilities related to the supporting assets identified in Step 2 (see Tables 2.1 and 2.2). For example, authentication services are vulnerable to credential theft and phishing attacks due to weak password policies. Similarly, user interfaces are exposed to injection attacks because of insufficient input validation. Network components face threats such as denial of service (DoS) attacks and interception of sensitive data. Some key threats and associated vulnerabilities include:

Threat	**Vulnerability**
Zero-day exploit	Lack of monitoring and intrusion detection systems
Ransomware attack	No frequent backups / no segmentation

Step 4: We evaluated the impact and risk levels of the threats identified in Step 3 (see Tables 3.1 and 3.2). The highest priority risks to mitigate include:

Supporting Assets	**Threat**	**Impact**	**Likelihood**	**Risk Level**
Firewall	Zero-day exploit	5	4	Very High
Company datacenter	Ransomware attack	5	4	Very High

Step 5: To mitigate the identified risks, we proposed targeted security controls (see Table 4) to lower the residual risk, allowing us to not exceed the 'Medium' threshold. These include the following examples:

Threat	Pre-control	Post-control	Residual Impact	Residual Likelihood	Residual Risk Level
Zero-day	Intrusion Detection Systems, honeypot	Emergency patching, configuration hardening	4	1	Low
Ransomware	Automated patching, frequent backups, network segmentation	Emergency patching, isolation	3	3	Medium

ANNEX
An integral part of the report we attach the following documents:

1. Excel document reporting the application of SESAR SecRAM method (see file SecRAM.xlsx).

REFERENCES

1. SecRAM 2.0: Security Risk Assessment methodology for SESAR 2020
2. Cisco: What Are the Most Common Cyber Attacks?
3. Amazon: Revising the Airspace Model for the Safe Integration of Small Unmanned Aircraft
4. Kardach, Monika & Fuc, Pawel & Galant, Marta & Maciejewska, Marta. (2019). Risk Assessment of Remotely Piloted Aircraft Systems. Journal of KONBiN. 49. 10.2478/jok-2019-0005
5. Fiondella et al. (2019) – Drone Cyber Security: Assurance Methods and Standards