COMPTIA SECURITY+ SY0-701 · WEEK 13

Identity, Access, and Automation



Objectives 4.6 and 4.7 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Describe the account lifecycle from identity proofing and provisioning to attestation and removal.
2. Explain how federation and SSO work with LDAP, SAML, and OAuth, and why interoperability matters.
3. Choose among mandatory, discretionary, role-based, rule-based, and attribute-based access control.
4. Design MFA with factors from different categories and compare tokens, biometrics, and security keys.
5. Apply password best practices, password managers, and passwordless sign-in to a scenario.
6. Explain just-in-time permissions, password vaulting, and ephemeral credentials for privileged access.
7. Weigh the benefits of security automation against its complexity, cost, and supportability.

AGENDA

9 min	The account lifecycle
9 min	Federation, SSO, and interoperability
9 min	Access control models and least privilege
8 min	Exercise 1: name the model
9 min	Multifactor authentication
9 min	Passwords, password managers, and passwordless
7 min	Privileged access management
9 min	Automation and orchestration use cases
8 min	Benefits and considerations of automation
10 min	Exercise 2: automate the clinic's IAM work
3 min	Wrap-up

An account's life runs from proofing to removal

1

Proof identity

Verify the person is who they claim to be

2

Provision

Create the account from a role template

3

Assign

Grant only the permissions the job needs

4

Attest

Managers confirm access is still needed

5

Deprovision

Disable on the last day; remove access everywhere

One login, many services, through trust

Protocol	What it does	Typical use
LDAP	Queries and updates a directory of users	Directory lookups; LDAPS on TCP 636
SAML	Signed XML assertions from IdP to SP	Web SSO to business SaaS apps
OAuth	Grants an app limited access with a token	Let an app read your calendar
OpenID Connect	Adds authentication on top of OAuth	Sign in with an existing account
Federation	Trust between separate identity domains	Partner staff use their own logins

Who decides access, and on what basis

Model	Who or what decides	Example
Mandatory (MAC)	System labels and clearances	Secret clearance reads Secret files
Discretionary (DAC)	The owner of the resource	A file owner shares a folder
Role-based (RBAC)	The user's job role	The Nurses group can open charts
Rule-based	Admin-set rules applied to everyone	Firewall ACL; no sign-in from abroad
Attribute-based (ABAC)	Attributes of user, resource, context	Doctor, own patient, on clinic network
Time-of-day restrictions	The clock	Front desk sign-in 7 a.m. to 7 p.m. only

Exercise 1: name the access control model



6

MINUTES · INDIVIDUAL

Name the access control model each scenario describes. For the last two, name the principle broken and the fix.

1. Files are labeled Top Secret and checked against clearance
2. Anyone in the Billing group can open the billing system
3. A file's owner decides to share it with a coworker
4. Access only for doctors, to their own patients, from the clinic
5. A firewall blocks all inbound traffic except TCP 443
6. Temporary staff accounts cannot sign in on weekends
7. A new hire's account is copied from a 10-year employee's
8. The IT intern is a domain admin so tickets close faster

MFA means factors from different categories



Something you know

A password, PIN, or answer to a security question

Weakest alone; can be phished



Something you have

A hard token, authenticator app, smart card, or security key

TOTP app, FIDO2 key



Something you are

Biometrics: fingerprint, face, iris, or voice

Tuned by FAR, FRR, and CER



Somewhere you are

Location from GPS, IP address, or network

Block sign-ins from abroad

Long, unique, and stored in a manager

Password best practices

- Length: long passphrases matter most
- Complexity: mixed character types if policy requires
- Reuse: password history blocks old passwords
- Expiration: maximum age forces a change
- Age: minimum age stops cycling back

Beyond the password

- Password managers make unique passwords practical
- Passwordless: FIDO2 passkeys, Windows Hello
- The private key never leaves the device
- Resists phishing because the site is checked

Give admin rights only when and while needed

Just-in-time

Admin rights granted for a task, then removed automatically

Two hours, approved by ticket

Password vaulting

Admin passwords kept in a vault, checked out, and rotated

Session recorded on checkout

Ephemeral credentials

Short-lived credentials created for one use, then expired

Cloud token valid for one hour

Automate the tasks people repeat or forget

Use case	Example
User and resource setup	New hire gets an account; templates build servers
Guard rails	Block a public storage bucket before it deploys
Security groups	Add users to groups by role; remove on job change
Tickets and escalation	Alert opens a ticket; pages on-call if unanswered
Services and access	Disable an account and its sessions at termination
CI, testing, and APIs	Scan every build; connect tools through their APIs

Automation multiplies whatever it is given

Benefits

- Efficiency, time saving, and faster reaction time
- Enforces baselines and standard configurations
- Scales without adding staff
- Workforce multiplier for a small team
- Employee retention: less tedious work

Other considerations

- Complexity: harder to understand and debug
- Cost to build, license, and maintain
- Single point of failure if the engine breaks
- Technical debt from quick, undocumented scripts
- Ongoing supportability when the author leaves

Exercise 2: automate the clinic's IAM work



8

MINUTES · SMALL GROUPS

For each task, decide whether to automate it, name the use case, and give one benefit and one risk.

1. Create accounts and groups for each new hire from the HR system
2. Disable accounts when HR marks a termination
3. Weekly report of accounts with no MFA or no login in 30 days
4. Approve a doctor's request to see another clinic's records
5. Isolate a laptop automatically when EDR detects ransomware
6. Rotate the domain admin password after each use

REVIEW

Five questions: write your answers first

1. What is identity proofing, and when does it happen?
2. Why is OAuth not, by itself, an authentication protocol?
3. How does role-based access control differ from rule-based access control?
4. Is a password plus a security question multifactor authentication? Why or why not?
5. What is the difference between password vaulting and ephemeral credentials?

TAKEAWAYS

Four things to take with you

01

Access follows the person

Proof, provision, review, and remove access the day people leave.

02

Know who decides access

MAC, DAC, RBAC, rule-based, and ABAC each answer who decides.

03

Factors must differ in kind

Two passwords are one factor; FIDO2 security keys resist phishing.

04

Automate, then support it

Scripts act fast and consistently, and must be documented and owned.

NEXT Lab 13: MFA, least privilege, and a short automation script