SOC FOUNDATIONS

Understand how data is protected, how users are verified, and why these ideas matter for SOC work.

THE CIA TRIAD

CIA = the foundation every security decision is built on.

CONFIDENTIALITY (keep secrets safe)
Only authorized people should see sensitive information.

Why it matters:
If attackers read private data = trust is destroyed.

Examples:

- customer records
- health information
- passwords
- payment details

Common protections:

- encryption (scrambles data)
- strong passwords
- access control (who is allowed to see what)
- role-based permissions (only need-to-know people see data)

Typical confidentiality failures:

- sending data to wrong email
- weak passwords
- public Wi-Fi without protection
- misconfigured cloud storage

SOC relevance:
Confidentiality breaches = data leaks, insider misuse, exfiltration alerts.

INTEGRITY (keep data accurate and unchanged)
Information must remain correct, complete, and trustworthy.

Real example:
If an attacker changes logs, investigators lose evidence.

What protects integrity:

- hashing (detects changes)
- digital signatures (proves origin)
- checksums (verification numbers)
- backups (restore original data)

Integrity threats:

- malware altering files
- unauthorized edits
- database tampering
- log wiping

SOC relevance:
Analysts must detect tampering and validate data sources.

AVAILABILITY (keep systems usable)
Authorized users must access systems when they need them.

Example:
Hospital systems must stay up — downtime risks lives.

Availability problems:

- DDoS attacks
- server crashes

- hardware failure
- natural disasters
- poor maintenance

How organizations protect availability:

- backups
- redundant servers
- failover systems
- monitoring
- incident response plans

SOC relevance:
When systems slow, crash, or are attacked, SOC teams investigate.

CIA QUICK CHECK

When assessing incidents, ask:

Did someone see data they shouldn't? → Confidentiality
Did someone change data wrongly? → Integrity
Did someone block access? → Availability

AUTHENTICATION — PROVING "WHO YOU ARE"

Authentication answers:

Is this really the correct user?

Three authentication categories:

1. Something you know
   (password, PIN, security answer)
2. Something you have
   (OTP code, smart card, phone token)
3. Something you are
   (fingerprint, face, iris, voice)

Multi-Factor Authentication (MFA):
Uses 2 or more of the above — makes accounts far harder to hack.

SOC relevance:
Many incidents start with stolen passwords — MFA reduces risk.

AUTHENTICATION EXAMPLES (REAL LIFE)

- logging into email (password + OTP)
- banking app (fingerprint + phone)
- office entry (badge + fingerprint)
- social media (password + login link)

Pattern to remember:
More layers = stronger protection.

IDENTITY ASSURANCE — CONFIRMING REAL PERSON

Authentication proves login.
Identity assurance proves the **person behind it** is legitimate.

Used in:

- banks
- government portals
- telecom verification
- hiring/onboarding

Methods:

- ID document check
- personal info verification
- face/photo match
- fraud screening

SOC relevance:
Stops fake accounts and identity abuse.

NON-REPUDIATION — NO “I DIDN’T DO IT” EXCUSES

A user cannot deny their actions later.

How:

- digital signatures
- audit logs
- transaction records
- timestamps

Example:

A signed digital contract proves exactly who agreed and when.

SOC relevance:

Logs help trace attackers and support investigations.

PRIVACY — PROTECTING PEOPLE, NOT JUST FILES

Privacy focuses on respecting personal data.

Good privacy practices:

- only collect necessary data
- store securely
- restrict access
- use only for legitimate purposes
- delete when not needed anymore

Bad privacy example:
A company storing copies of IDs forever “just in case.”

SOC relevance:
Privacy violations often become legal incidents.

PRIVACY AT WORK — GOOD SECURITY HABITS

Most breaches come from human mistakes, not hacking.

Important habits:

- lock screens when leaving
- don’t leave papers on desks
- don’t share credentials
- think before clicking links
- report suspicious emails

Rule:
If something feels off — report it.

DEFENSE IN DEPTH — LAYERS OF SECURITY

Idea:

No single control is perfect.

Security uses layers so if one fails, others still protect.

Layers include:

- policies and rules
- user training
- authentication controls
- encryption
- network monitoring
- firewalls
- physical security
- backups

SOC relevance:

SOC monitors several layers at once.

KEY TAKEAWAYS

- CIA Triad is the base of security
- Authentication proves identity
- MFA is one of the strongest protections
- Identity assurance prevents fake accounts
- Non-repudiation gives proof of actions
- Privacy protects real people
- Defense-in-depth uses layers, not one control

WHY THIS MATTERS FOR SOC ANALYSTS

SOC analysts constantly ask:
What part of CIA was impacted?
Was identity abused?
Was data leaked, changed, or blocked?

These foundations shape:

- alert triage
- investigation logic
- risk assessment
- communication with teams

Tools make sense only when concepts are understood.

REFLECTION

Cybersecurity is really about building trust:
Trust in systems, trust in data, trust in identity, trust in privacy.

Today built the mental framework I'll use every day as a SOC analyst.