Incident Reporting and Response

What Incidents Should Be Reported?

- Any suspicious activity should be reported
  - This includes suspicious user account behavior, computer system failures or misbehavior, accidental publication of internal email, loss of equipment / account information, etc.
- Reporting methods
  - Internal
    - Online support ticketing system
    - Technical support email
  - External
    - Abuse / incident email contact
    - Public web-based contact form
    - Telephone number specifically for reporting abuse

Information for Reporting An Incident

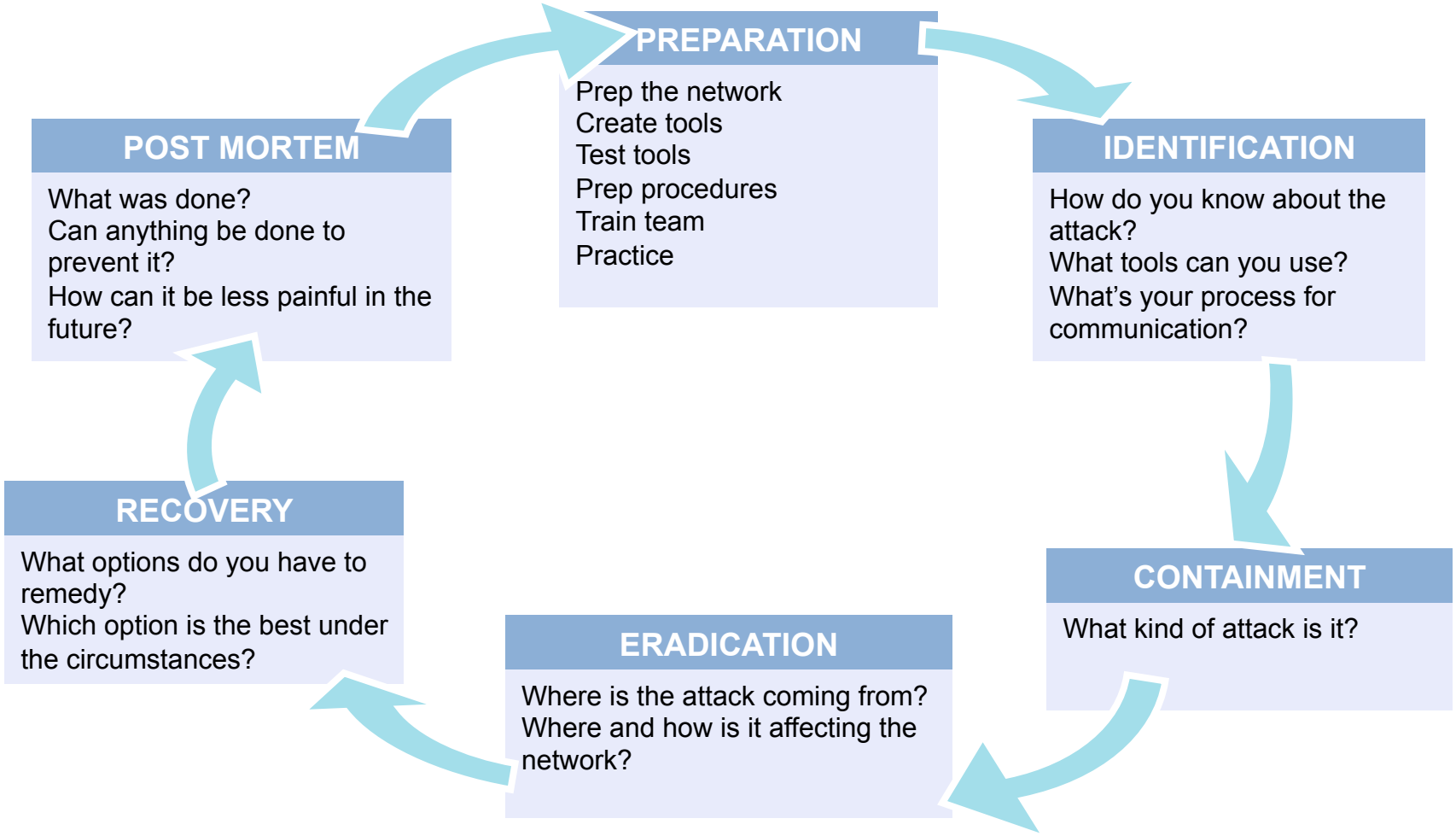
- Date and time of the event
- Description of the event
- Assets that are affected or at risk as a result of the event
- Whether the event is in progress or has concluded
- Actions taken by the party reporting the event
- Informal assessment of the harm or impact to the asset
- Informal assessment of collaterally affected assets
- Data (logs, files, reports) that may assist the CIRT in analyzing the event

Incident Response

- It is always best to have a plan in place before something bad happens
- DO NOT PANIC!
- If you set appropriate guidelines now, it will make things a lot easier when a security incident happens

Create a checklist that can be followed when a significant security incident does occur!!

Six Phases of Incident Response



Preparation

- Includes technical and non-technical elements
- Know the enemy
  - Understand what drives the miscreants
  - Understand their techniques
- Create the security team and plan
  - Who handles security during an event? Is it the security folks? The networking folks?
- Harden the devices
- Prepare the tools

Preparation – Key Elements

- Policy
- Response Plan or Strategy
- Communication
- Documentation
- Team
- Access Control
- Tools
- Training

Identification

- Goal is to gather events, analyze them and determine whether you have an incident
- Assign Incident Handlers
  - Select a person to handle identification and assessment
  - Empower them to escalate if needed
- Control the Flow of Information
  - Enforce “need to know” policy
  - Tell details to minimum number of people possible
- Create Trusted Communication Channels

Identification

- Understand the details and scope of the attack
  - Identification is not sufficient; once an attack is identified, details matter
  - Guides subsequent actions
- Qualify and quantify the attack without jeopardizing services availability (e.g., crashing a router):
  - What type of attack has been identified?
  - What's the effect of the attack on the victim(s)?
  - What next steps are required (if any)?
- At the very least:
  - Source and destination address
  - Protocol information
  - Port information

How Do You Know You Are Under Attack?

Containment

- Stopping the Damage
  - Prevent attacker from getting any deeper into the impacted systems, or spreading to other systems
- Inform Management
- Notify your local or organizational incident handling team
- Additional 3 phases
  - Short term containment
  - Gathering evidence / backup
  - Long term containment

Short Term Containment

- Try to prevent attacker from causing more damage
- Want untainted evidence
- Some possible actions:
  - Disconnect network cable
  - Pull the power cable (loses volatile memory and may damage drive)
  - Isolate switch port so that system can no longer send/ receive data
  - Apply filters to routers and/or firewalls
  - Change a target's name in DNS to point to a different IP address

Image Creation

- This is never easy under pressure
- Hint: Play with these tools and make sure you know how to use them before an incident happens
  - dd for Unix/Linux and Windows
  - Ghost (the latest versions – default is not bit-by-bit so know how to configure)
  - Drive duplicator hardware and write blockers

Long Term Containment

- Once back-up created for forensics analysis the changes for long term containment can begin
- Apply temporary solution(s) to stay in production while building a clean system
  - Patch system
  - Change passwords
  - Remove accounts used by hacker
  - Change file permissions
  - Shutdown backdoor processes used by attacker

Eradication

- Goal is to get rid of any traces on network device(s) that an attack occurred
- Determine how the attack was executed from the gathered evidence
- Restore operating systems and configurations from clean backups
- May require starting from completely wiped systems
- Improve defenses

Recovery

- Goal is to get impacted systems back into production in a safe manner
- Perform system validations
  - Run vulnerability scanners
  - Carefully check application and device logs
- Use network and host-based intrusion detection systems to monitor reoccurrence of attack
- Apply any newly identified mitigation techniques

Post Mortem

- A post mortem will help analyze the event after normal operations has resumed (and people have caught up on sleep)
- Have the meeting soon after the incident passed so everyone has details fresh in their minds
- Do NOT blame anyone for doing something incorrectly
- The primary goal is to address lessons learned and not make the same mistakes next time
- What can you do to make recovery faster, easier, less painful in the future?

Do You Have A CIRT?

- You should have a Computer Incident Response Team established
- Who is part of this?
- What are their responsibilities?
- Important – define a single individual to be in charge of final decisions (also have a backup for this individual)
- Know who you need to contact
  - Legal / regulatory responsibility
  - Upstream ISPs who may help filter on DDoS attacks
  - Impacted individuals