# Incident Response Service

Analysing different attack scenarios and solve them either by patching the environment, or eradicating the threat according to known fixes or self-developed patches, during runtime.

One Pager

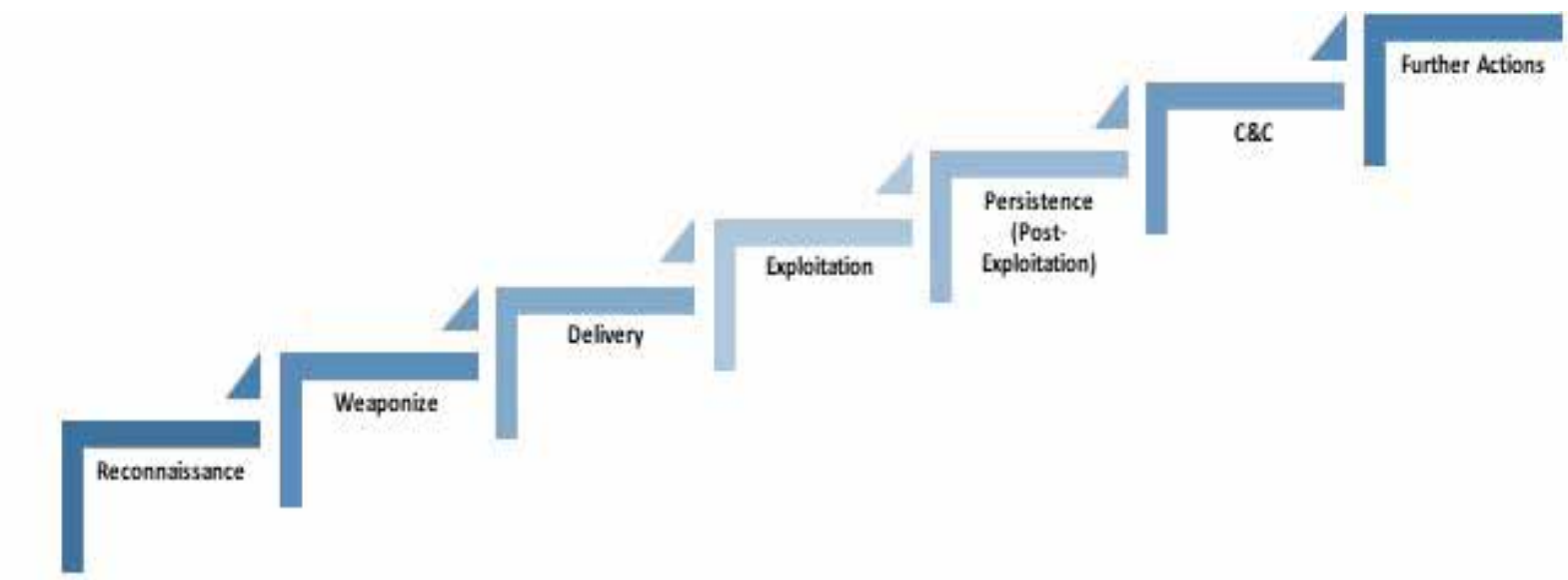
# Incident Response Service

## What is Comsec's Incident response ?

Comsec's Incident response team is combined from experts with vast experience in many fields such as application security, infrastructure security and digital forensics. The team is capable of analysing different attack scenarios and solve them either by patching the environment, or eradicating the threat according to known fixes or self-developed patches, during runtime.

## How do we define an attack?

The Execution Chain- When performing a cyber-attack, the attacker follows a structured set of actions. One of the models that describe this set of actions is the execution chain. By defining each attack stage, Comsec's response team is able to find indications of compromise (IOCs) that were the source of the incident.




**Reconnaissance** - at this stage, the attacker collects information about the targeted organization and its assets. For example, the attacker tries to obtain information about the structure of the targeted organization, its technology stack, and the organization's security measures. To achieve the goals of this stage, the attacker can use passive reconnaissance and active reconnaissance.

**"Weaponize"** - at this stage, the attacker uses the information obtained during the reconnaissance stage to determine how the attack should be performed. The attacker chooses the exploit, the payload and the method of delivering the exploit and the payload to the targeted organization.

**Delivery** - at this stage, the attacker delivers the exploit to the targeted organization. Means of delivery usually include spam email that contains infected attachments or links to external malicious resources. The attackers may also use other means to trick organization's employees into visiting malicious or previously compromised web resources.

**Exploitation** - at this stage, the exploit takes advantage of the discovered vulnerabilities and delivers the payload.

**Persistence** - at this stage, the payload installs itself, and tries to hide its activity to avoid detection or deletion. Typically, the payload will try to install itself in such a way as to keep itself operable and undetected even if the vulnerability used by the exploit is found and fixed.

**C&C** - at this stage, the payload waits for incoming commands from the attacker. The most common way of receiving the commands is by establishing a connection to the command and control server (or C&C server) within the targeted organization's network (The C&C server is controlled by the attacker). Once the connection is established, the attacker can send commands to the payload and take actions to achieve objectives.

**Further Actions** - at this stage, the attacker uses the payload and other software that was downloaded in the course of the attack to achieve the goals of the attack. Once the attacker compromises one of the organization's assets, he or she will try to steal, change, or destroy data available on the compromised asset.

# Incident Response Service

## Our Response Methodology

The response team is following a well-defined methodology used by large vendors and research institutions around the world, including SANS. By following the next steps, the response team handles the incident:

**Identify** - The Identification process is the actual opening shot of the IR process. During this phase, the team classifies the indications of compromise (IOCs) within the network and moves to the containment phase, after firm conclusions have been made.

**Contain** - Once the team knows what incident type they are dealing with, the next move is to contain it. The key is to limit the scope and magnitude of the issue at hand. To do that, the response team has to understand in what stage of the attack they are dealing at that point of time (refer to the execution chain below).

**Eradicate** - Eradication is the process of actually getting rid of the threat in the system or network. This step should only take place after all external and internal patches are completed.

**Recover** – at this stage, the team returns the organization to normalcy by restoring services and performing validations that the threat no longer exists.

**Lessons Learned (Aftermath)** – as the incident was resolved, the response team conducts the aftermath session, which is crucial to improving an organization's security posture and readiness to face security incidents in the future.