CC in a Nutshell

Security Operations

By BELKHIR Selma

Data Security and Handling

-DATA HANDLING PROCESS: CREATE, STORE, SHARE, USE, MODIFY, ARCHIVE, DESTROY.

- DATA CLASSIFICATION: HIGHLY RESTRICTED, MODERATELY RESTRICTED, LOW SENSITIVITY, UNRESTRICTED PUBLIC DATA.

Data Security and Handling

-ENCRYPTION: SYMMETRIC (SAME KEY) AND ASYMMETRIC (DIFFERENT KEYS).

- HASHING: CONVERTS DATA INTO A FIXED-LENGTH VALUE; USEFUL FOR VERIFYING INTEGRITY.

System Hardening

OBJECTIVE: REDUCING THE ATTACK SURFACE BY APPLYING SECURE CONFIGURATIONS TO HARDWARE, COMMUNICATION SYSTEMS, AND SOFTWARE.

CONFIGURATION MANAGEMENT:

STEPS: IDENTIFICATION, BASELINE, CHANGE CONTROL, VERIFICATION & AUDIT.

ELEMENTS: INVENTORY, BASELINES, UPDATES, PATCHES

Best Practice Security Policies

TYPES OF POLICIES: DATA HANDLING, PASSWORD, ACCEPTABLE USE, BRING YOUR OWN DEVICE (BYOD), PRIVACY, CHANGE MANAGEMENT

**PASSWORD POLICY:** CREATION, AGING, AND PROTECTION GUIDELINES TO ENSURE STRONG PASSWORD USAGE.

BYOD POLICY: APPROPRIATE USE OF PERSONAL DEVICES (E.G., CELL PHONES, TABLETS, LAPTOPS).

Change Management

ACTIVITIES: DECIDING TO CHANGE, MAKING THE CHANGE, AND CONFIRMING IT WAS CORRECTLY IMPLEMENTED.

STEPS: REQUEST FOR CHANGE (RFC), APPROVAL, ROLLBACK.

Security Awareness Training
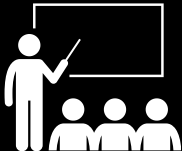
TRAINING TYPES: EDUCATION, TRAINING, AND AWARENESS.

SOCIAL ENGINEERING TECHNIQUES: BAITING, PHISHING, PRETEXTING, TAILGATING.