Muhammad Izham Bin Norhamadi

B032020039

No.:

Date:

Question 1

a. 1) Log events on the system

2) Managing User authorization to assets

~~retention and translation of security protocol data into relevant risk management information~~

b. 1) Align business and IT strategies

2) Increase business and IT agility

3) Establish and refine future architecture vision

4) Govern technology decisions and direction

5) To protect an organization's IT operations and assets against internal and external threats

c. 1) EEM - Eterprise Event Management

Provides registration to the event in a private access and authentication through a gateway

2) SIM - Security Information Management

Facilitating the collection, retention and translation of security protocol data into relevant risk management information

3) SEM - Security Event Management

Real time monitoring and event management to support IT security operations

4) SIEM - Security Info Event Management

A set of tools that combine SIM and SEM

Muhammad Izham Bin Norhamadi
B03202-0039

No.: Date:

d. 1) Smartphone as user authentication - members of an organization may required to install an app to authenticate before being allowed to use organization's assets.

2) Employee badge - An RFID station will detect and scan for the chip on employee's badge before permitting entry through electronic door.

e. 1) Solarwinds Kiwi Syslog Server receives syslog messages and SNMP traps from network devices and Linux hosts.

2) PRTG capture and monitor syslog messages using centralized Syslog Receiver Sensor

3) Logstash opens a TCP port and listen for incoming connections, looking for syslog data

Question 2

a. 1) Syslog content
2) Syslog application
3) Syslog transport

b. 1) Without a standard format syslog can be hard to make use of

2) Syslog employs User Data Protocol (UDP) to transport information, this means log messages could be lost if there is a network congestion.

3) Syslog does not include any authentication processes to prevent a machine from impersonating another.

4) Classic syslog traditionally is not useful to handle early boot or late shutdown system logging.

2

Muhammad Izham Bin Norhamadi
B032020039

No.:   Date:

c. Syslog (system logging protocol) is a standard protocol used to send log or event message to a syslog server to collect various device logs from different machines for monitoring and review. Syslog is helpful in various ways such as identifying critical network issues and reduce downtime of servers and other devices in your infrastructure.

d. 1) Define scope and boundaries of ISMS
2) Identify security risks by identifying the asset involved and threats to those assets.

e. The flow of the logs are more predictable and controlled, This help to ensure the most time-sencitive security data is relied and processed.

Question 3

a. 1) SIMATIC WinCC is a SCADA and Human-Machine Interface (HMI) system from Siemens.
2) ABB Ability Network Manager SCADA is a real-time platform to securely and efficiently manage all remotely controlled operations accross energy genration, transmission and distribution systems
3) Experion SCADA is an intuitive and scalable solution, is the heart of Honeywell's SCADA system.

b) MTU initiates communication with remote units and interfaces with the DAS and the HMI while RTU is a small computer that will write its data to memory and send it to the controller

Muhammad Izham Bin Norhamadi
B032020039

No.: .... Date: ....

c. We can use software attestation to :
1- Check the integrity of program memory
2- Detect modification through malicious code
3- Gain insight of our sensor behavior
4- Observe presence of any malicious code in the system

d. 1) Communicate between PLCs, valves and switches
2) Ideal protocol for RTU applications where wireless communication is required.

Question 4

a. 1) Prevents computer attempt to brute force authentication
2) Minimize and limit hacker's dictionary attack
3) Prevents bots from spamming submissions.
4) Deters bots from accessing while allowing humans to access

b. One of the methods is to generate a password using OTP along with a secret key that has already been shared with the user, which comes with an application installed on the user's mobile device and does not require any internet support

c. 1) Physical obstruction such as walls, doors and gates
2) Sensors and monitoring tools such as CCTV and face detection to monitor all entry to building
3) Security Surveillance such as guards and guard dogs to secure the perimiter around building
4) Automatic authentication such as electric doors using smart card

Muhammad Izham Bin Norhamadi
B032020039

Date:

No.:

d. 1) The employee credentials may be compromised and another user is using it for unauthorized access.
2) The employee may have left a workstation without properly logging out of session

e. By analysing logs generated by network devices and systems we can determine and monitor cyber attacks that have occurred as we have an insight into the inner workings of the system and its behavior.

5