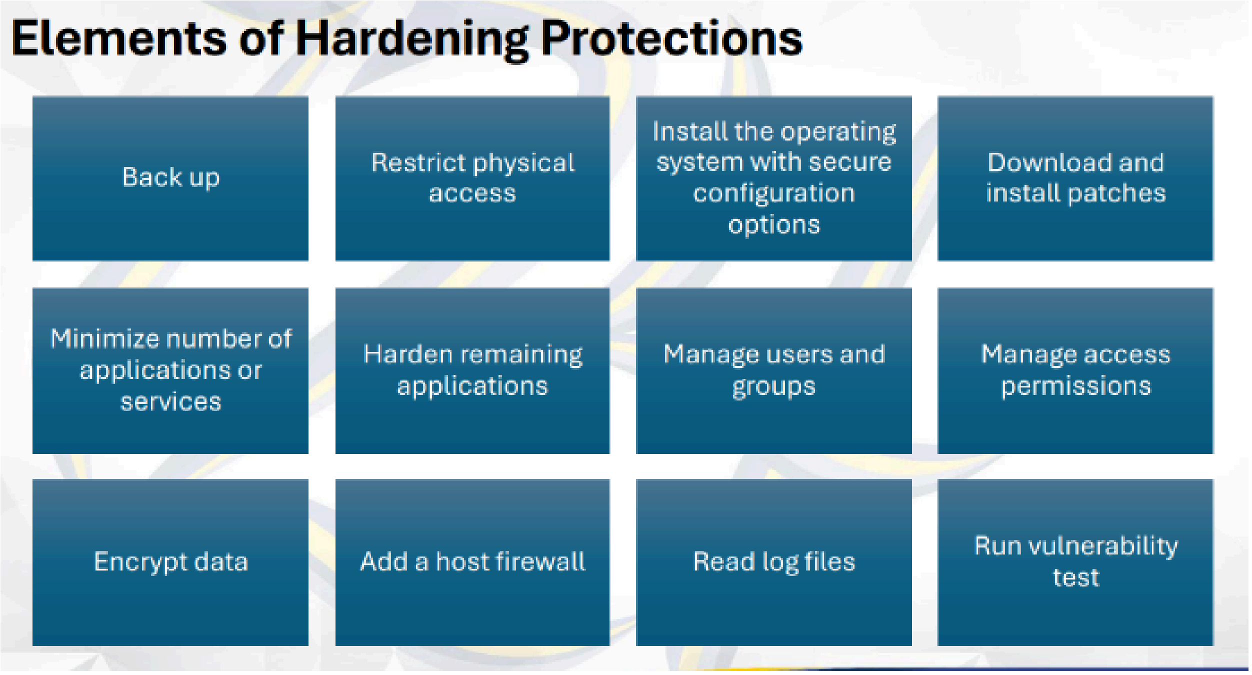
HOST HARDENING - 1

Host

- Any device with an IP address is a host
- Servers, clients, routers, firewalls, and even many mobile phones

Host Hardening

- The process of protecting a host against an attack
- Hardening is the number of protections that often have little in common with each other



Elements of Hardening Protections

Back up	Restrict physical access	Install the operating system with secure configuration options	Download and install patches
Minimize number of applications or services	Harden remaining applications	Manage users and groups	Manage access permissions
Encrypt data	Add a host firewall	Read log files	Run vulnerability test

Security Baselines

- Set of specific actions to be taken to harden all hosts of a particular type and of particular versions within each type
- Needed for servers with different functions such as webservers and email servers

Virtualization

- Allows multiple operating systems with thei associated applications and data to run independently on a single physical machine
- They run their own OS and share local system resources

Benefits of Virtualization

- Provides multiple benefits in the hosting hardening process
- Allows system administrators to create a single security baseline for each server (or remote client) within the organization

- Subsequent instances of that server can be cloned from an existing hardened virtual machine in a few minutes instead of hours or days
- Virtual environments can also benefit businesses by reducing labor costs associated with server administration, development, testing, and training

System Administrators

- IT employees that manage individual hosts or group of hosts are called system administrators
- They dont administer the network

Network Operating System

- Windows Server
- Windows NT, 2003, 2008, 2016, 2022, 2025

Computer Management Microsoft Management Console

- Most administrative tools in windows server come in the same general format called the microsoft management console (MMC)
- They all have the same general organisation with an icon bar a tree pane and sub sub-objects pane

UNIX (Including Linux) Servers Interface

GUI

- Gnome

Command-line interfaces (CLI)

- In UNIX its called shells

Vulnerabilities and Patches

Vulnerabilities

- The security weaknesses that open a program to attack

Exploits

- Programs that take advantage of the vulnerability

Zero-Day-Attacks

- Attack that come before fixes are released

Fixes

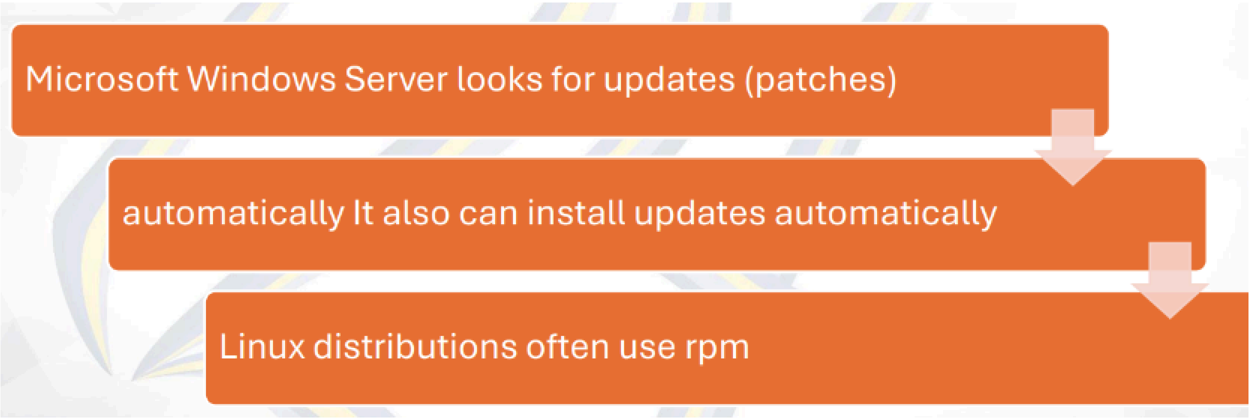
- When vendors discover that they have vulnerabilities, they create fixes

1. **Work Around**
    - Manual actions to be taken No new software
    - Labor intensive and therefore expensive and error prone

2. **Patches**
    - Small programs that fix vulnerabilities
    - Easy to download and install

3. **Service Packs**
    - Collections of patches and improvements (Microsoft Windows)

4. **Upgrading to a new version of the program**
    - Often security vulnerabilities are fixed in new versions
    - If the version is too old the vendor may even stop offering fixes



Microsoft Windows Server looks for updates (patches)

automatically It also can install updates automatically

Linux distributions often use rpm

Managing Users and Groups

Accounts

- Every user must have an account

Groups

- Individual accounts can be consolidated into groups
- Can assign security measures to groups
- Inherited by each groups individual members

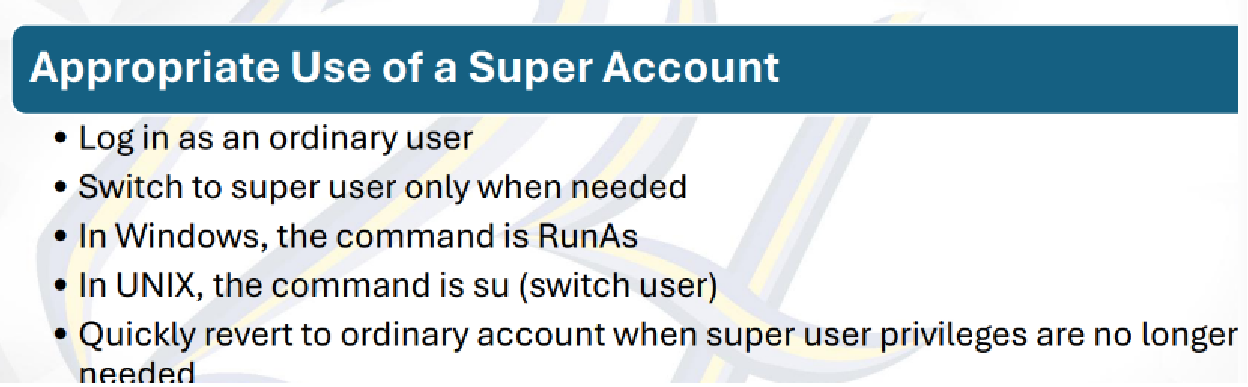
Why Assign Security Measures to Groups?

- Reduces labor costs compared to assigning security measures to individual accounts

- Assigning permissions to groups reduce errors because group permissions are more obvious than individual permission

Super User Account

- Every operating system has a super user account
- The owner of this acc can see or do anything
- Called as Administrator in Windows
- Called as Root in UNIX



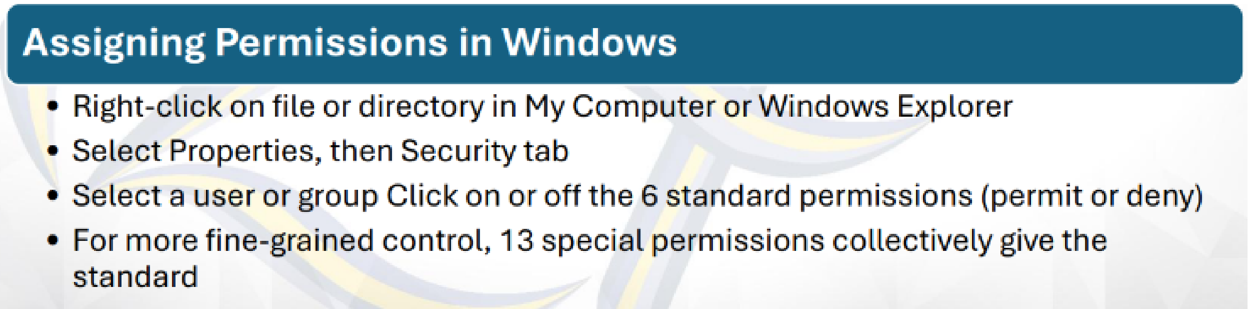
Appropriate Use of a Super Account

- Log in as an ordinary user
- Switch to super user only when needed
- In Windows, the command is RunAs
- In UNIX, the command is su (switch user)
- Quickly revert to ordinary account when super user privileges are no longer needed

Managing Permissions

Permissions

- Specify what the user or group can do to files, directories and subdirectories



Assigning Permissions in Windows

- Right-click on file or directory in My Computer or Windows Explorer
- Select Properties, then Security tab
- Select a user or group Click on or off the 6 standard permissions (permit or deny)
- For more fine-grained control, 13 special permissions collectively give the standard

Host Hardening - 2

Testing Vulnerabilities

- Attempts to find any weaknesses in a firm's protection suite before attackers do
- To do a vulnerability testing a security administrator installs vulnerability testing software on his or her PC then runs it against the servers within the security administrator realm of concerns

Vulnerability Testing Plan

- Tester should prepare an exact list of testing activities
- Supervisor must approve in writing to cover the tester supervisor must agree in writing to hold the tester blameless if there is damage
- Tester must not diverge from the plan

Client PC Security Baselines

- Fore each version of each operating system
- Within an operating system for different types of computers (desktop versus notebook, in-site versus external, high risk versus normal risk etc.)

Windows action Center

- The control panel for most common security features system and security category for most common security features system and security category allows access to each individual component

Automatic Updates for Security Vulnerabilities

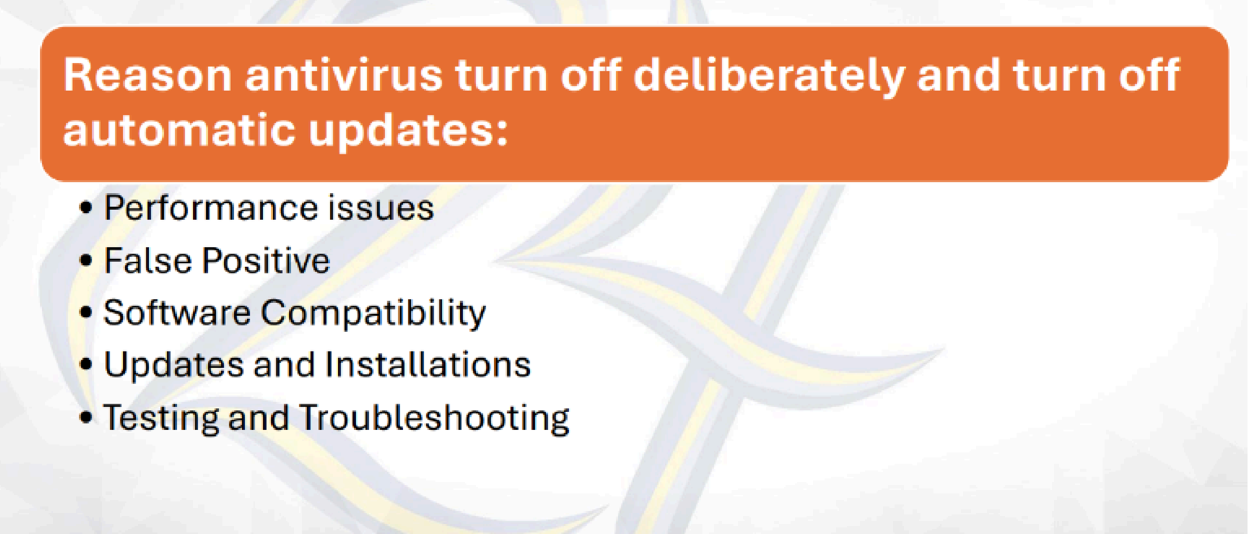
- Completely automatic updating is the only reasonable policy

Anti virus and Anti spyware Protection

- Important to know the status of anti virus protection

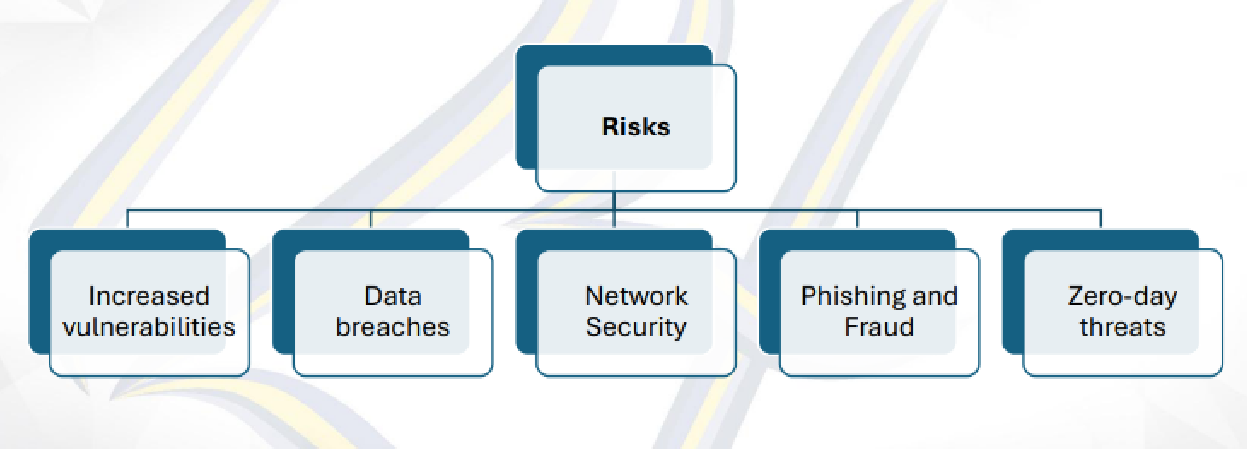
Anti-virus protection is critical but it is easy to make antivirus programs ineffective

- Users turn off deliberately
- Users turn off automatic updating for virus signatures
- Users do not play the annual subscription and so get no more updates



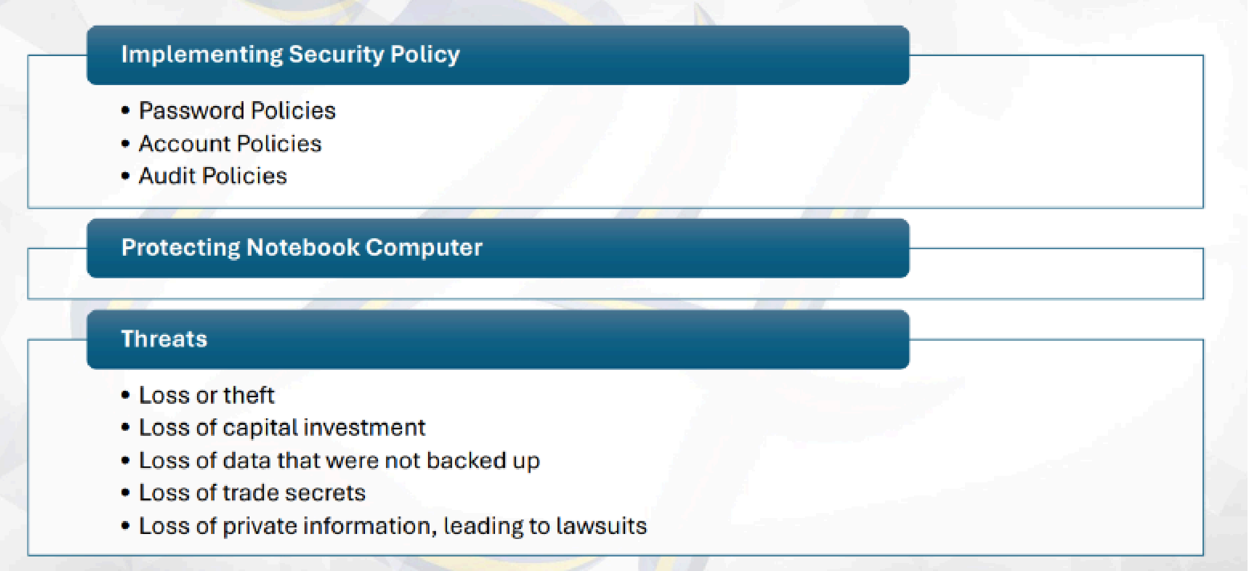
Reason antivirus turn off deliberately and turn off automatic updates:

- Performance issues
- False Positive
- Software Compatibility
- Updates and Installations
- Testing and Troubleshooting



Windows firewall

- This stateful packet inspection (SPI) firewall has been included in all subsequent silent versions of Windows
- **Action Center** - lets users check the status of their windows firewall installations



Implementing Security Policy

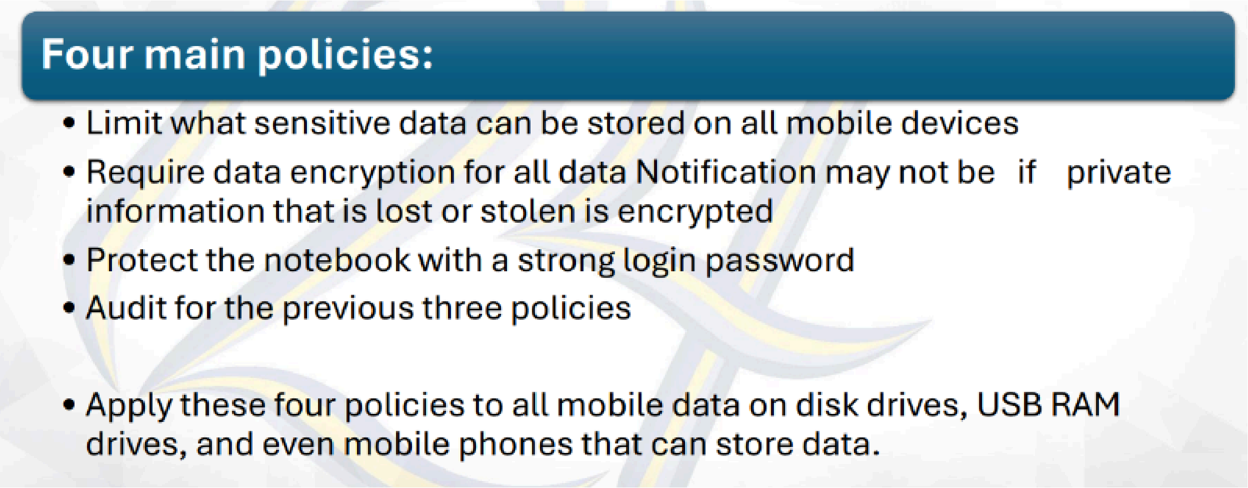
- Password Policies
- Account Policies
- Audit Policies

Protecting Notebook Computer

Threats

- Loss or theft
- Loss of capital investment
- Loss of data that were not backed up
- Loss of trade secrets
- Loss of private information, leading to lawsuits

Policies for Sensitive Data



Four main policies:

- Limit what sensitive data can be stored on all mobile devices
- Require data encryption for all data Notification may not be if private information that is lost or stolen is encrypted
- Protect the notebook with a strong login password
- Audit for the previous three policies

- Apply these four policies to all mobile data on disk drives, USB RAM drives, and even mobile phones that can store data.

Centralized PC Security Management

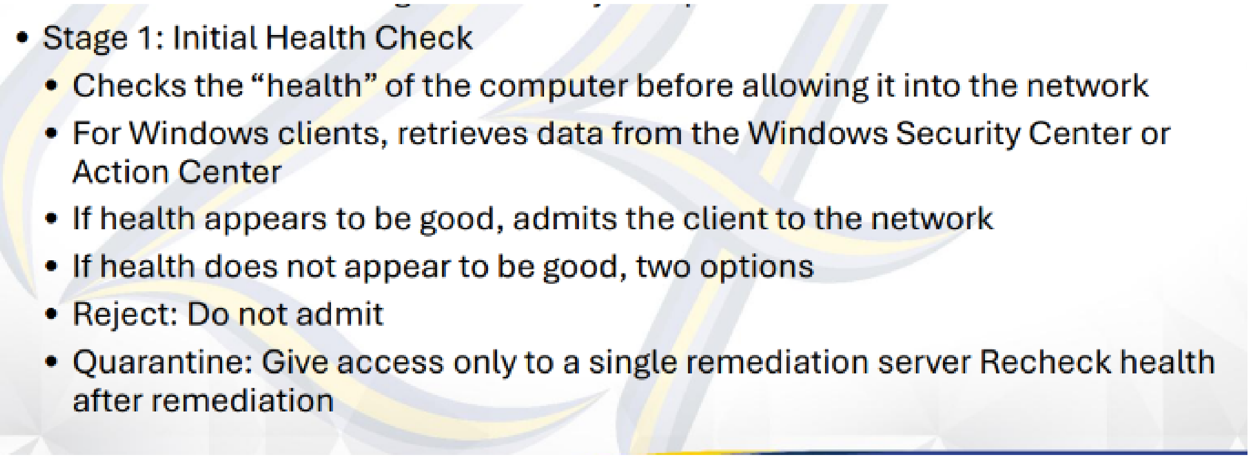
- Ordinary users lack the knowledge to manage security on thei PC
- They sometimes knowingly violate security policies
- Also centralized management often can reduce costs through automation

3 major approaches

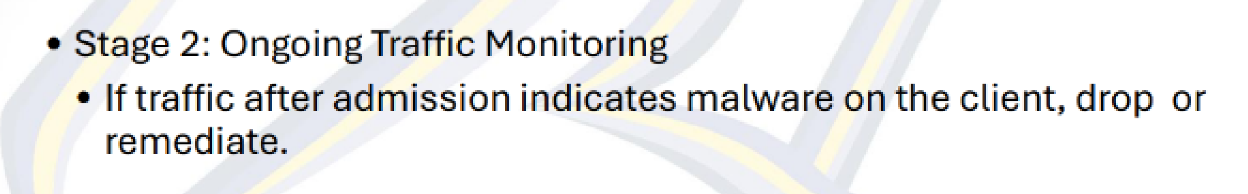
1. **Standard Configuration for PC**
    - May restrict applications, config settings, and even User Interface
    - Ensure that the software is configures safely
    - Enforce policies

- More genrally reduce maintenance costs by making it easier to diagnose errors

2. **Network Access Control (NAC)**
    - goal is to reduce the danger check bt computers with malware



- Stage 1: Initial Health Check
    - Checks the “health” of the computer before allowing it into the network
    - For Windows clients, retrieves data from the Windows Security Center or Action Center
    - If health appears to be good, admits the client to the network
    - If health does not appear to be good, two options
    - Reject: Do not admit
    - Quarantine: Give access only to a single remediation server Recheck health after remediation



- Stage 2: Ongoing Traffic Monitoring
    - If traffic after admission indicates malware on the client, drop or remediate.

3. **Windows Group Policy Objects (GPOs)**
    - Sets governing a particular class of computers (e.g. on-site, normal risk desktops)
    - Domain controller pushes GPO out to target computers
    - Target computers obey the policy set