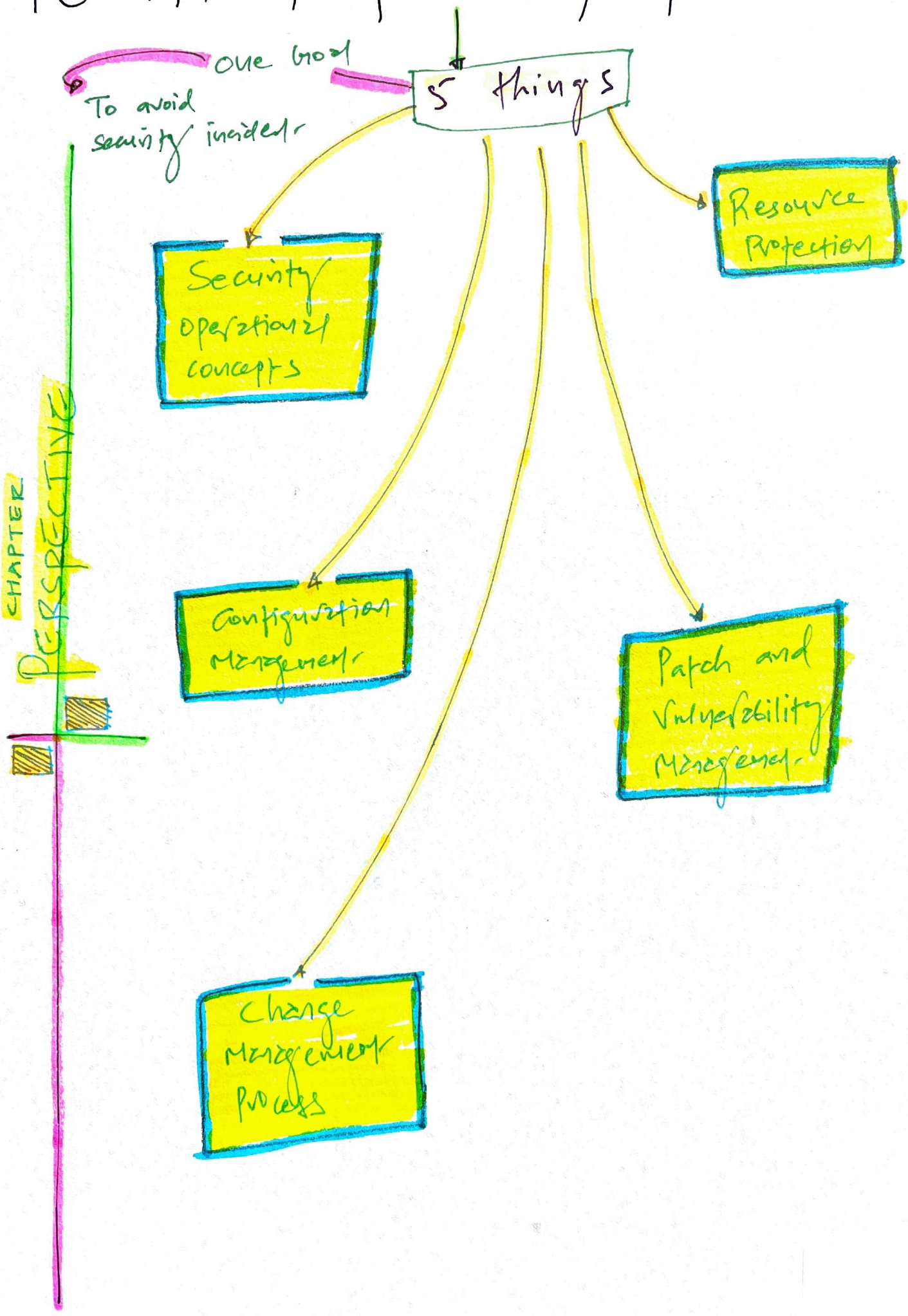
16. Managing Security Operations



APPLYING SECURITY OPERATIONS CONCEPTS

Senior Management → Responsible → Due Care
Responsible → Due Diligence

Address Fundamental Security operation concepts to reduce the risk.

Taking good care of Information & Asset on ongoing basis.

* Need-to-know (only permissions) & Least Privilege (Rights + Permissions)

Need-to-know (only permissions)

Focus on Permission (Allows access to object such as files)

Allowed to go & read time

Associated with Security clearance

Dave has security clearance for secret data. It doesn't mean he can access all the secret data.

Admin provide access to limited secret data based on Need-to-know.

Least Privilege (Rights + Permissions)

Focus on privilege (Rights + Permission)

Rights refer to ability to take actions

Allowed to go & change the time

- This principle needs well defined job descriptions

When you control Privilege

it controls Confidentiality and Integrity of data

Admin doesn't mean Full control = Consider only privilege

* Additional concept with Need-to-know and Least privilege

Entitlement

Privileges we get when Account is set up for first time.

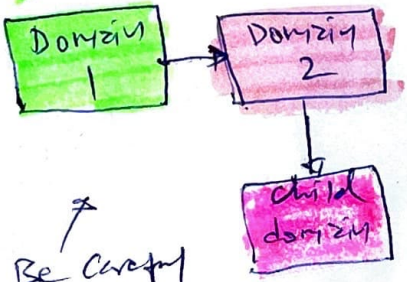
Aggregation

Privilege creep - user continue to gain privilege

↓

Revoke

Transitive Trust



Be careful

- Non-transitive trust enforce principle of least privilege.

* Separation of Duties & Responsibilities

Golden Eye +

Once Upon A Time In Mumbai

+ Movie Theatre ticket operation

Still chance of Collusion but takes more effort

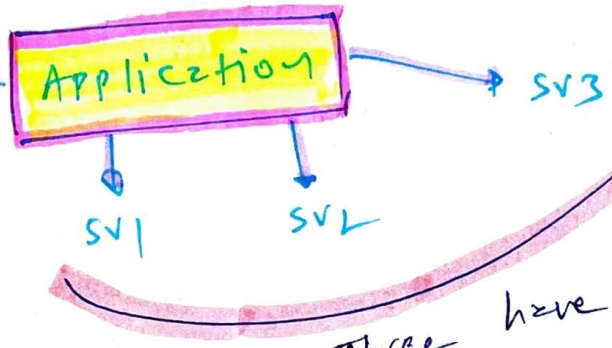
- Separation of duties ⇒ reduce fraud by requiring collusion

↓

Divide by security capabilities + functions among individuals.

Seperation of Privilege = Granular rights + permissions

Builds on top of Least privilege → Apply to Process + Apps



Three have access to specific functions within Apps = seperation of privilege.

Segregation of Duties

- Refer to (← P.T.O) movies + theatre example
- Goal = Restrict individuals having excessive system to reduce fraud.
- If seperation not possible = consider compensating controls to mitigate the risk

Require for SOX - Sarbanes Oxley Act

Two-person control = Holder Eye

Split knowledge = seperation of duties + two-person control

- Need 2 keys to open Box
- Need CEO + CFO to take critical business decision

* Job Rotation

As security control

As → Reduce Fraud

Control → Cross Training

Act As → Deterrent mechanism — if employee know their someone will take their job role, they less likely to involve in fraud activity.

Act As → Detective mechanism

* Mandatory Vacations

To detect → Fraud

To detect → Collusion

Deterrent

Detection

* PAM - Privilege Account Management

Personnels don't have more privileges than they need + they don't misuse privilege

Elevated privileges can be misused to harm CIA of Assets.

Monitoring of privileged entities is important.

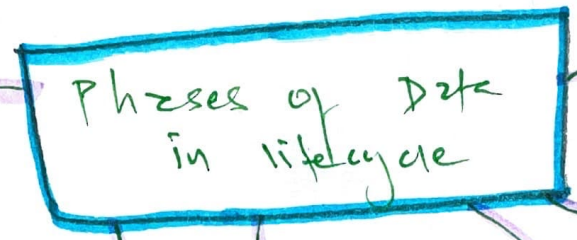
→ Tools available to Automate this

! - it can also detect Advanced Persistent threat (APT) activities

* Managing the Information Lifecycle

Protect Data → Based on classification

Security control → To protect information throughout lifecycle



1 Creation (capture)

- Either information is created or captured (from logs)

2 Classification

- Identify sensitive information based on classification
- Marking (labeling) to recognize data value

3 Storage

- Security controls based on data classification
  - (a) Prevent Unauthorised Access
  - (b) Encrypt Data
  - (c) Back-up
  - (d) Physical control
  - (e) Environmental control

4 Usage

Data-in-use + transit = Encryption

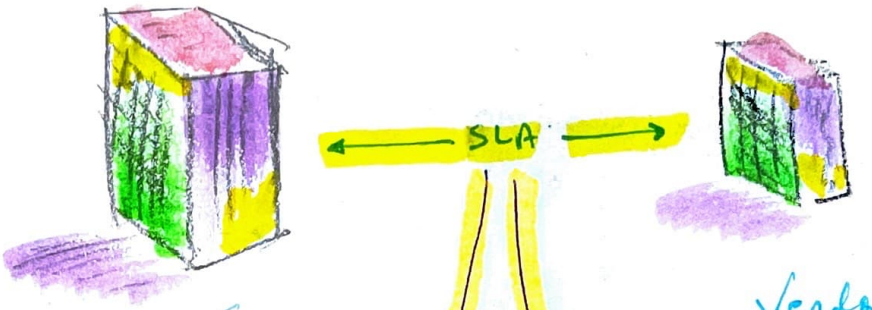
5 Archive

Off-site data retention need same security control considerations

6 Destruction (Purging)

- Sanitizing media
  - NIST 800-88R1

* Service Level Agreements (SLA) — NIST 800-47



Performance Expectation

Availability of services

Also use **MOU** — Memorandum of Understanding + Interconnection

Not as effective as SLAs

ISA — Security Agreement

Used to define technical requirements (Encryption, Protocols) if two parties transmit sensitive data

* Addressing Personal Safety & Security

Duress

- Lonely guard can't fight with mob. He just press alarm button or play around with the phrase over phone "Everything is fine."

Emergency Management

- DRP (Ch. 18)

Security Training and Awareness

~~DRP (Ch. 18)~~

When Employees Travel = secure!

- Sensitive Data
- Malware & Monitoring Devices
- Free Wi-Fi
- VPNs

2

SECURELY PROVISIONING RESOURCES

Focus:
Provisioning + Management
of

- H/W + S/W Assets
- Virtual Assets
- Cloud-based Assets.

* Managing Hardware & Software Assets

Hardware Inventories

- track hardware assets with barcode
- RFID expensive than barcode but reduce inventory time
- Sanitize H/W
- Treat portable media with table = include in inventory

Software Licensing

- Protect license key
- Ensure unauthorised software is not installed
  - SCCM can detect (configMgr)

Protecting Physical Assets

- Protect organization's Building and contents
- Consider physical security controls.

* Managing Virtual Assets

Virtualization's primary software component → **Hypervisor**

Additional layer of software on physical server = introduce additional attack surface

Virtual Assets to

- VM
- VDI
- SDNs
- VSAN

secure

* Managing Cloud-Based Assets

NIST SP 800-145 + 800-144

- **SaaS**
  - Full service via web browser
  - e.g. Gmail
- **PaaS**
  - H/w + s/w + Apps
- **IaaS**
  - cloud → Infra (server + storage) + networking resources
  - customer → Install + maintain OS + Apps

cloud Deployment

- Private
- Public
- Hybrid
- Community

* Media Management

↑ Is stored data secure?

FROM

- Unauthorised access
  - physical location
  - logical Access (technical controls)
- Environmental protection
  - temp
  - Humidity
- Lable / marking to ensure CIA

* Tape Media

Don't expose to magnetic field = corrupt data (Erase)

2 copies
- on-site
- off-site (dr recovery)

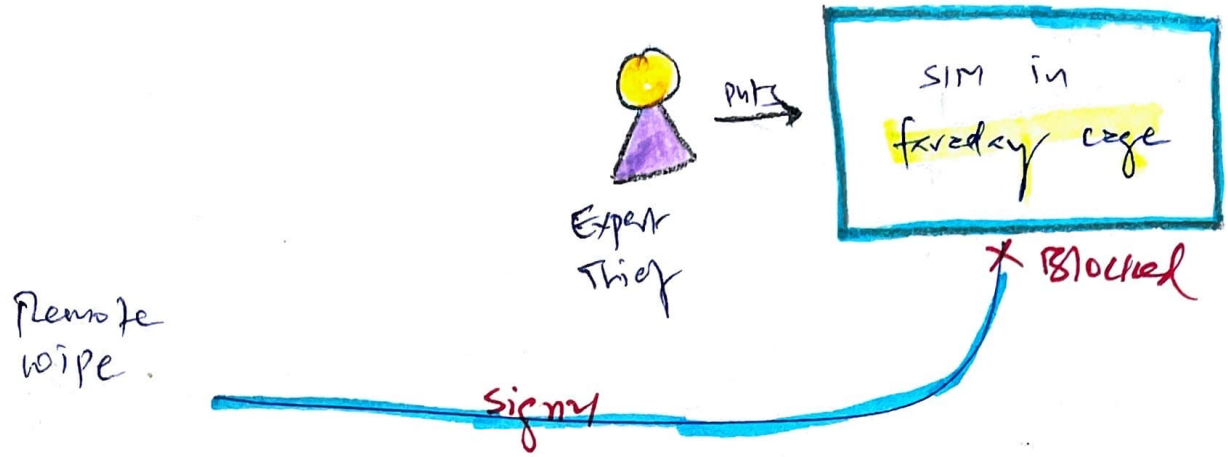
← Apply security controls

* Mobile Devices

BYOD is challenging for organization → moving to → COPD

COPD → Easy to manage + enforce security with MDM

→ Controls = Encryption, Remote wipe, MFA, Screen lock



* Managing Media lifecycle

When media reaches ⇒ MTTF (Mean Time To Failure)

MTTF value presents number of times media can be reused

Destroy Media

Destroy based on the classification

Sensitive = brutal destruction

SSD

Degaussing doesn't remove data — just burn the SSD!

MTTF VS MTBF (Mean Time Between Failures)

Can't repair after fail.

Time b/w failure to when personnel will repair it

3 MANAGING CONFIGURATION

Focus = Deployed systems are consistently secure throughout the lifetime

Baselining

Achieve with secure baseline configuration for deploying images

Manual baseline = human error

Automate Tools ← Microsoft Group Policy.

Using Images For Baseline (3 step process) ← protect from malware

1 → Admin → PC
- Configure OS with security
- Test

2 → Export to single Image from that PC.

3 → Deploy secure image to all the systems

Benefits → security
→ less time = less cost
→ Easy to maintain

4 MANAGING CHANGE

Purpose: To reduce unanticipated outages caused by unauthorised changes.

CHANGE ?

|

it can

Affect 'A' of CIA triad

Reduce security

change Mgmt process

Document

Request the change

|

via s/w
- ServiceNow
- BMC

Review change

|

Peer Review

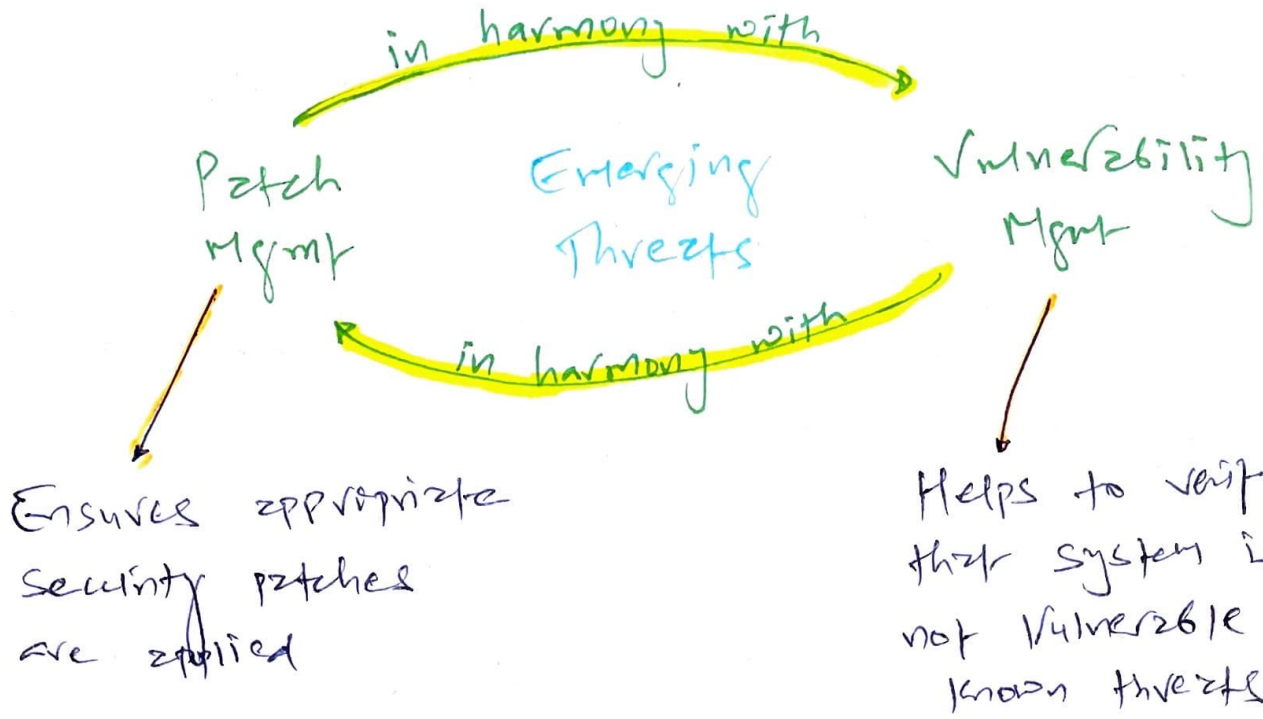
Approve/ Reject change

Based on peer review

Test change

Schedule/ implement

5. MANAGING PATCHES AND REDUCING VULNERABILITIES



* Patch Management

Most of security incident → No patch mgmt policy.

Equifax attack in 2017

Effective Patch Mgmt program steps

- Evaluate Patches
  - Is it required for system?
- Test Patches
  - Test in isolated non-prod
- Approve the patches
  - via change mgmt process
- Deploy patches
  - Automated (wordpress plugin)
- Verify that Patches are deployed
  - Test & Audit with Vulnerability Assessment Tools (Tripwire)

* Vulnerability Management

Regularly identify vuls. → Evaluate them → Mitigate risk based on criticality

2 Elements

Vulnerability Scanning

Goal is to detect vulnerabilities & mitigate them before attacker discovers them.

- Uses database of known security issues - constantly updated for zero-day attacks
- Nessus / Rapid 7 = first scan open ports for services & checks for known system vulnerabilities

Nessus: Do more than scanning
- Database scanning for input validation

* Blame mgmt if they don't address vulnerabilities, or accept the risk.

Vulnerability Assessment

- Part of risk analysis / risk assessment

1. identify value of assets
2. identify threats & vulnerabilities
3. Perform risk analysis to determine overall risk