# Setting up a Threat Hunting and Intelligence Ecosystem for Banking Organizations

## PREAMBLE

To ensure a safe and secure ecosystem that comply with industry standards while preventing emerging security threats, Banks have to follow specific rules and regulations set by regulators and auditors when deploying their security solutions. According to a report published in security magazine, it was stated that the banking industry experienced a 1,318% increase in ransomware attacks in 2021. As an example, on the morning of Wednesday, March 23, 2022, the Tunisian Central Bank detected a cyber-attack on his security system and experienced some disturbances on its activities, including the website. In this context, Innovation Technology Consulting (ITC), as a cyber-security firm, is seeking to set up a next generation security operation center (SOC) with threat hunting and intelligence capabilities for the banking sector. The solution to be deployed should embrace a unified management dashboard that facilitates and centralizes the management and monitoring of the bank's IT infrastructure.

## PROJECT OVERVIEW:

The main purpose of this project is to implement a Proof of Concept (PoC) of a Threat Hunting and Intelligence ecosystem while considering the requirements expressed in the current project specification sheet. In particular, the goal of this project is to design a functional and technical architecture, benchmark open-source solutions, install and test the solutions chosen to integrate them in the same environment, and verify their operational readiness.

The following features must be considered in the deployed solution:

- **Data Integration:**
    - Ensure the platform can integrate with diverse data sources such as logs, network traffic, endpoints, and cloud services.
    - Support for standard data formats like Syslog, JSON, and various log types to accommodate different data streams in a banking environment.
    - Implement cryptographic methods to ensure data confidentiality and authenticity. The platform should support data encryption for sensitive information

at rest and in transit and use digital signatures to verify the integrity of logs and alerts.

- **Data Correlation and Enrichment:**
  - Ability to correlate and enrich data from different sources to provide a more comprehensive view of potential threats.
  - Customize SIEM rules to align with banking-specific threat scenarios.
  - Integration with threat intelligence feeds to enrich data with known indicators of compromise (IoCs).
- **Advanced Analytics and Machine Learning:**
  - Incorporation of advanced analytics, machine learning, and behavioral analysis to identify anomalous patterns and potential threats.
  - Support for custom algorithms and models to adapt to specific organizational needs.
- **User and Entity Behavior Analytics (UEBA):**
  - Capability to analyze and baseline normal behavior of users and entities within the network to detect deviations that may indicate a threat.
  - Behavioral profiling to identify suspicious activities based on user interactions with systems.
- **Real-time and Historical Analysis:**
  - Support for real-time analysis to detect and respond to active threats.
  - Ability to conduct historical analysis for retrospective threat hunting, enabling the identification of past incidents.
- **Automated Playbooks and Workflows:**
  - Develop and document threat hunting playbooks tailored to banking environments.
  - Automation of repetitive tasks through playbooks and workflows to streamline the threat hunting process.
  - Integration with orchestration and automation tools to execute response actions.

- **Scalability and Performance:**
  - Scalability to handle large volumes of data and diverse data sources.
  - Efficient performance, especially during peak times, to avoid delays in threat detection and response.
- **Threat Hunting Collaboration:**
  - Collaboration features that allow security teams to share insights, findings, and collaborate on investigations.
  - Integration with communication tools and platforms to facilitate collaboration among security analysts.
  - Ability to consume and act upon IoCs from various sources.
- **Alerting and Notification:**
  - Customizable alerting mechanisms to notify security teams of potential threats.
  - Integration with popular communication channels for immediate notification, such as email, messaging apps, collaboration solutions and SIEM solutions.
- **Compliance and Reporting:**
  - Features to support compliance requirements and generate reports for audits.
  - Customizable reporting templates to address specific compliance standards and regulations such as ISO2700x, GDPR, SWIFT, SOX, GLBA, Basel III, and PCI DSS.
- **Integration with Existing Security Infrastructure:**
  - Compatibility and integration with existing security tools, such as SIEM, endpoint protection, and firewalls.
  - Ensuring seamless communication and data sharing between different security tools in the environment.
- **AI-Driven Threat Intelligence:**
  - Regularly update and enhance threat intelligence feeds using AI to stay current with emerging indicators of compromise.
  - Integrate with reputable external threat intelligence sources and sharing platforms to expand threat coverage and improve response.
  - Implement AI-driven threat detection mechanisms capable of correlating and analyzing data from multiple sources.

- Conduct post-incident reviews to identify improvement areas, using AI insights to adapt and refine security strategies as new threats emerge.
- Design dashboards that visualize threat trends, indicators of compromise (IoCs), and vulnerability impact to aid IA teams in understanding the scope and urgency of threats.

- **Incident Simulation and Training:**
  - Tools for simulating incidents and conducting training exercises to ensure readiness and skill development among the threat intel platform.
  - Conducting pilot testing before full deployment to identify and address any potential issues or challenges.
- **Audit Mission Emulation:**
  - Conduct mission emulations to assess system resilience and response capabilities.
  - Perform automated audits and penetration tests to identify vulnerabilities and ensure compliance.
  - Comprehensive Reporting: Generate PDF reports with both summarized and detailed findings for clear security insights.

## PROJECT OBJECTIVES

You have received this project specification sheet and are asked to technically examine the overall physical and virtualized systems, encompassing both functional and security aspects. The objectives are to:

- ✓ Provide a comprehensive perspective to grasp the business context of the proposed solution. Identify critical assets, potential threats, vulnerabilities, and delineate the repercussions of a security incident.
- ✓ Design and provide a layered architecture that modularizes the proposed Infrastructure and the SOC components.
- ✓ Deploy, configure, and integrate appropriate security solutions for both physical and virtual infrastructures.
- ✓ Create a Threat hunting platform with the capability to integrate external threat feeds.

- ✓ Test the effectiveness and efficiency of the deployed solution.
- ✓ Provide a comprehensive review of the organization's adherence to regulatory compliance.

## DELIVERABLES

You are invited in addition to the PoC to furnish the following documents:

1. A presentation of a general approach for carrying out the project. This approach contains:
    a. Scope of the project
    b. Required Resources (human and material resources)
    c. Constraints and Assumptions
    d. Cost Analysis and Pricing Relationship
    e. Work Breakdown Structure
2. A technical study that contains the presentation of technical and organizational solutions that can be adopted. This study should contain a detailed architecture with all the products and solutions that will be installed.
3. A Work schedule that contains:
    a. Activity definition
    b. Activity sequencing
    c. Activity duration estimation
4. Audit Report: A thorough audit report documenting the project's compliance, findings, and recommendations based on the audit process. This report should highlight security gaps, risks, and suggested improvements.

### Additional information

1. All documents and communications related to this project must be in English.
2. Tutors have the right to add additional services and change technical choices.
3. A dedicated Slack channel must be created for each team to facilitate regular updates, discussions, and document sharing.