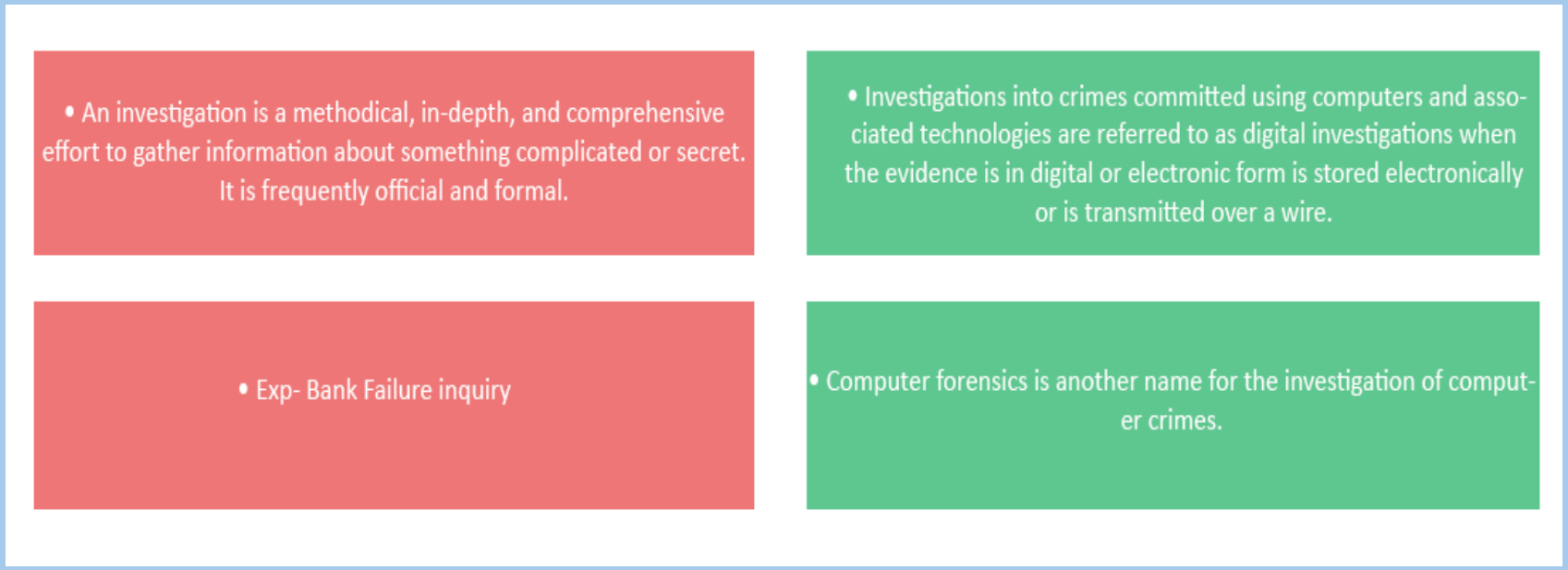
Domain 7

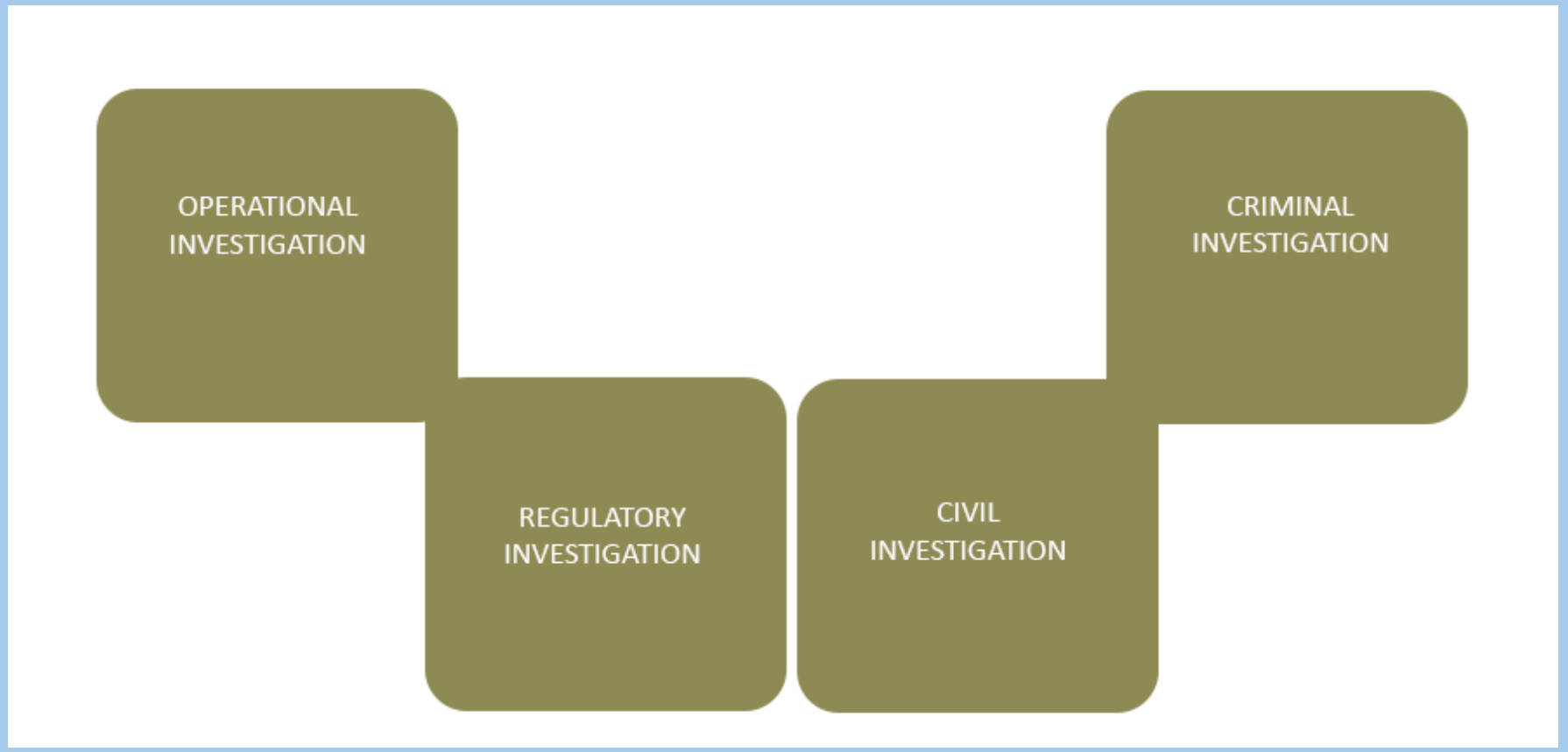
Security Operations

Types of Investigation

- Security issues – what/why/when/who -> if any Security issue occur -> who is responsible
- Establish Accountability – If any event occurs – collect evidence/Analyze



Types of Investigation



Types of Investigation - Operational

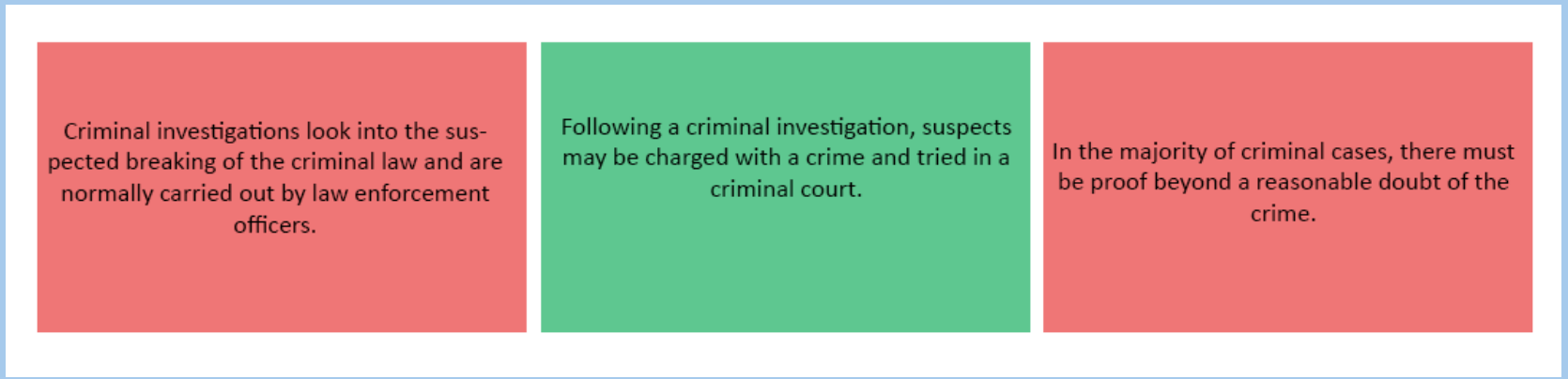
Any operational issue -> server outage -> investigate the reason

Types of Investigation - Regulatory

Security Incidents violated -> regulatory issues related to HIPAA, PCI-DSS (regulatory bodies involved)

Types of Investigation - Civil

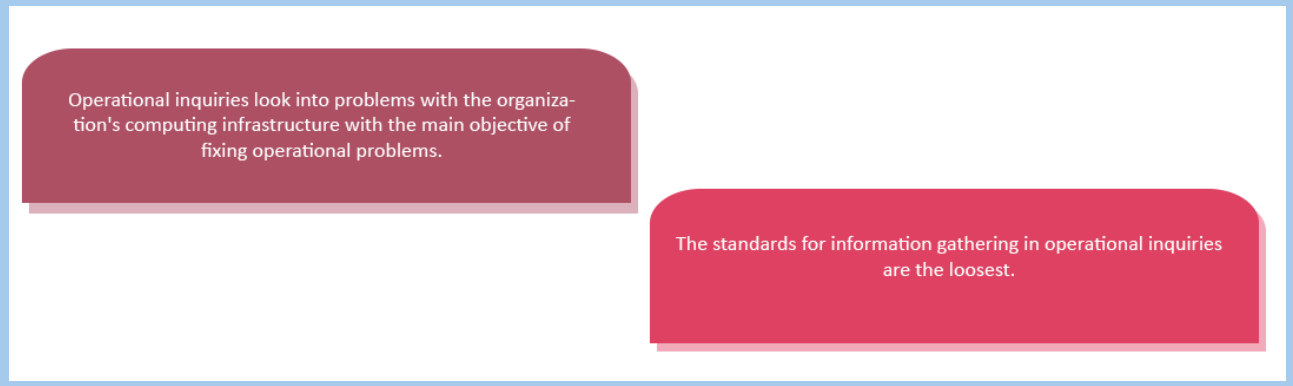
When contract violated -> due to Security issues
- Agreement between two companies
- If agreement breach – engage external parties
- IF NDA violated



Types of Investigation - Criminal

Security issues -> violated criminal issues -> law enforcement agencies involved
Investigation agencies involved
Prison or financial penalty

Investigation agencies involved
Prison or financial penalty



Investigation Challenges

- Limited time
- Intangible info (digital)
- Difficulty in gathering evidence
- Location of evidence

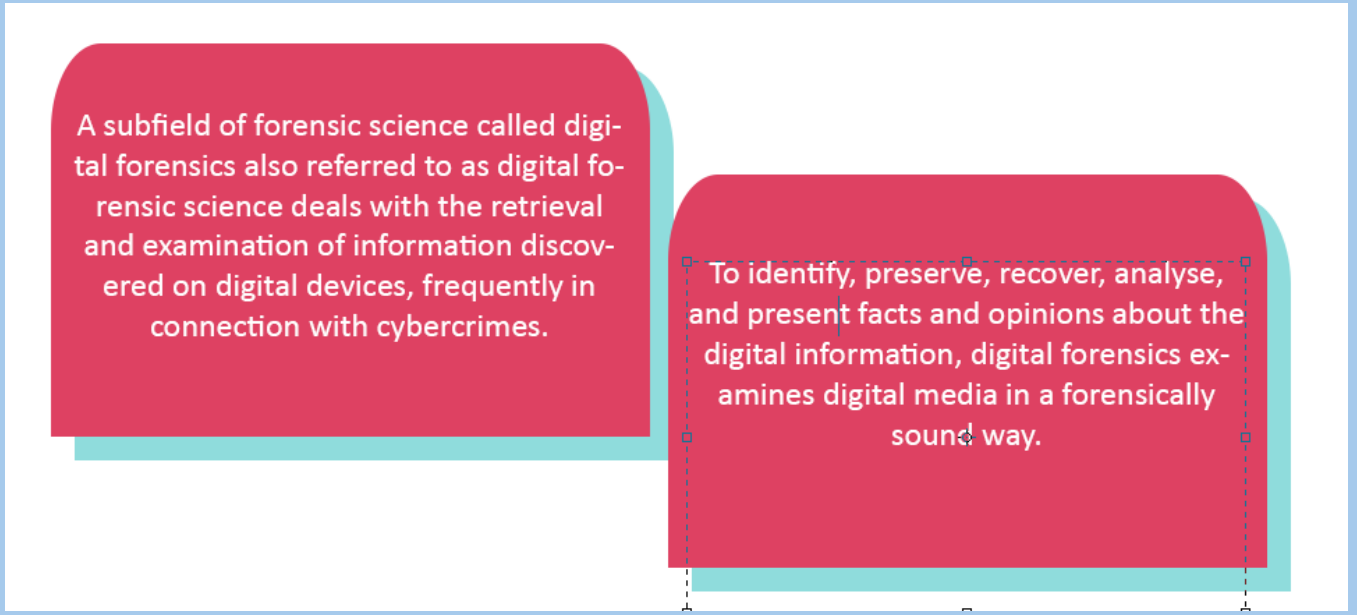
Components of Evidence

- Identification
- Once identified – protect the environment
- Take photographs
- Evidence identified
- Capturing the evidence
- Analyze the evidence
- Establish chain of custody (who are involved)
- Copy the evidence
- Store on media

Digital Forensics

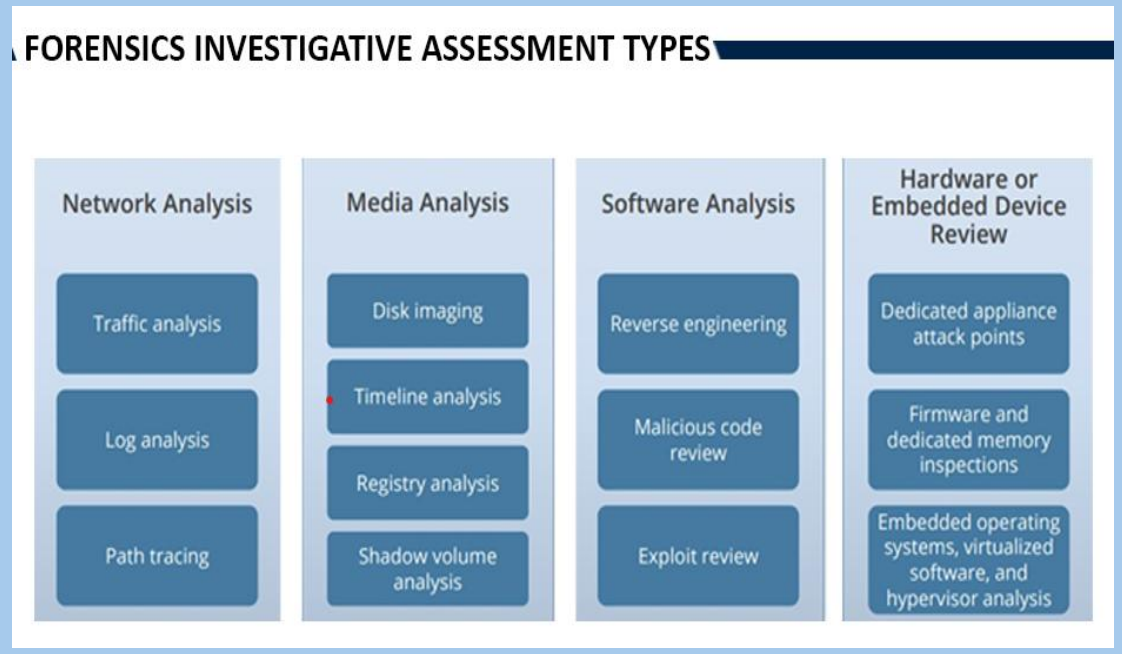
- Identify evidence
- Protect
- Examine
- Preserve

Gathering and Protecting the evidence



Forensic Investigation Types

- **Network Analysis Investigation**
  - All networks related logs to be captured
- **Media Analysis Investigation**
  - Image of particular hard drive
- **Software Analysis Investigation**
  - If any malware attack occur
- **Hardware or Embedded Review**
  - All the relevant device info to be captured

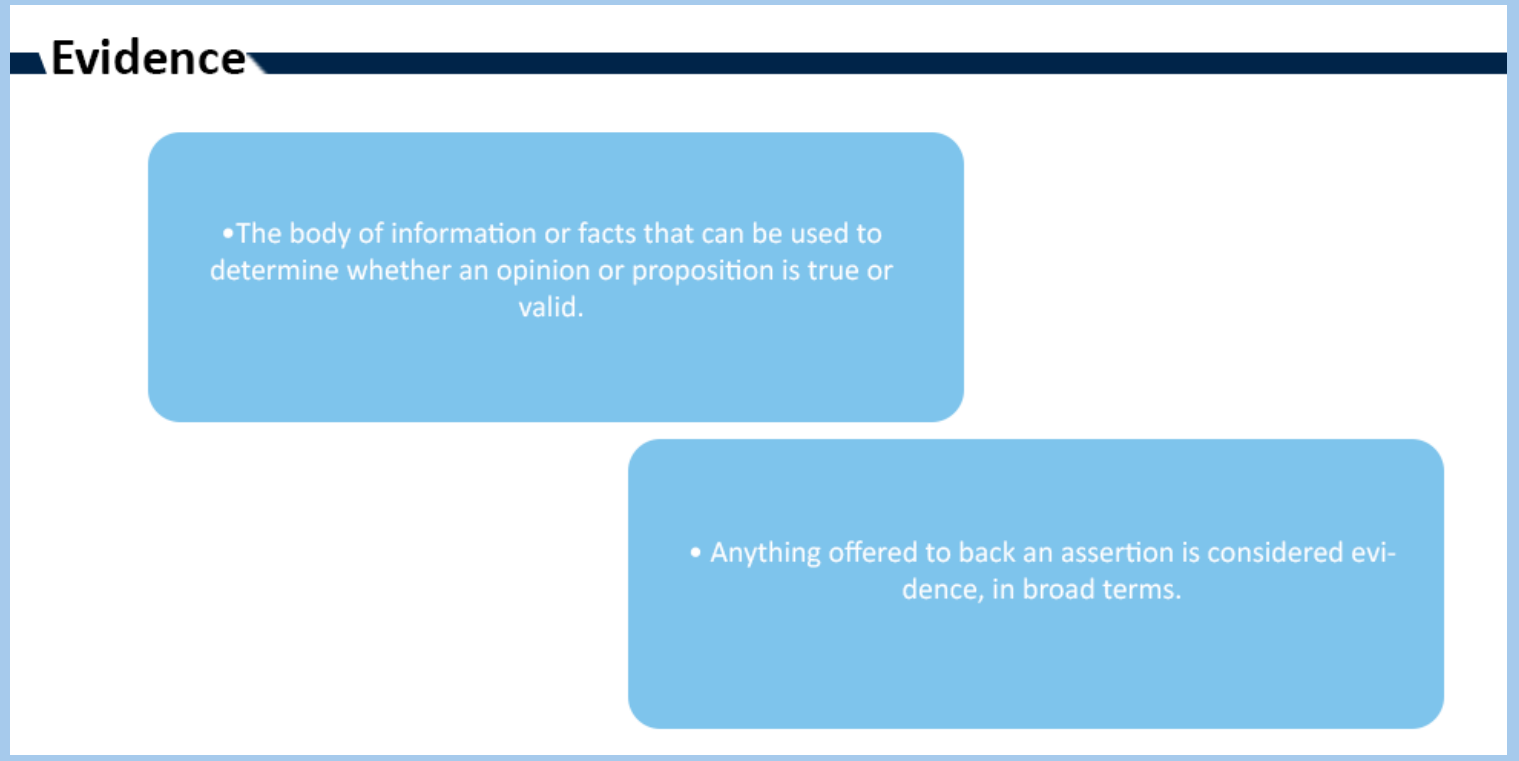


Evidence

Any tangible or intangible assets

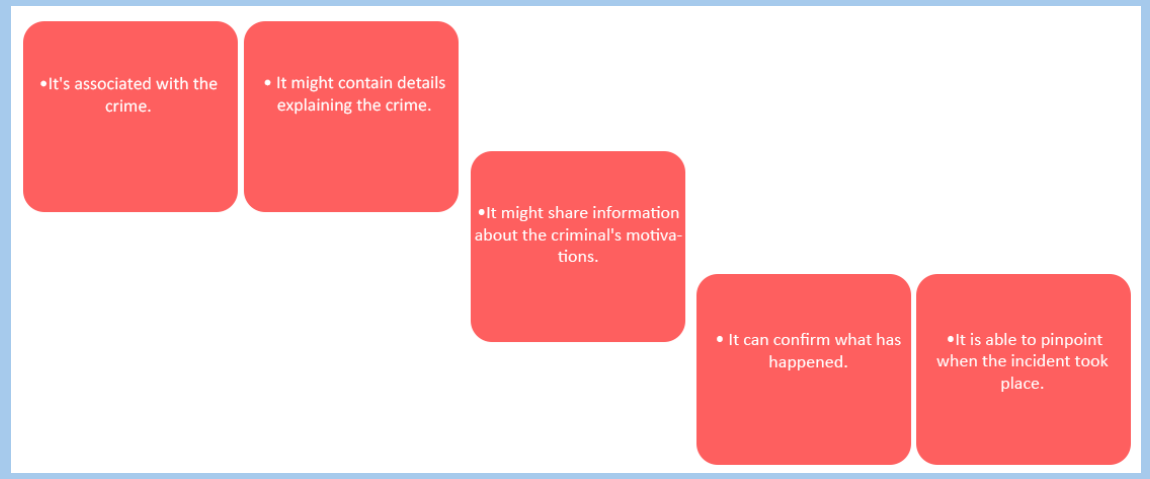
Five (5) Rules of Evidence

Evidence should be Authentic (confirm correct source)
Accurate
Complete
Admissible



Evidence Life Cycle

- Discover the evidence
- Protect
- Recording
- Collection
- Identify
- Preserve/Protect
- Transportation
- Present in court of law
- Return evidence to owner once done



- **Chain of Custody** (CoC)
  - Name, date, type, location etc.

- **E-Discovery**
  - If US justice system ask to provide evidence – they have to provide

- **Intrusion Detection System (IDS)** – Passive

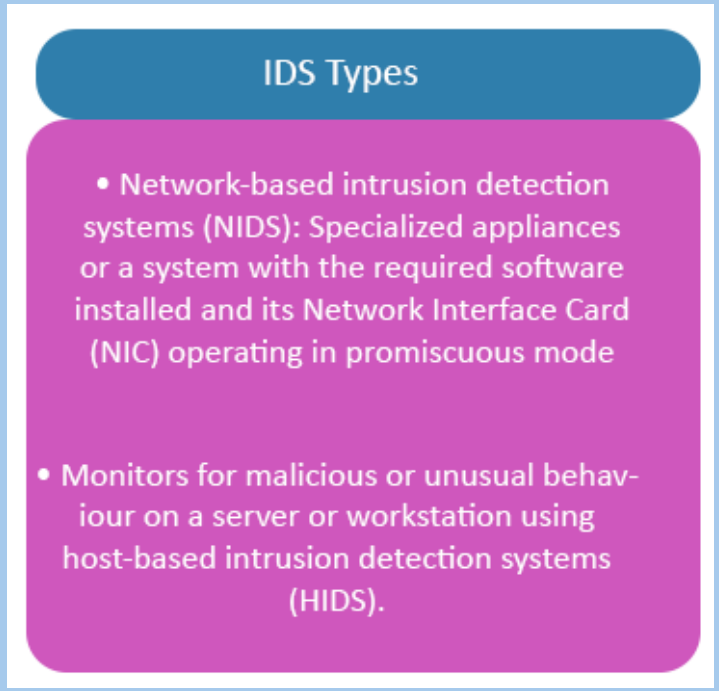
  - NIDS – Install on networks
  - HIDS – Install on hosts

  - If Firewall allow traffic from port 443 -> then some malware can bypass -> IDS can detect and generate alerts

- **Intrusion Prevention System (IPS)** - Active

  - Router ----Firewall----NIPS----Switch----NIDS

  - If Firewall install before NIDS → then Firewall blocks all the ports except the rule defined
  - If NIPS install before Firewall → All the traffic goes from NIPS & generate many alerts



Signature Based Detection

- NIPS verify from their Database and matches – if it matches then generate alerts
- Once https traffic flows from NIPS – they compare all attacks from Database and can detect only known attacks

Anti viruses

Matches traffic against list of non-malicious traffic pattern

Use normal traffic baseline to monitor abnormal traffic

Firewall, routers, switches

Faster – check traffic against malicious signatures

- Scan against malware signature

Behavior Based Detection

If any new attack – they start learning phase and will take longer time and provide many false positives

NIPS – Has Data of all possible attacks

NIPS – use for external attacks

IDS – use for internal attacks

Firewall – Preventive Control

Types of IDS

Network based

Placed on network segment (switch)

Protect against DDoS attack, Brute Force, Port scan

Host based

Placed on client side (server or workstations)

Who uses the systems, resources, traffic

Security Information and Event Management – SIEM

- Security Information Management
- Event Management

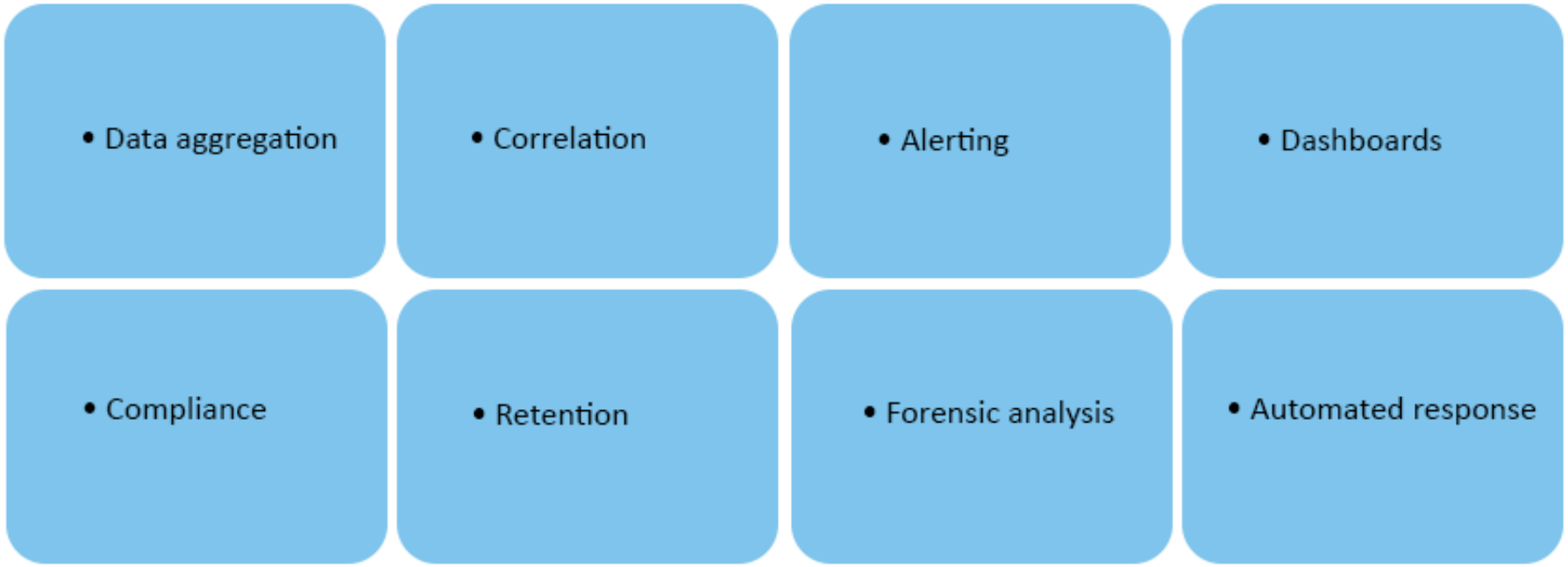
- **Security Information Management**
  - SIEM analyze logs info
    - Servers logs
    - Networks logs
    - IOT logs
    - Laptop logs

  - Those logs are for valid and invalid events
  - Invalid events are attacks

- **Information Management**
  - SIEM Tools have ability to read the logs and store on central place

- **Correlation**
  - Capture logs from different devices
  - Server logs
  - Networks logs
  - App logs
  - IOT logs

Functions of Security Information and Event Management (SIEM):



SOAR (Security Orchestration, Automation & Response)

- For tasks automation - Integrate with SIEM
- IPS
  - Signature based
  - Anomaly based
    - Tuning – is most important
    - Learning Period
    - False Positive
    - System tuned

Integrate with AI to respond automatically if any Incidents occur

Response Security Incidents automatically

Used for Incident Response

Honeypots

Designed to confuse the attackers that it's a real server

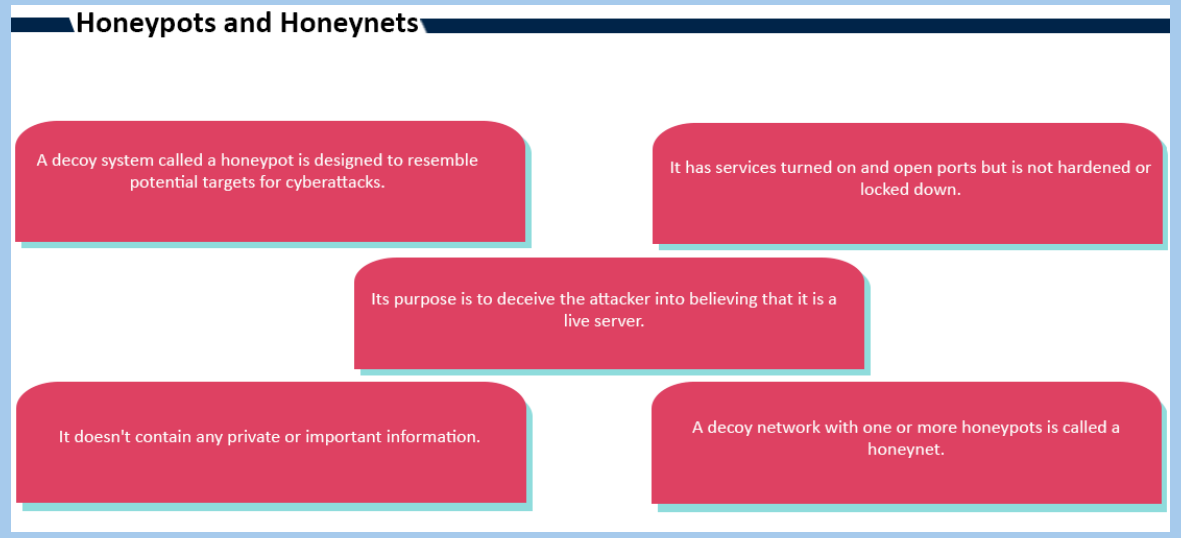
Looks like real system only to attract attackers

Honeypots from actual network by DMZ or firewall

File, folder that is used to attract attackers on single computer

Honeynet

Group of computers use to attract attackers



Data Aggregation

- Collected logs from different devices and store on central location

  Collection of Data from different sources for analysis

- SIEM – Logs
- IDS/IPS – Traffic

- CMaaS – Continuous Monitoring as a Service

- In organization, there are two types of traffic
  - **Ingress Filtering**
    - Traffic goes into organization
      - Firewalls
      - IDS/PDS

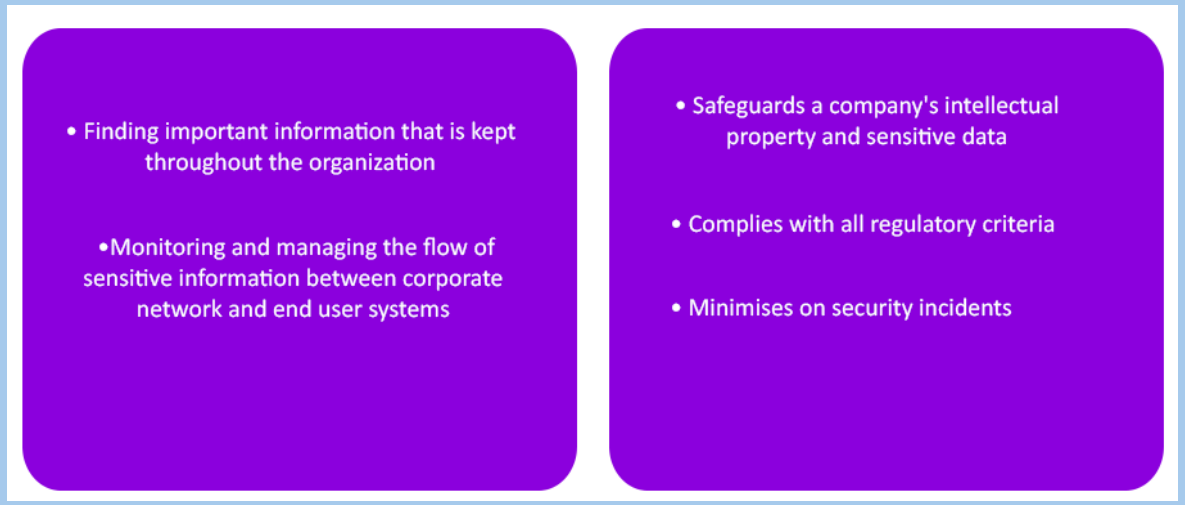
  - **Engress Filtering**
    - Traffic outside the organization
      - DLP, content filtering

Data Loss Prevention (DLP)

- Prevent Data breach when Data flowing outside the organization
- If Data is labeled – Ease to capture for DLP tool
- Monitor outgoing Data
- If Data going to invalid person, they stop

Protect & inspect Data when being sent out to the organization

Detect the Data steal attempt while Data in-use, transit or rest



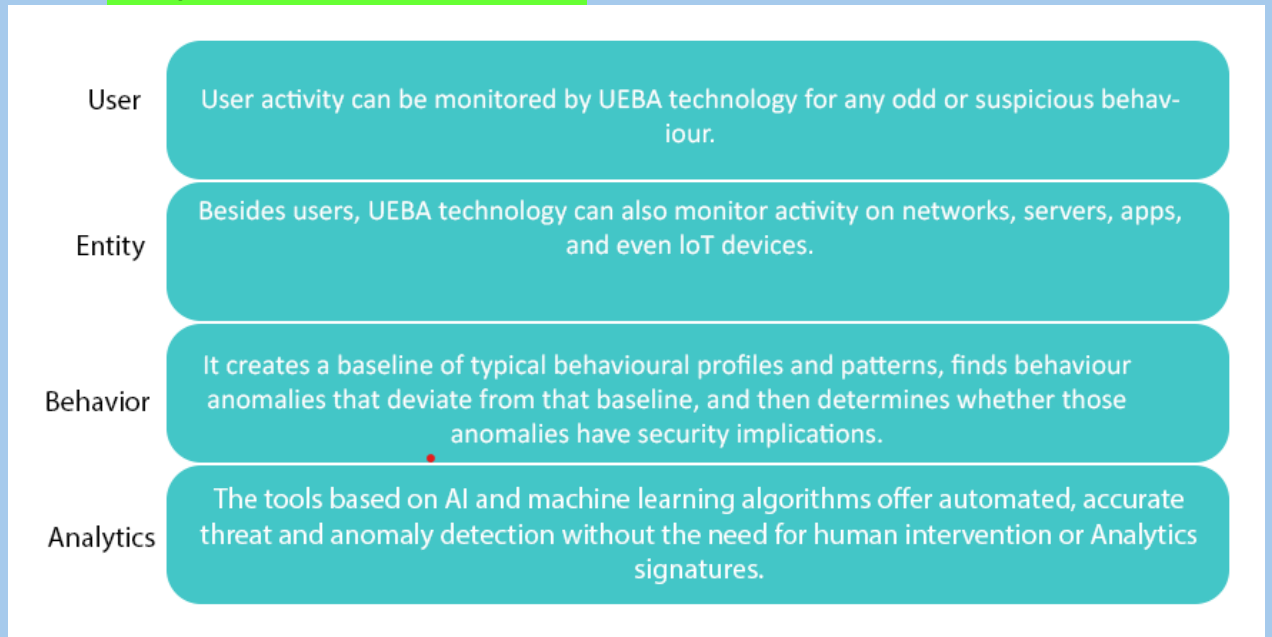
User & Entity Behavior Analysis (UEBA)

- See features helps to identify systems users based on their behavior
- Someone stolen username or password & login to the system
- UEBA identify the user because of different behavior
- User behavior -> how long user login -> which webSites user login -> which type of Data they are accessing
- Integrate UEBA with SIEM

Set baseline then we can find Threats and abnormalities

Provide automated identification of suspicious activities by user account

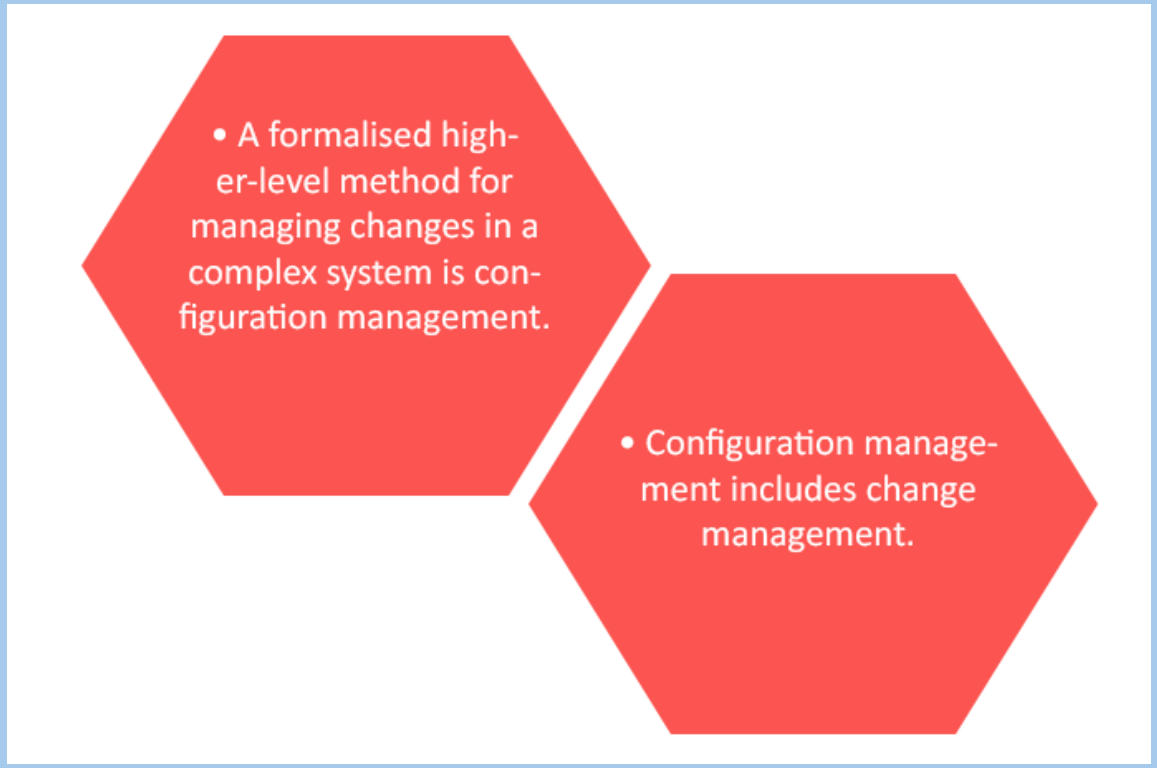
Dependent on AI & ML



Configuration Management

- All assets should be captured and documented
- When any configuration changes, it has to go through CHG Mgmt sys

Develop list of ports, services, accounts, applications etc



Provisioning

- When employee join organization, provisioning should be done to verify
  - User account
  - Assets

Provisioning
- Make new accounts
- Proper rights and privileges

Review
- Periodically verify accounts
- Deactivate inactive accounts
- Check regularly for excessive and creeping privileges.

Deprovisioning
- When employee leaves, immediately disable their account
- For temporary accounts, set account expiry date
- Delete expired account

Incident Management

- If there is Security issue – losses occurs
- Identify Incidents on timely manner and respond

Event

That can observe and reported

Incident

Event that negatively effect

System powered on

Criteria to find Incident types

Application started

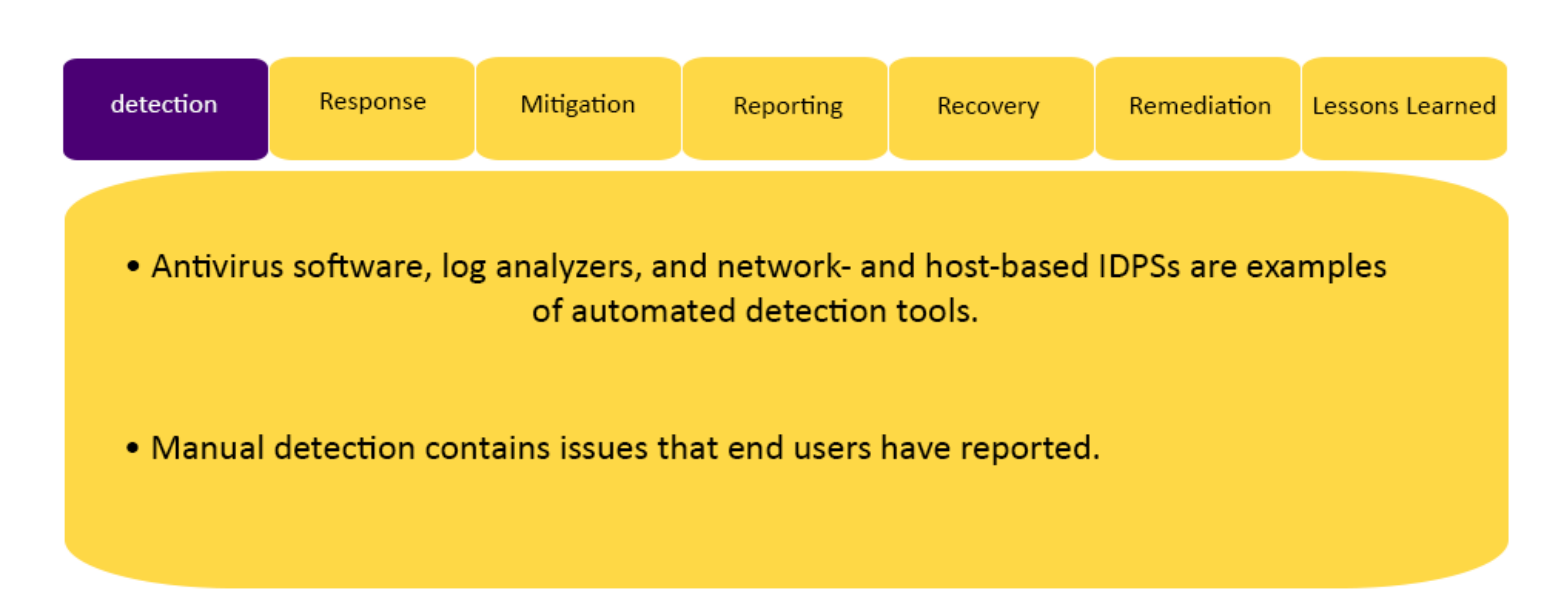
- **Planning and Preparation**
  - Create Incident Policy
  - Procedures
  - Response handling Methodologies
  - Communication Plan
  - Trainings
  - Incident Response Test & Drills
  - Collection of Threats & Vulnerability


Event
Every event that may be seen happening in a system or network
Incident
Any occurrence that harms the business and compromises its security stance
Incident response
A method of spotting a problem, figuring out what caused it, reducing the harm it causes, fixing the issue, and documenting each stage of the solution for future use.

Life Cycle of Incident Management

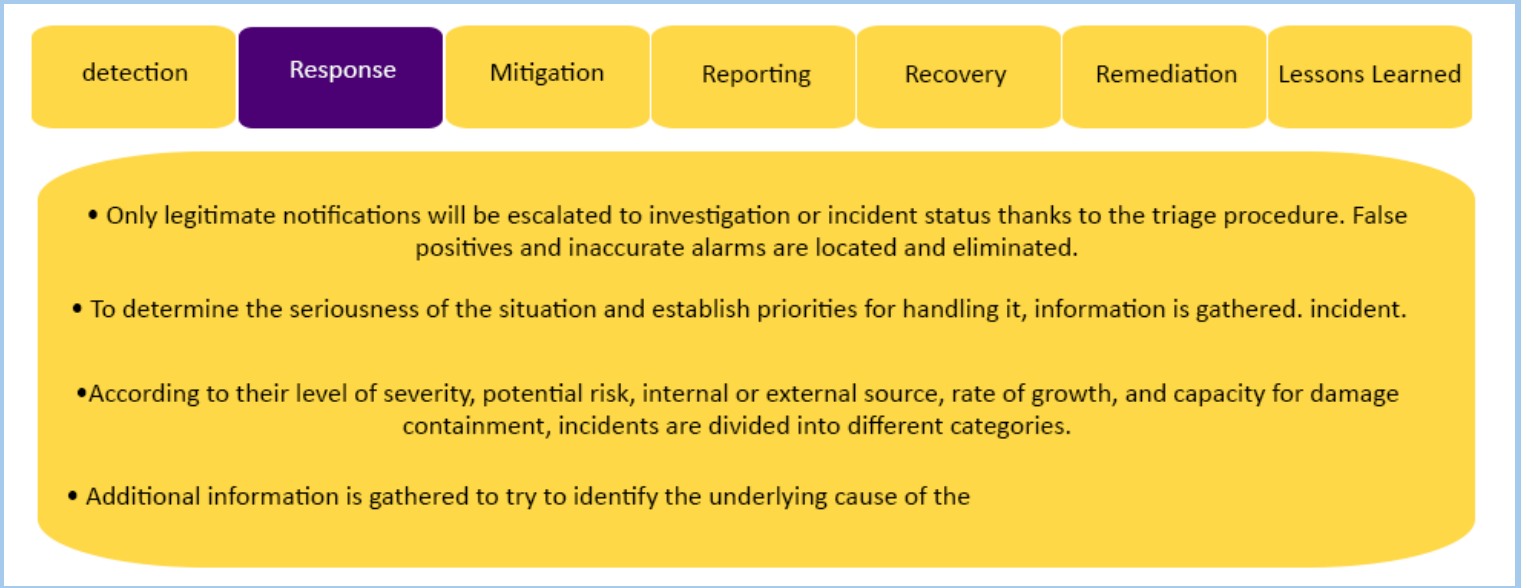
Detection

- Detect events using Tools - > network monitoring, logs, systems & apps monitoring
  - Tools and people working to see and report if any Incident occur



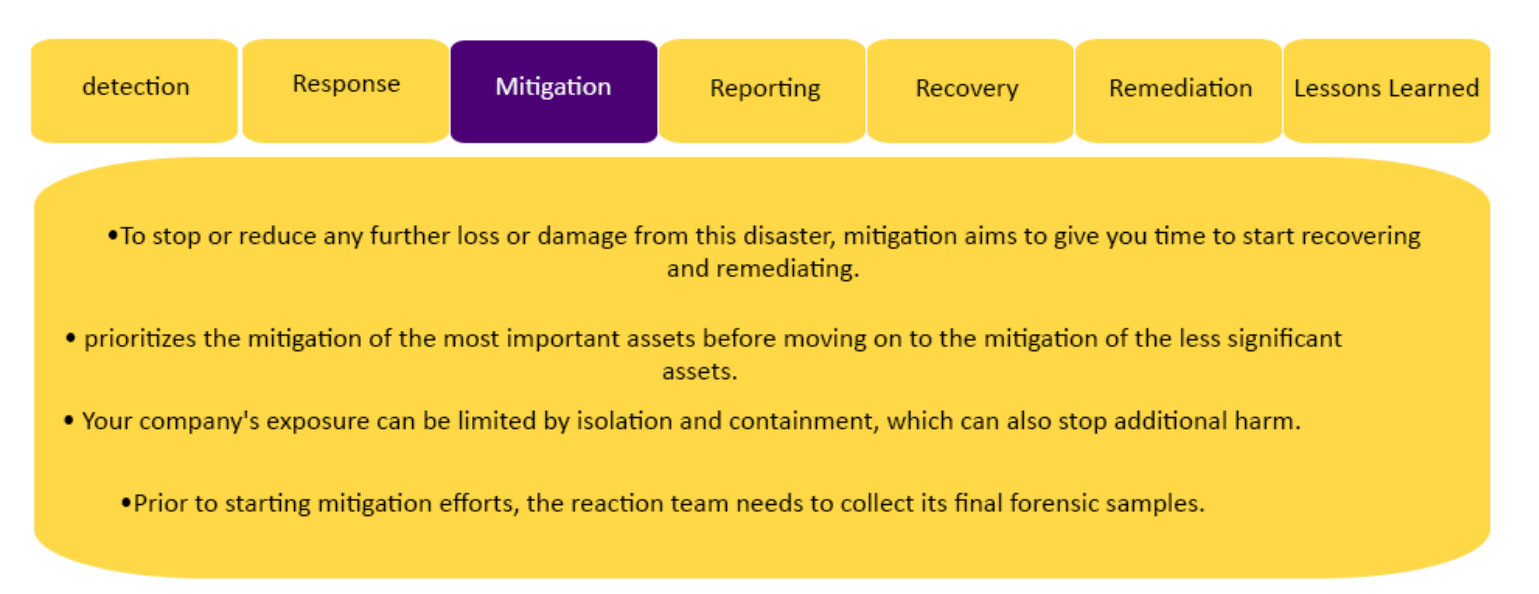
Response

Once alerts – Incident Team identify if there is any Incident or not
Preliminary verification and rating the Incident if any



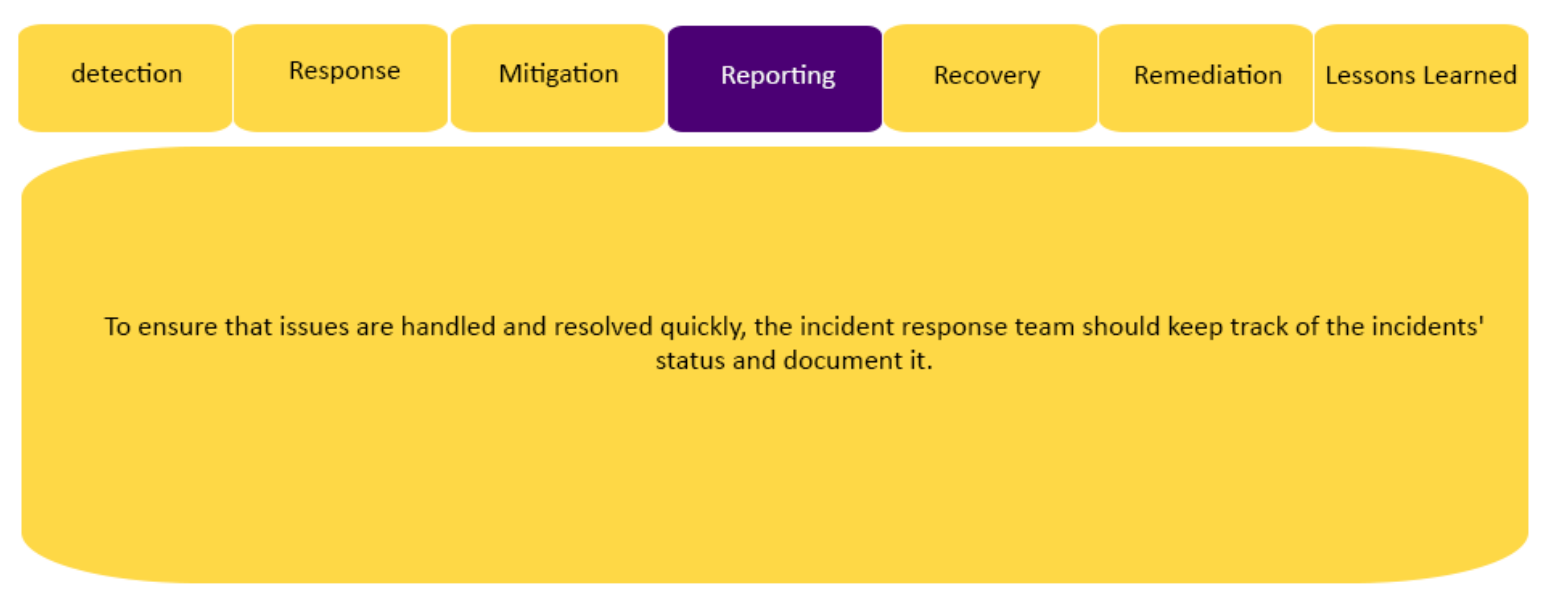
Mitigation

- Found Incident ‘Malware’
- Take immediate action
- If malware infected PC – disconnect from network



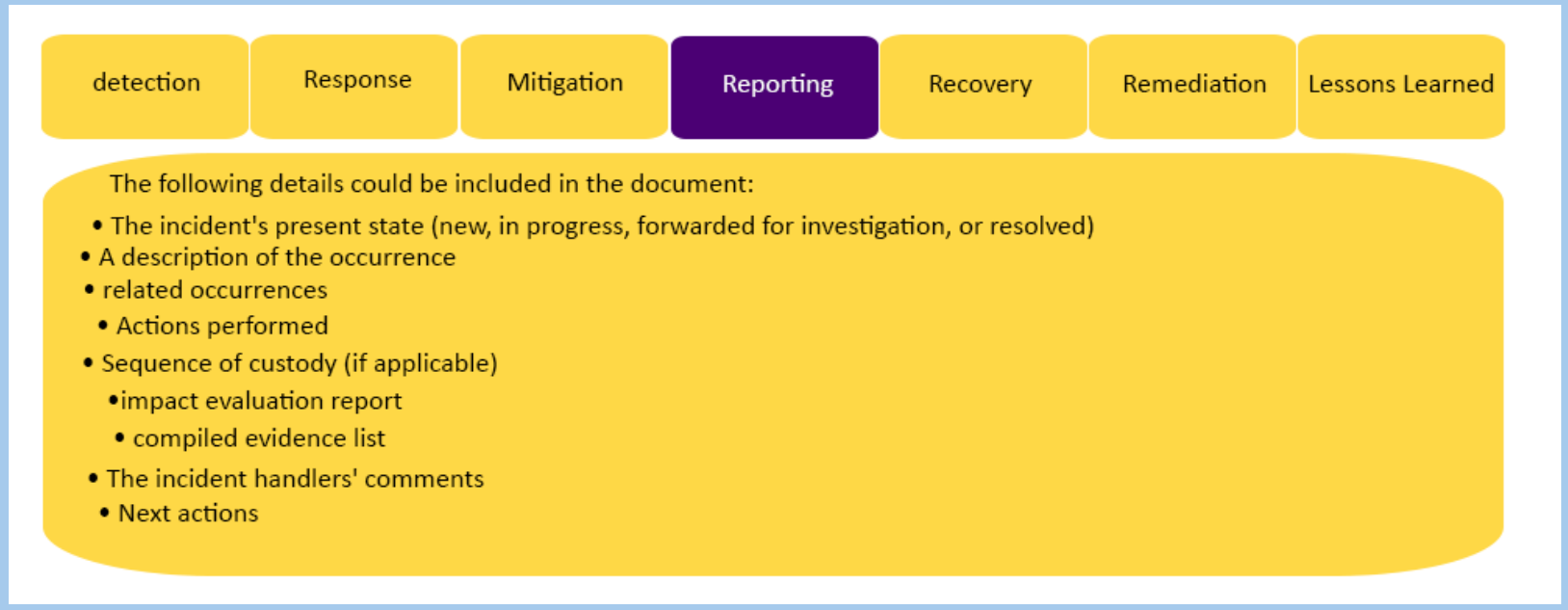
Reporting

Once mitigation done, then reported to Team
If Data breach – inform to customer or client



Recovery

- To solve Security Incidents
- Remove malware from PC
- Recover the Data
- Configuration change

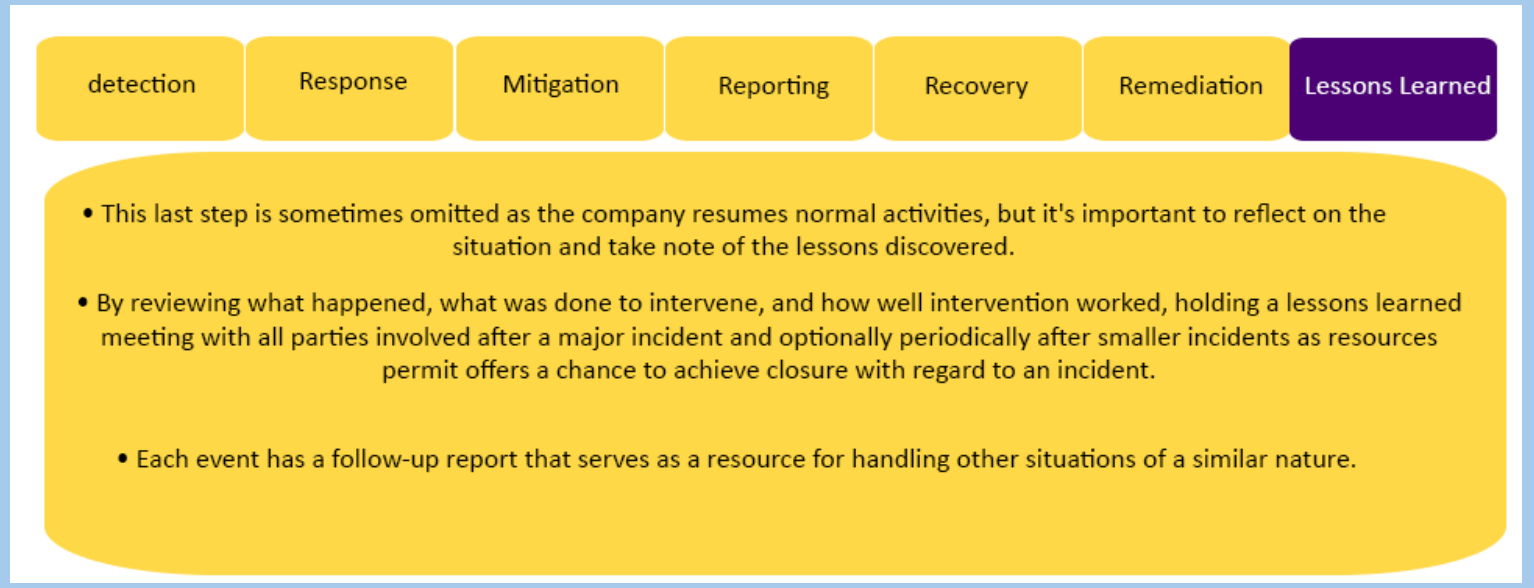


Remediation

To ensure this Incident not happen again
If any patch missing – it should install

Lesson Learned

Post Incident review
To improve Incident response



- **White Listing**
  - Nothing is allowed by default
  - The list mention what have to allow
  - This is good for Security

- **Black Listing**
  - Everything allowed by default
  - This is not good for Security

Patch Management

- Keep network secure, apply patches on regular basis

  - **Identify Patches**
    - Coordinate vendor to identify patches
  - **Rate the Patches**
    - Based on Security impact
  - **Test the Patches**
    - Once patch implemented - test and observe if cause any issue
  - **Rollout the Patches**
    - Install into the network
  - **Verify**
    - Whether patches install successfully

Patch monthly – apply patches on every month

OS patches, network, applications, IoT patches

Piece of software for problem fixing

- **Types of Patches**

  - **Hot fixes** = Small updates
  - **Service Pack** – all hot fixes and updates in a bundle

Data Backup Recovery Strategies

- **Full Backup**
  - Slow speed
  - Fast restoration

Backup everything that has changed from last backup

- **Incremental Backup**
  - Capture changes after last full or incremental backup

Backup everything since last full backup

- **Differential Backup**
  - Capture changes after last full backup

	Full backup	Differential backup	Incremental backup
Methodology	• It is the starting point for all other types of backups. • It contains all the data in the folders and files that are selected to be backed up. • A single full backup can provide the ability to completely restore all backed-up files.	• It contains all files that have changed since the last full backup, the latest full backup, and the latest differential backup is needed for a complete restoration.	• It stores all files that have changed since the last full, differential, or incremental backup. • When restoring from an incremental backup, the most recent full backup as well as every incremental backup made since the last full backup are needed.
Backup speed	Slow	Medium	Fast
Restoration speed	Fast	Medium	Slow
Storage space required	High	Medium	Low

Develop Recovery Strategies

- Responding to disaster
- Recover critical features
- Recover non-critical features
- Salvage and repair hardware & software
- Returning the primary Site for operations

- Move from backup Site to primary Site – DR over

- If any business down for 1 day – Disaster declared

The recovery procedure should concentrate on:

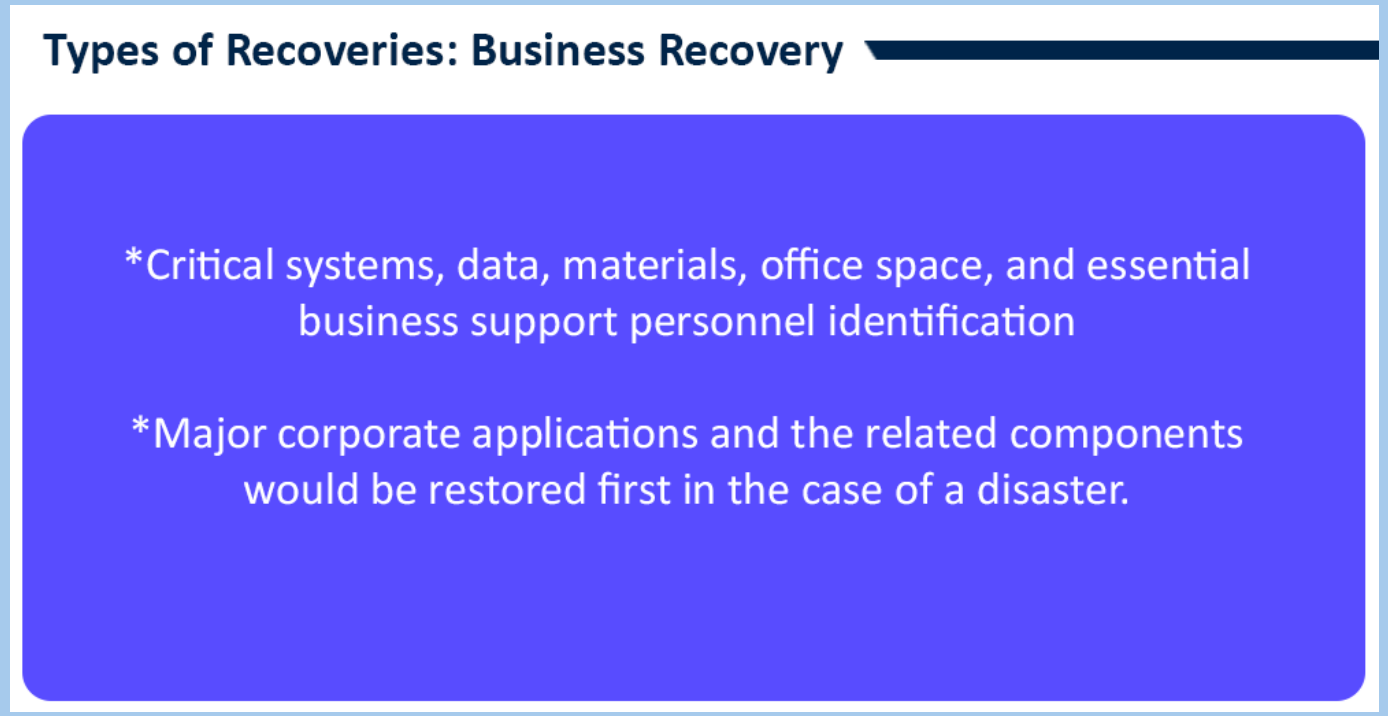
*Addressing the catastrophe
* Restoration of vital functions
* The restoration of non-critical tasks
* Salvage and software and hardware maintenance
* Going back to the main location for operations

Types of Recoveries

- Critical business assets
- Facility & supply recovery

- **User Recovery**
  - Team/resources

- **Operational Recovery**
  - IT/Technologies



Types of Recoveries: Operational Recovery

Operational recovery includes:

Recovery requires mainframes, systems, servers, LANs, peripherals, switches, routers, and other data communication equipment.

Deciding on alternate recovery sites in accordance with the MTD and acceptable expenses.

Types of Sites

- **Cold Site**
  - Utility – Yes
  - Networks – No
  - Data – No
- **Warm Site**
  - Utility – Yes
  - Networks – Yes
  - Data – No
- **Hot Site**
  - Utility – Yes
  - Networks – Yes
  - Data – Yes
- **Multi Processing Sites**
  - Rolling Site (Truck)
- **Reciprocal Site**
  - Agreement between two companies
- **Service Bureau**
  - 3rd provides DR services

Businesses can choose from the choices below for a secure location:

*mirror or duplicate site

*Hotsite

*Warm site

*Cold site

Reciprocal or mutual aid agreements, mobile sites, multiple processing centers, service bureaus, self-service, surviving sites, internal agreements, and working from home are additional location options.

HOT site

*After a major disruptions or catastrophe, an organisation would then relocate its data centre to a hot site.
*Servers, elevated floors, power, utilities, completely configured computers, hardware, and real-time mirroring of data for crucial applications make up this system.
*It enables the quick restart of crucial operations.

Warm site

*Warm site has connectivity and hardware but not real-time data.
*In order to restore a system after an interruption, it depends on backup data.
*Raised floors, electricity, utilities, computer peripherals, and completely functional computers are all included.
*It costs less, is more adaptable, and needs fewer resources to maintain.
*The site's activation takes more effort and time.

Cold site

*A cold site lacks technology that is easily available and has data back-ups.
*It takes longer to configure cold sites and restore crucial IT functions. In addition to electricity, utilities, and physical security, it has a raised floor.
*It is not constrained by resources or location.

Mobile site

*The term mobile sites can also refer to mobile data centres.
*It has HVAC, fire suppression, and physical security equipment, as well as towable trailers that contain computer equipment.
*It prevents harm to the data centre while maintaining the facility.

Fault Tolerance

Redundancy

- If one hard drive fails, second is available

- **RAID 0**
  - No redundancy – if one h/d fails – cant recover the Data

    Stripping with no mirroring – no fault tolerance

    Minimum 2 disks

    Faster read/write speed

- **RAID 1**
  - 2 h/d – if one h/d fails – can store Data from second one
  - Write simultaneously on both disks
  - ta

Fault Tolerance

RAID 5

Used in servers

Minimum 3 disks

RAID 6/10

If 2 h/d fails – can recover the Data

If 3 h/d fails – cant recover the Data

Clustering

- Cluster – Server 1 & Server 2
- If 100 request forward to 1 server, they divide 50/50 to each server
- If one server fails other can process

Two or more servers working together to perform

- **Active-Active Mode**
  - Both servers active same time
  - 100 request – split 50/50
- **Active-Passive Mode**
  - 1 server running all request

*A cluster is a collection of two or more computers that work together as one logical server.
*In general, clusters run in one of the following modes:
1. Active-active mode
*Both servers are running and responding to inbound requests.

Data backup & Recovery Strategies

- **Shadowing**
  - Mirroring simultaneously

  Exact copy of Database on another location

- **Electronic Vaulting**
  - Periodically store Data on remote Site

  Data backup on certain intervals

- **Remote Journaling**
  - Data store when any change occurs

  Data store once any change occurs

BCP/DR strategy

1. Scope
2. Business Impact Analysis
3. Recovery Strategy
4. Develop plan
5. Testing and Training
6. Maintenance

BCP Teams structure

Rescue Team

Activation

Notification

Recovery Team

Bring facility back to normal

Salvage Team

Work on primary Site to back on operation

Testing of BCP/DR

- **Review**
  - Each Team review the docs
  - Initial review
- **Checklist**
  - Detailed doc review
- **Structured Walkthrough**
  - Entire BCP Team attend the meeting
- **Simulation Test**
  - Do everything related to BCP – Don’t move on backup Site
- **Partial & Complete Business Interruption Test**
  - Test everything and move on backup Site
  - Business interrupted
- **Parallel Processing**
  - Primary Site can move to anytime on backup Site without business interruption

Key Factors to consider in Disaster Recovery

RPO – Recovery Point Objective (3hr)

- Data backup frequency
- If system down for 3 hours -> no issue
- Every 3 hours -> we have to take Data backup

Acceptable amount of Data that cannot be recovered

If we take backup every 3 hours, we have to accept up to 3 hours Data loss

RTO – Recovery Time Objective (2hr)

- Time to recover system
- If server down -> it should be recover in 2 hours

Hardware recovery

Must be less than or equal to MTD

WRT – Work Recovery Time (2hr)

MTD-RTO = WRT

Once servers issue fixed -> start Data backup

Software restored

MTD – Maximum Tolerable Down Time

MTD = RTO + WRT

MTBF – Mean Time Between Failure

How often we can expect hardware fail

MTTR – Mean Time To Repair

How long will take to recover the failed system