Καλημέρα και καλή Χρονιά!
Σήμερα επειδή θα συνδεθεί και το αμφιθέατρο στην Λαμία, θα ξεκινήσουμε στις 11:30.

Security Incident Handling

From Containment to Recovery

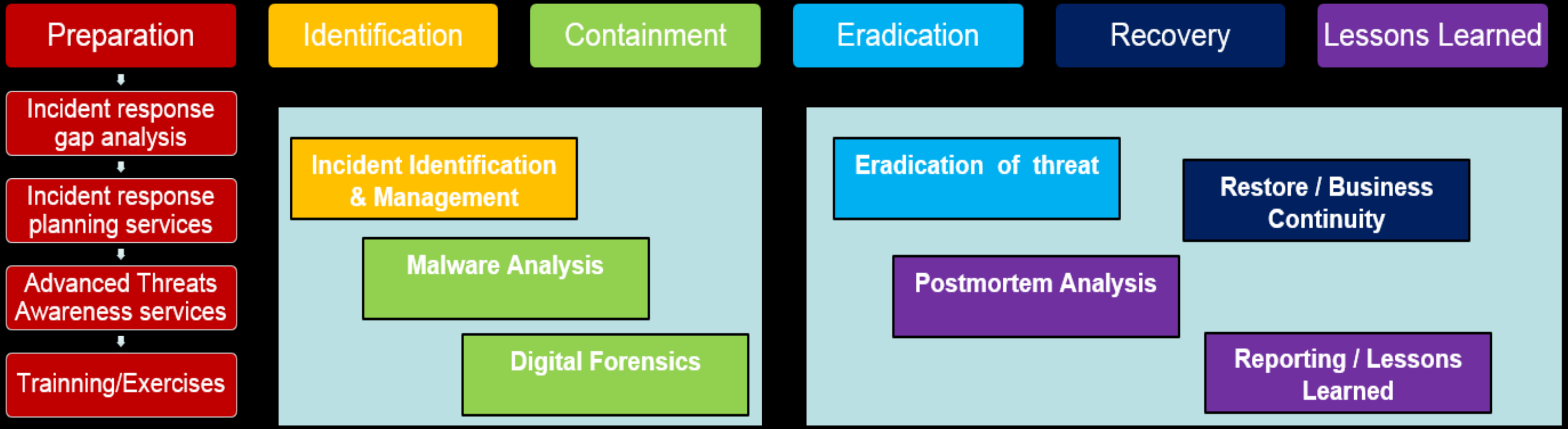
TOC

- 5. The Six Phase Approach
- 6. Basic Forensic Procedure
- 7. Useful Resources

5. Six Phase Approach

- **Incident Management Strategy**
  - **1. Preparation**
  - **2. Identification**
  - **3. Containment**
  - **4. Eradication**
  - **5. Recovery**
  - **6. Lessons learned**

5. Six Phase Approach



Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Incident response gap analysis

Incident response planning services

Advanced Threats Awareness services

Trainning/Exercises

Incident Identification & Management

Malware Analysis

Digital Forensics

Eradication of threat

Restore / Business Continuity

Postmortem Analysis

Reporting / Lessons Learned

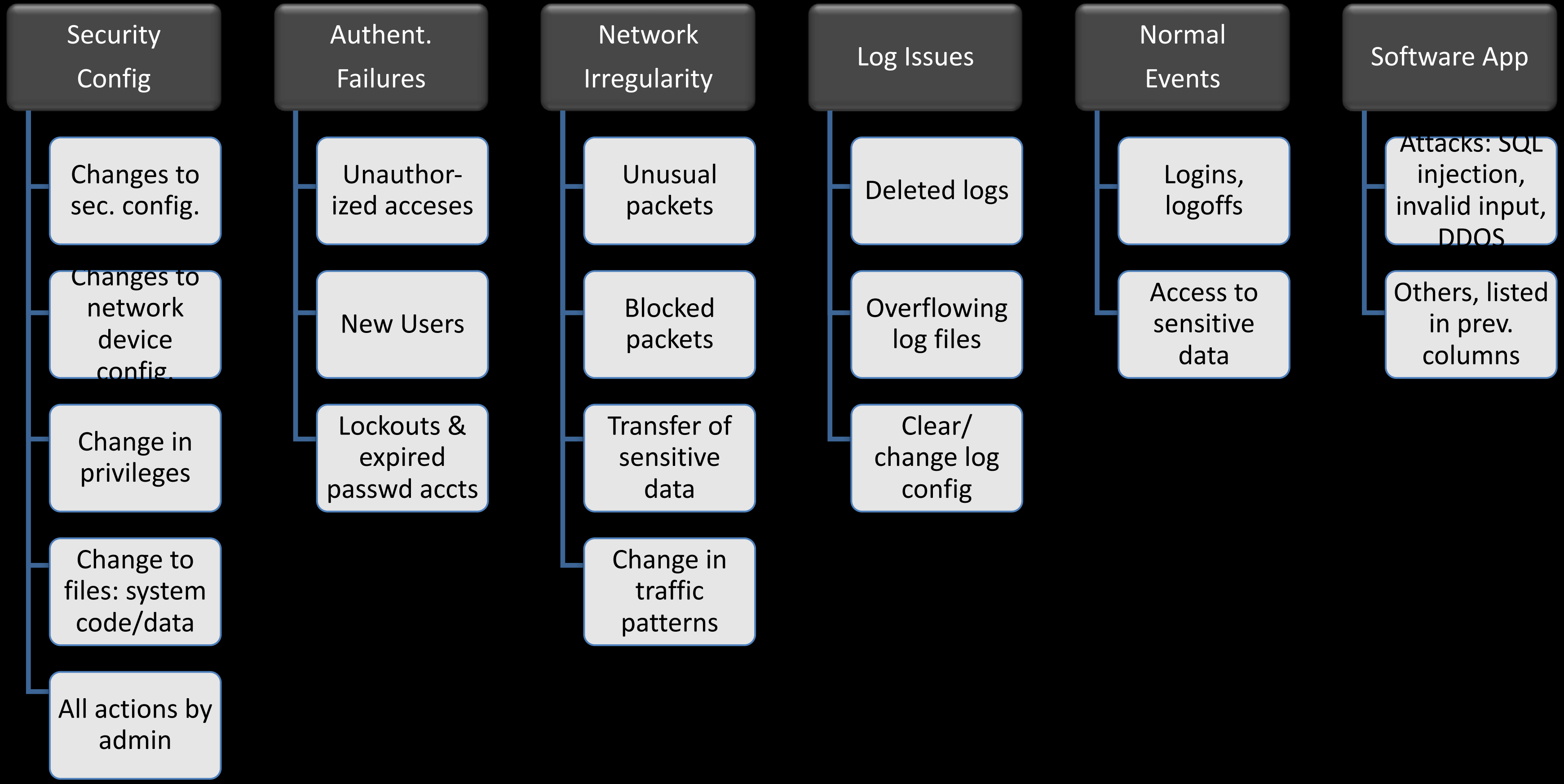
Incident identification tools

- Why is incident response important?
    - $201: average cost per breached record
    - 66% of incidents took > 1 month to years to discover
    - 82% of incidents detected by outsiders
    - 78% of initial intrusions rated as low difficulty

Detection Technologies

- Organization must have sufficient detection & monitoring capabilities to detect incidents in a timely manner. Two main ways to react:
- Proactive Detection includes:
    - Network Intrusion Detection/Prevention System (NIDS/NIPS)
    - Host Intrusion Detection/Prevention System (HIDS/HIPS)
    - Antivirus, Endpoint Security Suite
    - Security Information and Event Management (Logs)
    - Vulnerability/audit testing
    - System Baselines, Sniffer
    - Centralized Incident Management System
        - Input: Server, system logs
        - Coordinates & co-relates logs from many systems
    - Tracks status of incidents to closure
- Reactive Detection: Reports of unusual or suspicious activity

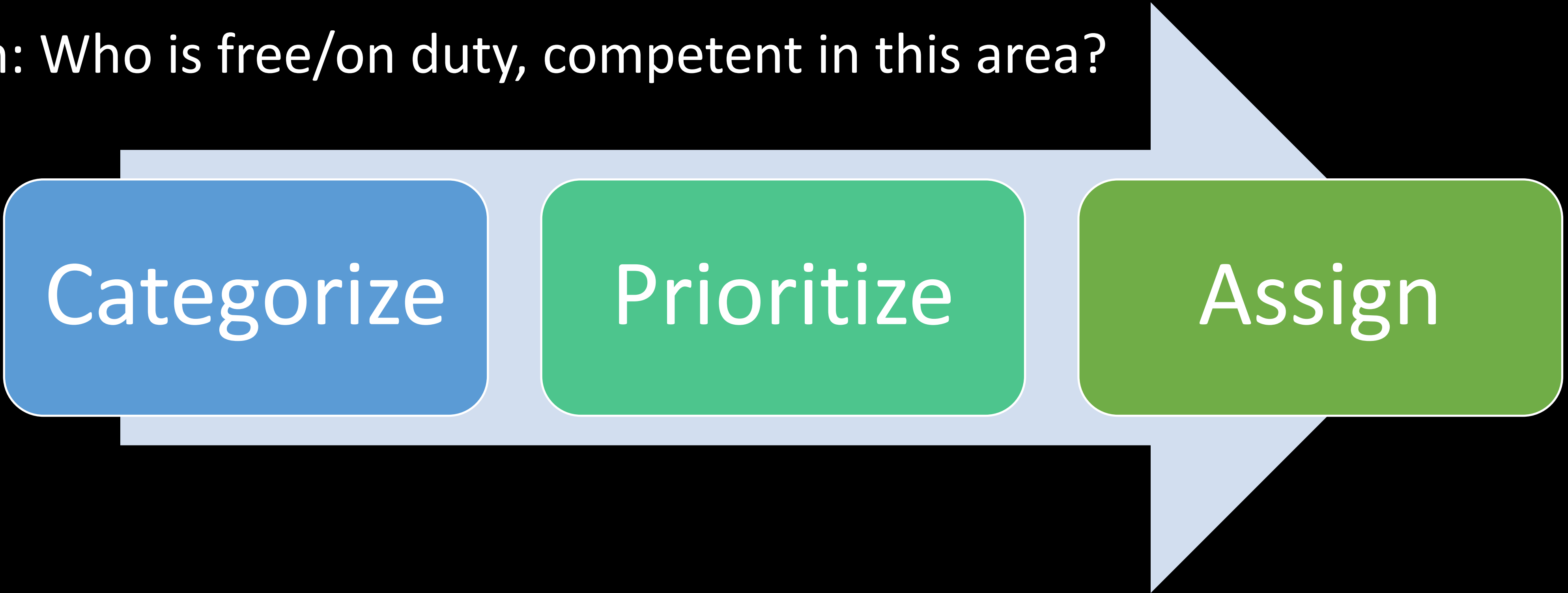
Logs to Collect & Monitor



- Security Config
  - Changes to sec. config.
  - Changes to network device config.
  - Change in privileges
  - Change to files: system code/data
  - All actions by admin
- Authent. Failures
  - Unauthorized acceses
  - New Users
  - Lockouts & expired passwd accts
- Network Irregularity
  - Unusual packets
  - Blocked packets
  - Transfer of sensitive data
  - Change in traffic patterns
- Log Issues
  - Deleted logs
  - Overflowing log files
  - Clear/ change log config
- Normal Events
  - Logins, logoffs
  - Access to sensitive data
- Software App
  - Attacks: SQL injection, invalid input, DDOS
  - Others, listed in prev. columns

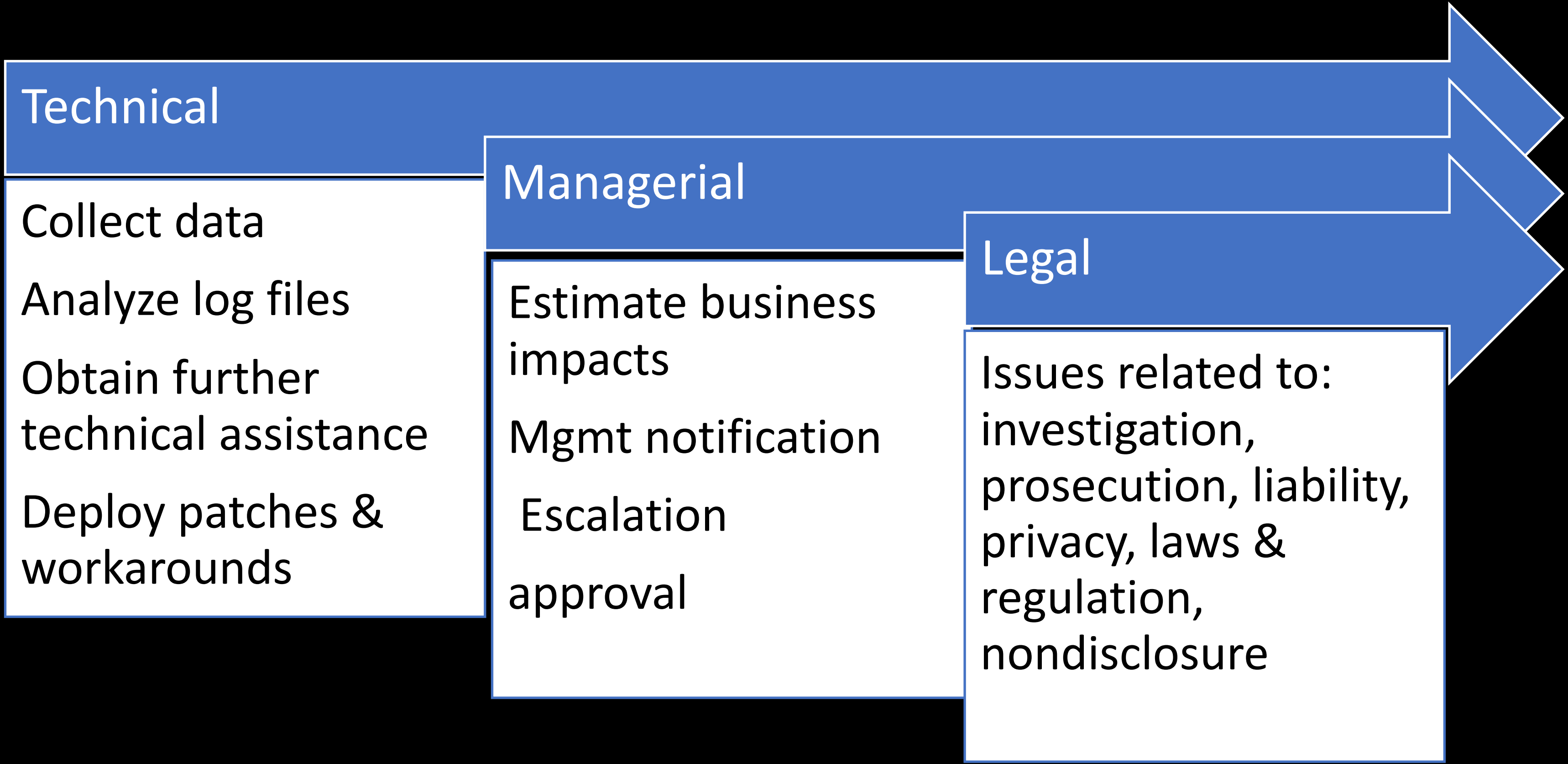
The identification Triage

- Snapshot of the known status of all reported incident activity
  - Sort, Categorize, Correlate, Prioritize & Assign
- Categorize: DoS, Malicious code, Unauthorized access, Inappropriate usage, Multiple components
- Prioritize: Limited resources requires prioritizing response to minimize impact
- Assign: Who is free/on duty, competent in this area?



Containment

- The Goal is to stop the bleeding.
  - Stop the attacker to get any deeper.
- We will cover the following:
  - The Sub-phases of containment.
  - Methods of short-term containment
  - Backup
  - Method of long term containment.



Technical

Collect data

Analyze log files

Obtain further technical assistance

Deploy patches & workarounds

Managerial

Estimate business impacts

Mgmt notification

Escalation

approval

Legal

Issues related to: investigation, prosecution, liability, privacy, laws & regulation, nondisclosure

Short-term Containment

- Secure the equipment / computer if possible.
  - Stop all personnel other than the incident handlers from touching, accessing, and possibly making things worse on the affected system.
  - Secure doesn't mean 'patch holes' or make configuration changes at this point!

Remember this is your crime scene!

Short-term Containment

- “**Abort, Retry, Ignore, Fail**?”
  - Determine risk of continuing operations
  - “Plugged-in or Unplug?”
  - Consult system owners
- Beware of:
  - Booby traps
  - Compromised system binaries
  - “Homing device” that alerts intruder
  - Temptation to locate alleged source

Initial analysis

- Keep low profile
- Analyze the copy of the forensic image:
  - Make an image ASAP
  - Use Blank Media
  - If possible take bit-by-bit image
  - Never analyze the original.
  - Keep original intact for evidence.

Isolate the system

- First thing you isolate , then image.
  - Use CD do not use USB.
  - Do not grace shutdown the system.
  - Store the image in safe place.
    - Original (Evidence)
    - Image1 (May be put back into production)
    - Image2 (Analysis)
    - Use drive duplicators if possible
    - Train on the image creation.

- Change all passphrases
  - Try not to cause panic or rumors.
  - If a real-time password interceptor is at large, change passphrases at a trusted, dedicated machine(s).
- Review logs from neighboring systems.
- Report to Command Decision Team.
- Apprise affected parties of progress.

Continuing Operation

- Acquire the logs and other sources of information.
- Review logs from neighboring systems.
- How far did the attacker get.

- Make recommendation for log term containment.
  - It is a business decision

Long-Term Containment

- As long as you got your evidence and image backup , you can make changes to the system.
- Ideal: keep system off line.
- Less than ideal :if system must be kept in production , perform long term Containment.

Long Term containment

- Numerous potential actions:
  - Patching the system and neighboring systems.
  - Change password
  - Null routing ???
  - FW
  - Remove accounts used by attackers.
- Do not forget (you still need to eradicate)
- The ideal long-term containment is to apply temporary solution till you build a clean system.

Six Phase Approach: Eradication

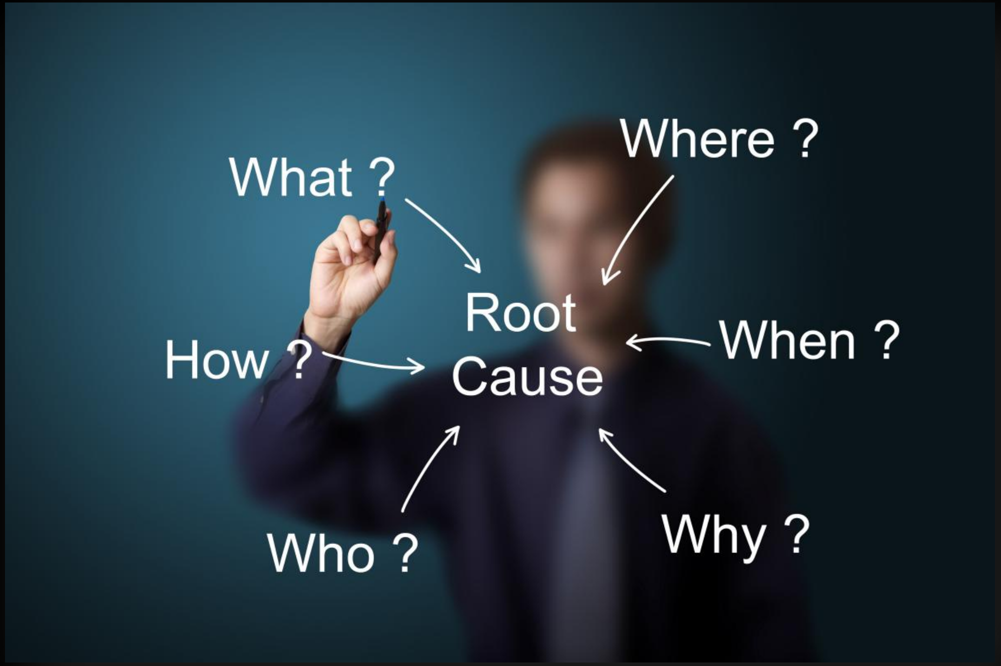
- Objectives / Activities
  - Determine cause and symptoms of incident
  - Analyze threat and vulnerability
  - Raise defense
  - Remove cause of incident
  - Report actions to Command Decision Team, IT support staff, and Help Desk.

Six Phase Approach: Eradication

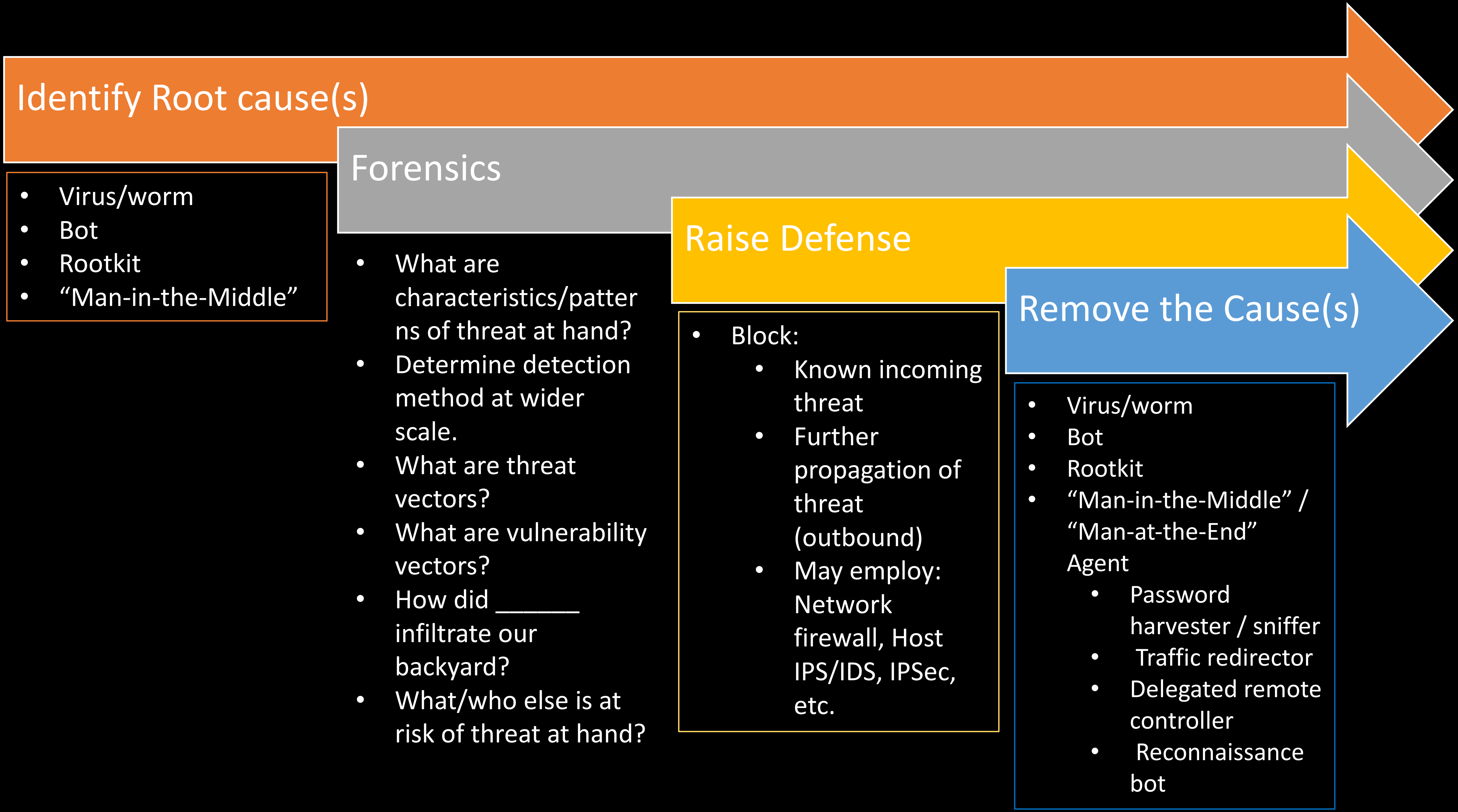
- First Step: Analysis
- Determine how the attack occurred: who, when, how, and why?
    - What is impact & threat? What damage occurred?
- Remove root cause: initial vulnerability(s)
    - Rebuild System
    - Talk to ISP to get more information
    - Perform vulnerability analysis
    - Improve defenses with enhanced protection techniques
- Discuss recovery with management, who must make decisions on handling affecting other areas of business

Six Phase Approach: Eradication

- First Step: Analysis
  - What happened?
  - Who was involved?
  - What was the reason for the attack?
  - Where did attack originate from?
  - When did the initial attack occur?
  - How did it happen?
  - What vulnerability enabled the attack?



Eradication Process



Identify Root cause(s)

- Virus/worm
- Bot
- Rootkit
- “Man-in-the-Middle”

Forensics

- What are characteristics/patterns of threat at hand?
- Determine detection method at wider scale.
- What are threat vectors?
- What are vulnerability vectors?
- How did _______ infiltrate our backyard?
- What/who else is at risk of threat at hand?

Raise Defense

- Block:
  - Known incoming threat
  - Further propagation of threat (outbound)
  - May employ: Network firewall, Host IPS/IDS, IPSec, etc.

Remove the Cause(s)

- Virus/worm
- Bot
- Rootkit
- “Man-in-the-Middle” / “Man-at-the-End” Agent
  - Password harvester / sniffer
  - Traffic redirector
  - Delegated remote controller
  - Reconnaissance bot

Six Phase Approach: Eradication

- Remove root cause
  - If Admin or Root compromised, rebuild system
  - Implement recent patches & recent antivirus
  - Fortify defenses with enhanced security controls
  - Change all passwords
  - Retest with vulnerability analysis tools

Critical!!!

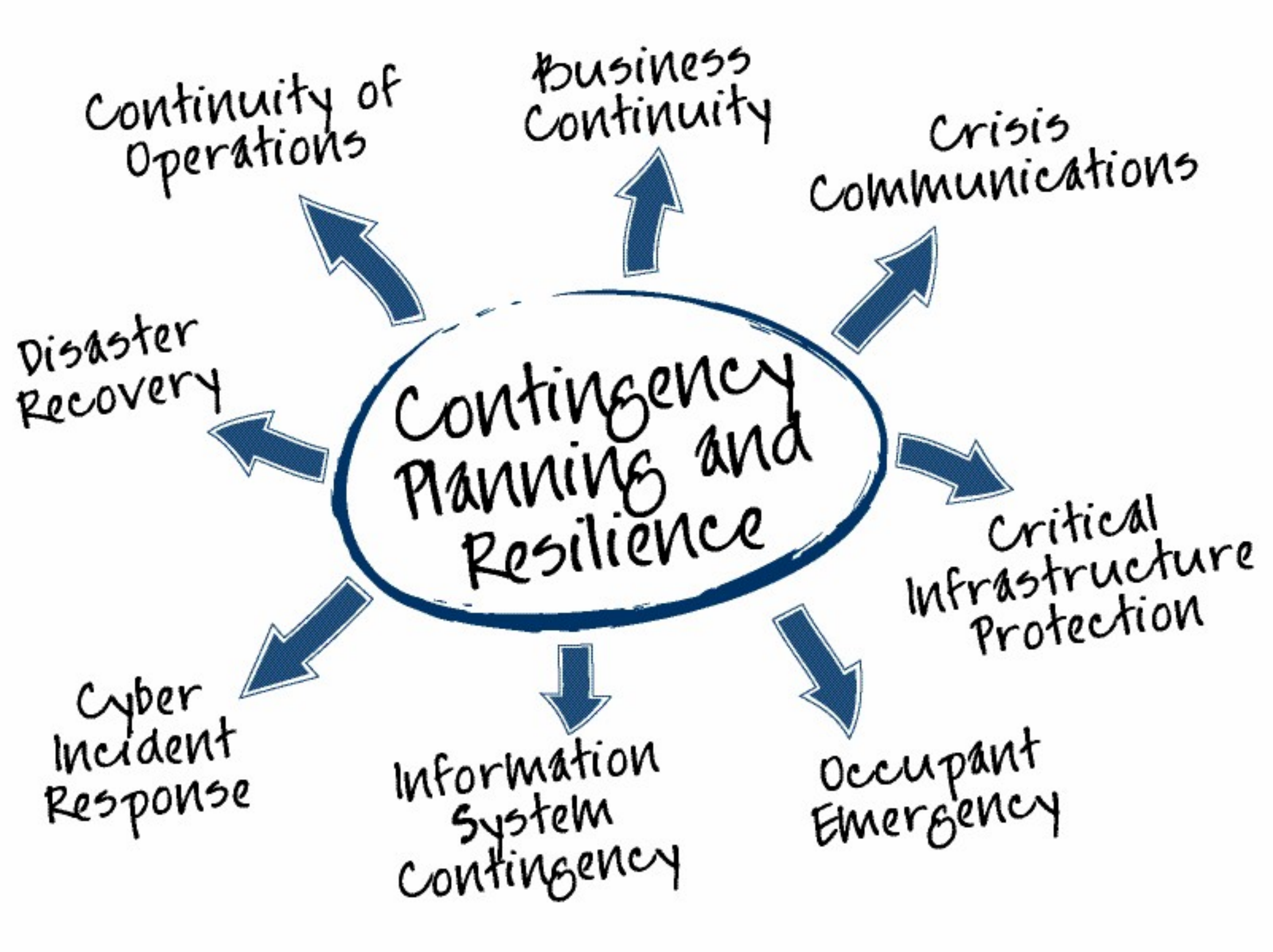
- Try not to let the intruder discover your corrective actions.

Six Phase Approach: Recovery

- **Objectives / Activities**
  - • Restore normal service.
  - • Verify:
    - performed operation
    - service/system quality
  - Report actions to Command Decision Team, IT support staff, and Help Desk.

Six Phase Approach: Recovery

- **Objectives / Activities**
  - To be carried out by system owners.
    - Usually beyond the scope of IRT's responsibility
  - Continue to monitor known malicious/abnormal behavior and backdoor(s).

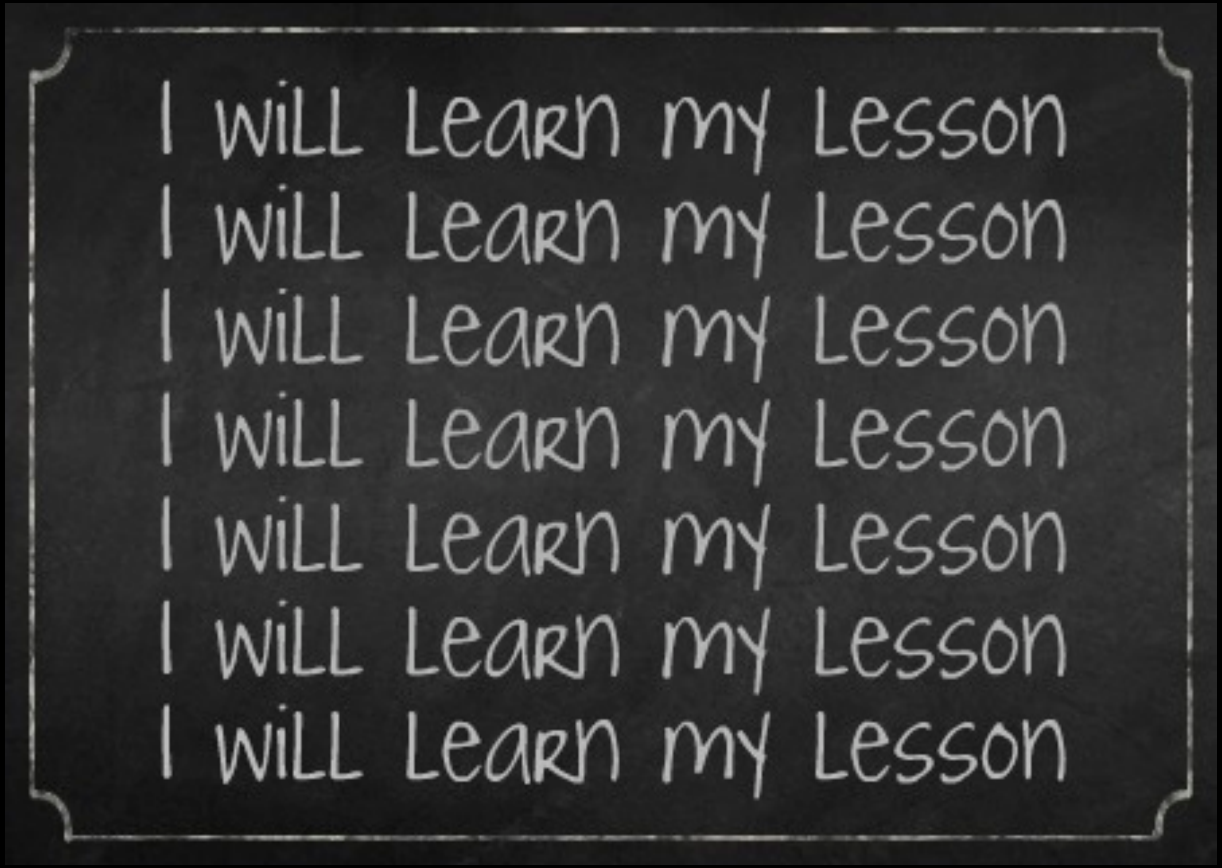


Six Phase Approach: Recovery

- **Objectives / Activities**
  - To be carried out by system owners.
    - Usually beyond the scope of IRT's responsibility
  - Continue to monitor known malicious/abnormal behavior and backdoor(s).
- Avoid worsening the impact with faulty, unexercised recovery process.

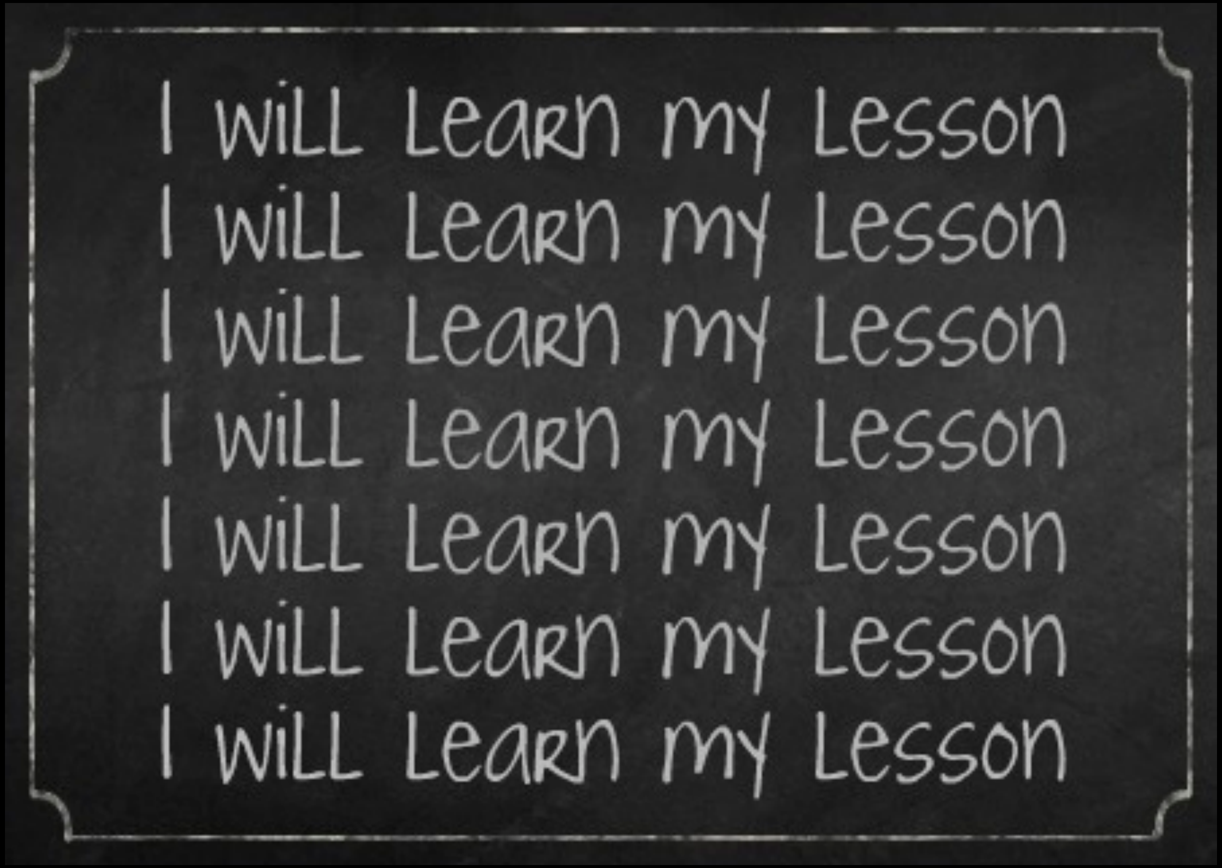
Six Phase Approach: Follow - Up

- **Objectives**
  - Search for lessons learned.
  - Improve incident handling capability.



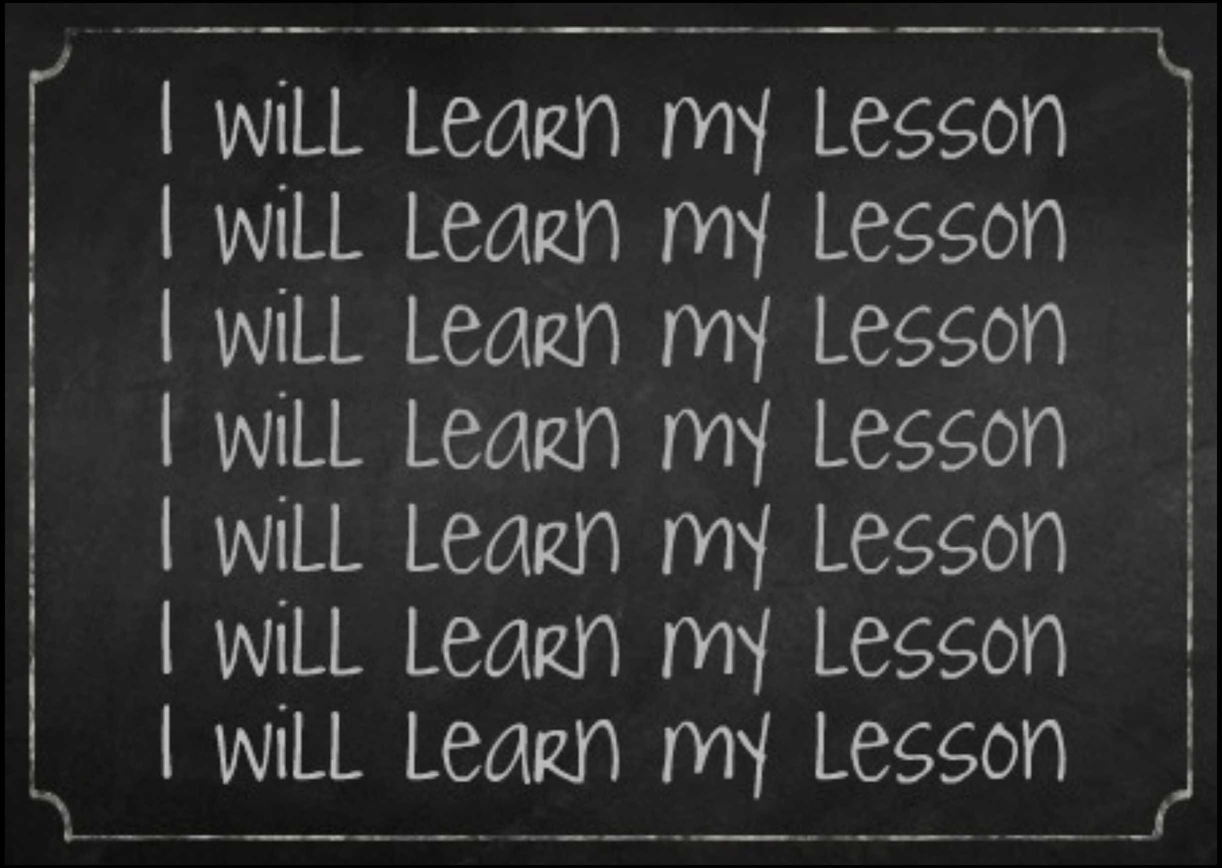
Six Phase Approach: Follow - Up

- **Activities**
  - Take a short break! But don't delay.
  - Review incident log(s).
    - Compare to initial IR plans and procedures
  - Draft 'lessons learned' in writing.
    - IRT subteams contribute.
  - Have a Lessons Learned meeting.



Six Phase Approach: Follow - Up

- **Activities**
  - Write an executive summary.
  - Submit recommended changes to senior management
    - Estimate of cost incurred
    - Impacts of implementing recommended changes vs. not
  - Implement approved actions.



Next : Introduction to Forensics /Malware analysis