

# Cyber Threat Assessment Report

This document comprises a report crafted following an assessment of threats encountered within the organizational network. The required details should be populated based on information gathered from the current evaluation. If necessary, this template can be updated and modified.

**Note:** Prior to building a threat assessment report, Section 1 and Section 2 must be filled with all required details.

## Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
Additional Contact Information:	

## Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

## Section 3: Test Details

Test Start Date	
Test End Date	
Duration of Test	
Network Analyzed	
Functions Enabled	

## Executive Summary

Security and Threat Prevention		
Number of Attacks Detected	Malicious Applications Detected	
User Productivity		
Top Application Category	Top Web Category	Top Website
Network Utilization		
Top Host by Bandwidth		
Host with Highest Session Count:		

## Commonly Targeted Assets

Targeted Assets				
Serial #	Asset Name	ID	Category	Location

## Correlating Threats

Threat Correlation	
Technique Used:	
Results Obtained:	

## Recommendations

Threat Type	Threat Description	Threat Likelihood	Impact Rating	Risk Exposure Rating	Recommendation
T1					
T2					
T3					
T4					
T5					

Actions Taken		
Performed By	Date	Action Taken

## Conclusion

*[Conclusion of the assessment process.]*

A large, empty gray rectangular box with a thin black border, intended for the user to write the conclusion of the assessment process.

---

**Incident Handler's Signature**

---

**Date**