BACK TO SCHOOL

WITH

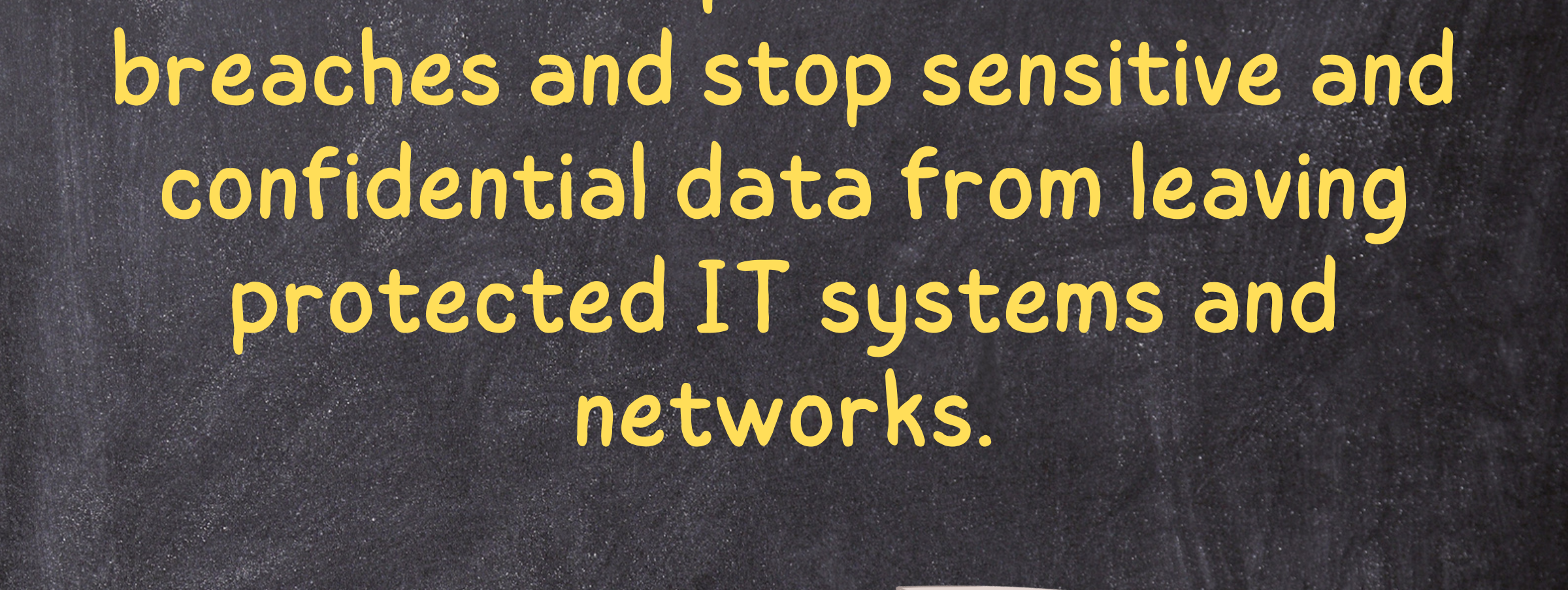
DATA LOSS PREVENTION

MINISTRY OF SECURITY

MINISTRY OF SECURITY

WHAT IS DLP?

Set of tools and processes used to detect potential data breaches and stop sensitive and confidential data from leaving protected IT systems and networks.



MINISTRY OF SECURITY

WHY DLP?

F-

INSIDER THREATS

An insider threat refers to the risk posed by individuals within an orgaization who may intentionally or unintentionally expose sensitive or confidential data to unauthorised entities.

Insider threats can be prevented through stringent data access controls, monitoring user activity, limiting privileges, and promptly revoking access when policy violations occur.

MINISTRY OF SECURITY

F- EXFILTRATION

Data exfiltration refers to the unauthorized transfer of sensitive information from a target's computer network or system to an external location or unauthorized party.

Data exfiltration can be prevented by monitoring outbound network traffic for sensitive data transmission, blocking restricted uploads or transfers, and alerting security teams about policy violations.

MINISTRY OF SECURITY

NEGLIGENCE

Negligence refers to when an individual fails to exercise reasonable care in safeguarding sensitive data, following security protocols, or adhering to policies for appropriate use of computer systems - potentially enabling data breaches.

Negligence can be prevented through comprehensive user training on handling policies, increased monitoring of user activity with data, and enabling features like confirming file transfers to encourage mindfulness before data operations.

MINISTRY OF SECURITY

WHAT NEEDS TO BE PROTECTED?

MINISTRY OF SECURITY

SECURING DATA IN MOTION

Ensuring the safe transmission of sensitive, confidential, or proprietary data while it moves across the network through encryption and/or other email and messaging security measures

MINISTRY OF SECURITY

SECURING DATA IN USE

Securing data being used by an application or endpoint through user authentication and access control

MINISTRY OF SECURITY

SECURING DATA AT REST

Protecting data that is being stored at any network location — including the cloud — through access restrictions and user authentication

MINISTRY OF SECURITY

DATA LEAK DETECTION

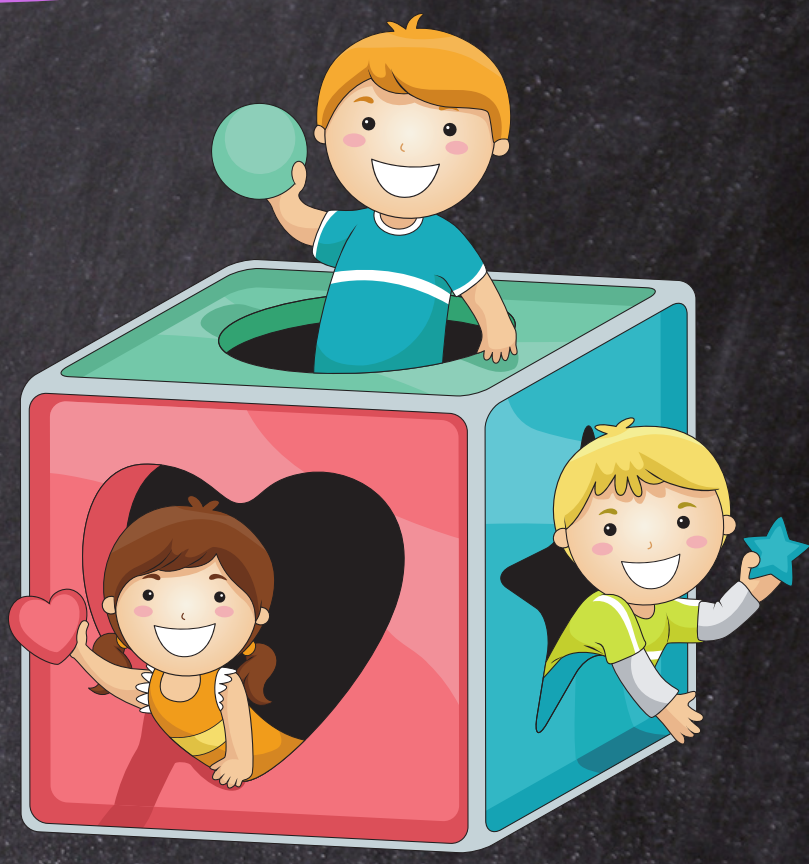
This technique involves setting a baseline of normal activity, then actively looking for unusual behavior.

MINISTRY OF SECURITY

TYPES OF DLP

NETWORK

Network DLP monitors network traffic to prevent confidential data from leaving the corporate infrastructure over email, web, messaging, or other internet access channels.



Analyze network flows by deeply inspecting packets

Identify sensitive data patterns within network traffic

Trigger real-time alerts when policy violations are observed for security analysis

Log extensive data for forensics reviews following a confirmed data breach

Provide dashboards and reporting to visualize network data flows and pinpoint risks

Enforce data loss prevention policies by blocking restricted data transfers

MINISTRY OF SECURITY

ENDPOINT

Endpoint DLP utilizes agent software on user devices to monitor locally stored, accessed or transferred data to prevent loss at the source via removable media or other means.

Install software agents on end-user devices to monitor device activity

Detect when users copy, share, or transfer files containing critical data

Block restricted data transfer attempts via cloud sync, external media like USB drives, web uploads

Alert administrators to potential policy violations regarding sensitive data handling

Provide advanced encryption, access controls and usage auditing capabilities

Track data movements from endpoints to email, printers, applications etc.

MINISTRY OF SECURITY

STORAGE

Storage or data-at-rest DLP scans structured and unstructured data in databases, file shares, and storage systems to discover sensitive data hotspots and apply access controls.

Discover regulated data like PII, PHI, and intellectual property distributed across unstructured data stores

Scan object and file meta-data to classify and label confidential data repositories

Map sensitive data locations and document data flows to quantify breach impact risks

Apply access controls, encryption policies and usage auditing to high-risk data

Enable forensics and speed up incident response when data breaches occur

Comply with privacy regulations requiring security controls on sensitive information-at-rest

MINISTRY OF SECURITY

CLOUD

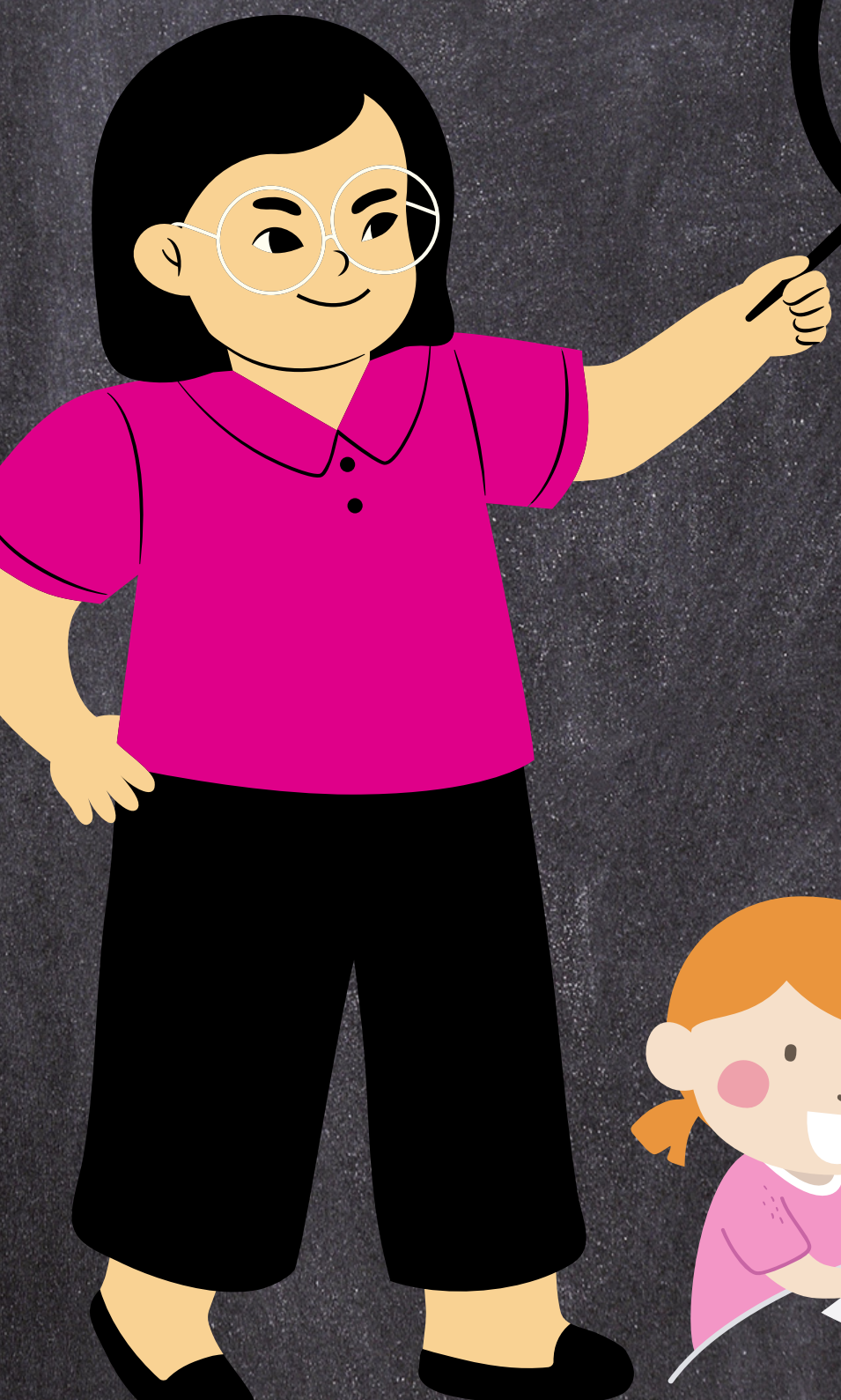
Cloud DLP secures sensitive data stored and processed in cloud apps by scanning for violations and preventing data exfiltration.

- Discover regulated data in cloud apps
- Continuously monitor access to confidential cloud data
- Enforce DLP policies spanning cloud and on-prem
- Unified compliance view across cloud and on-premises
- Facilitate compliance with privacy regulations
- Eliminate blind spots for consistent data protection

MINISTRY OF SECURITY

DLP IMPLEMENTATION

CONDUCT AN INVENTORY AND ASSESSMENT



MINISTRY OF SECURITY

CLASSIFY SENSITIVE DATA

MINISTRY OF SECURITY

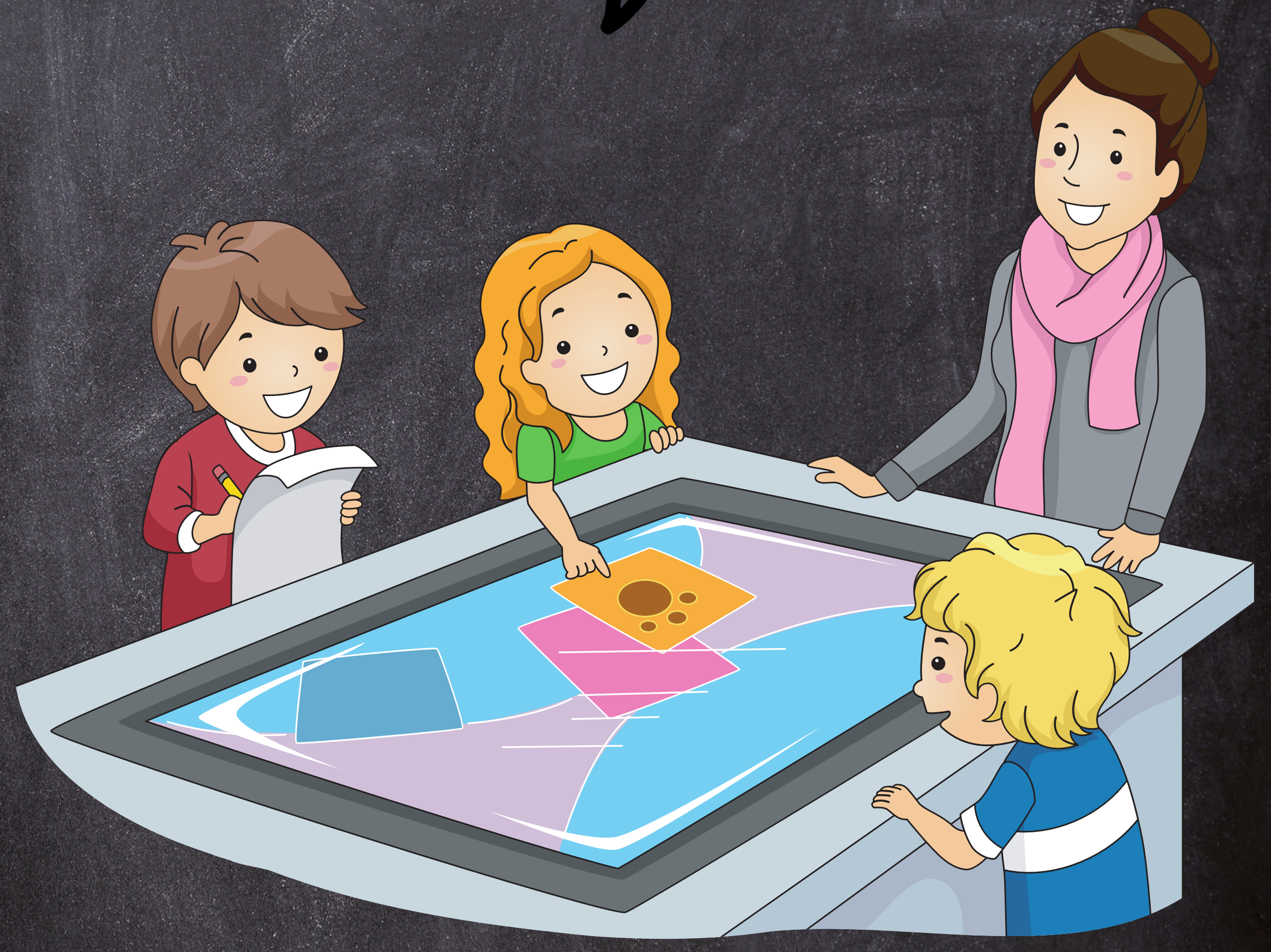
ESTABLISH DATA HANDLING AND REMEDIATION POLICIES

MINISTRY OF SECURITY

REDEFINE POLICIES BASED ON LEARNINGS

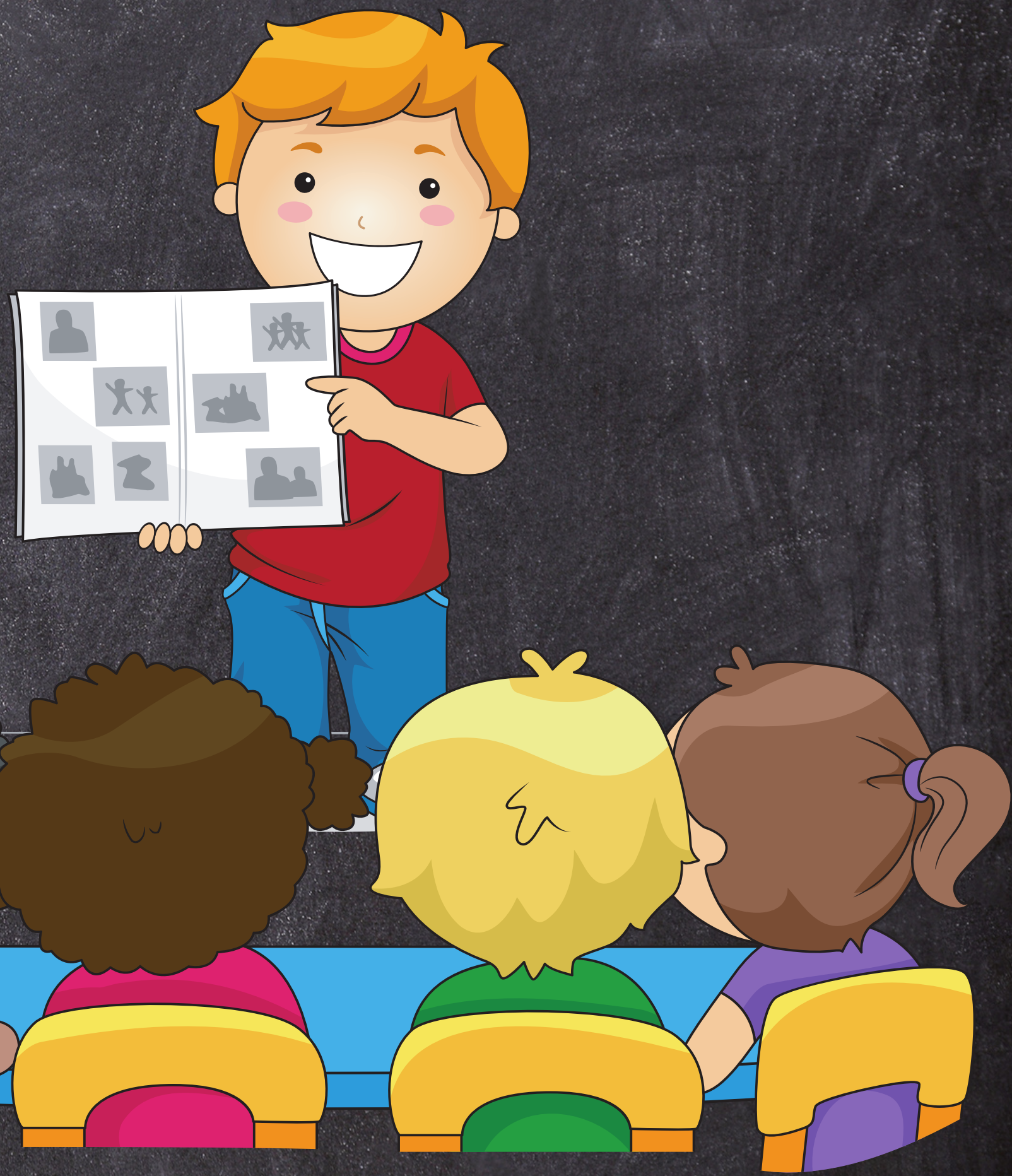
MINISTRY OF SECURITY

IMPLEMENT A SINGLE & CENTRALISED DLP PROGRAM



MINISTRY OF SECURITY

CONDUCT USER AWARENESS TRAINING



FOLLOW US FOR MORE FREE CHECKLISTS | PLAYBOOKS TEMPLATES | VIDEOS

PLAYBOOK MADE WITH ❤ BY

MINISTRY OF SECURITY

SECURITY & PRIVACY MADE EASY