**NAME: AGBEJA AYOOLUWA OREOLUWA**

**MATRIC NO: 15/MHS01/012**

**COE 510 COMPUTER SYSTEM TECHNIQUES ASSIGNMENT**

**QUESTION ONE**

The security policy to be developed will be as follows:

* Prior to initial use all devices must be registered with the company. A list of approved mobile devices and related software applications and utilities needed. Devices that are not on the list may not be connected to the company’s infrastructure; this approved list could be later updated in the future.
* At least every two years, the company should hire a good security company that will conduct tests on every device: a general sweep to fortify the security of the company’s overall network and reduce the rates of possible attacks.
* Implement strong authentication over password control. Users should be instructed to enable use of password to access their mobile devices. Also the company would enable the device to swipe clean temporarily should a number of failed password attempts occur.
* The mobile phones issued would have policies established such that the use of a third party software will be blocked. This way possible compromise and security breaches could easily be prevented.
* All mobile devices should be encrypted as wireless communications are easy to intercept. The use of VPNs should also be recommended for any communication between a mobile device and a company or cloud- based system or service. As VPNs also include strong encryption and provide opportunities for logging, management and strong authentication of users.
* Antimalware software should be updated for all operating systems to prevent being vulnerable or being a possible target for threats.
* Specific sites should be blocked as well as applications whose installation could be possibly dangerous.
* In the event an employee’s device is lost or stolen, its essential to have the authority wipe out the apps and information related to the business form the device. Although this may become tricky as his may include the employee’s personal data.
* Data on these devices should be encrypted. This throws an extra barrier in the event a device is stolen and/or hacked. This helps protect sensitive company and client information.

**QUESTION TWO**

After gaining employment hopefully, I will carry out the following

* Social engineering- I will engage in social conversations from older staff and us this try to obtain confidential information of the company; the people of interest that will be targeted will be the staff in the department whose job in nature is the most confidential. I will hopefully identify a weak link.
* Still using this social engineering skills on these targets, maybe developing an acquaintanceship will hopefully be able to go to his or her office rooms and infect his or her system.
* After the Trojan infection I will hopefully able to remotely control and steal information from the user’s computer.
* Gainfully accessing this confidential system I will be able to achieve the following agenda:
* Stealing client’s information- obtaining client’s information could be disclosed and used to cause harm to the company’s reputation.
* Trade secrets- it generally means protected information about existing products or products in development. This information may help your rivals make their products more competitive or even bring a similar product to the market faster than you can.
* Financial information- Financial information about your company can be used to offer better deals to your clients and partners, win bids, and even make better offers to your valuable employees.
* Marketing information- This will allow your competitors to prepare a timely answer for your marketing campaigns, which, in turn, may render them ineffective.

WAYS TO PREVENT

Ekran System – A monitoring solution for preventing industrial espionage. Ekran System is a universal employee activity monitoring solution specifically designed to combat insider threats, including industrial espionage.

It can monitor the actions of every user regardless of their level of privilege, allowing you to control the actions of system administrators and users with access to trade secrets and financial information. Particularly, Ekran System provides you with the following features for detecting and preventing industrial espionage:

* Manage access and audit user activity

The [PASM](https://www.ekransystem.com/en/product/privileged-access-management) solution in Ekran System helps you implement the [principle of least privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege.). It provides access management for privileged and general user accounts. You can specify endpoints that particular users can access, limit the time of their sessions, and provide temporary and permanent credentials.

* Monitor and investigate

[Screen video recording](https://www.ekransystem.com/en/product/user-activity-monitoring). You can watch all kinds of account sessions in a convenient YouTube-like player and filter them by username and IP. Videos are indexed with layers of text metadata, including visited URLs, typed keystrokes, and names of opened apps.

Ekran can record input and output audio streams on user endpoints. Recorded audio can be exported for further analysis.

Key episode search. Advanced session analysis allows investigators to search episodes by various parameters within the current session and across all recorded sessions.

* Respond to threats in real time

User and entity behavior analytics (UEBA) is an artificial intelligence-powered module that analyzes user activity to detect unusual behavior. The UEBA module will help you prevent data breaches long before they happen.

* [Actionable alert system](https://www.ekransystem.com/en/product/alerts-and-notifications). In addition to an impressive collection of alert templates, you can set custom alert rules based on any suspicious events like opened URLs, process names, or connected USB devices. When the system identifies a suspicious event, your security team receives a notification so they can act immediately.
* Automated incident response. An automated response guards your data even before the security team reacts. You can assign a risk level and choose between blocking a user, terminating an application (or process), blocking a connected USB device, displaying warning messages, and other options.

**QUESTION THREE**

1. 3 HAMLETS – M

1 ORACLE – O

9 MESSANGERS – R

1 SHELL – S

4 RODENTS – E

1 CALABASH –C

3 PROPHECIES- O

1 DESTINY – D

6 COWRIES – E

The result is MORSE CODE

1. SING THAT TRAP FALL

THINGS FALL APART

**NUMBER FOUR**

Encrypted message TSJSFRHGTJQTNZS

1. Caesar substitution cipher (key 5)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the English alphabets above Caesar shift of 5 gives:

VWXYZABCDEFGHIJKLMNOPQRSTU

Decrypted Caesar cipher – ONENAMCBOELOIUN

1. Columnar transposition cipher (key 5)

Using Key – abcde

a b c d e

1 2 3 4 5

o n c e i

n a b l u

e m o o n

Plain text – ONCE IN A BLUE MOON