# 1. INTRODUCCIÓ

Si es produeix un incident de seguretat informàtica a l'organització, es recomana seguir una sèrie de passes:

- Detecció de l'incident
- Anàlisi de l'incident
- Neutralització de l'atac
- Recuperació de les dades o sistemes afectats
- Recerca d'informació i rastreig de l'intrús
- Tancament de l'incident

# 2. ANÀLISI INCIDENTS

Un cop s'ha identificat un incident, s'ha de procedir a la seva anàlisi a fi d'aconseguir informació per poder restaurar les dades o els sistemes afectats.

Les passes per analitzar un incident de seguretat són:

- Consultar per consola l'estat del servidor
- Identificar nodes afectats
- Identificar servidors afectats
- Consultar *logs* servidors afectats
- Anàlisi *logs*

# 3. SCRIPT GESTIÓ INCIDENTS

El departament de seguretat de l'organització té a disposició dels especialistes un script de gestió d'incidents.

## 3.1. Consulta d'estat del servidor

$ **serverStatus**
*Es connecta als servidors i retorna la informació sobre el seu estat.*

### 3.2. Consultar els logs d'un servidor

$ **serverLogs -s *nomServidor***

*Es necessita indicar de quin servidor es volen consultar els logs. Es connecta als servidors i genera un fitxer amb els logs del servidor indicat.*

### 3.3. Desplegar un servidor usant un protocol

**$ serverDeploy -s *nomServidor* -p *nomProtocol***

*S'ha d'indicar tant el nom del servidor com el protocol a usar. Actualitza els valors actuals del servidor aplicant el protocol indicat.*
*Els protocols habituals són: coreUp, stepRight, jumpDown*

## 4. INFORMACIÓ LOGS

Els *logs* o registres d'activitat guarden seqüencialment tots els esdeveniments que afecten un procés (sistema, aplicació, xarxa…).

Informació que es pot obtenir dels *logs* del sistema:

- Moment exacte o "marca temporal" en què va ocórrer un esdeveniment (data, hora, minut, segon), la qual cosa permet analitzar passa a passa l'activitat.
- Categoria de l'esdeveniment: depuració, informació, advertència, error.

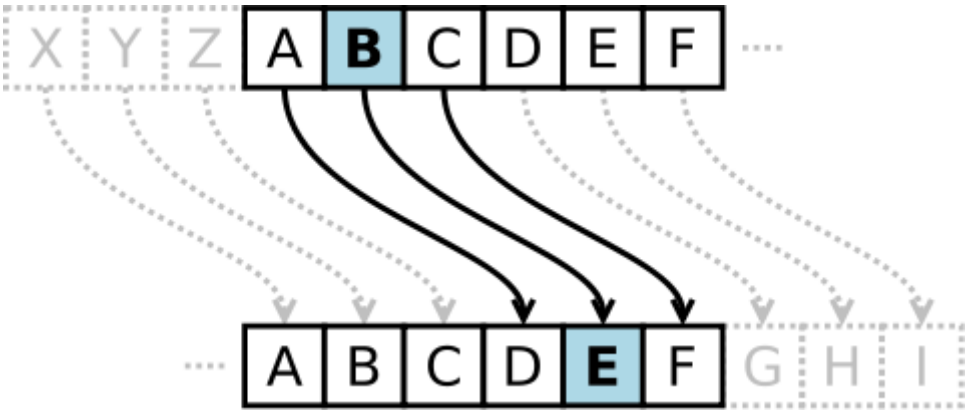
Aplicacions dels *logs*:

- Anàlisi forense
- Detecció d'intrusos
- Depuració d'errors
- Monitoratge
- Auditories

**ADVERTÈNCIA**
A fi de preservar la confidencialitat de la informació dels *logs* per preservar la seguretat del sistema, aquests es poden encriptar.
També poden ser emprats com evidències en incidents de seguretat. En aquest cas s'ha d'assegurar que no es modifiquen per mantenir la integritat de la informació.

## 5. XIFRATGE

Una tècnica de xifratge clàssic és el xifratge Cèsar. És un tipus de xifratge per substitució en el qual cada lletra del text clar se substitueix per una altra lletra que estigui un determinat nombre fix de posicions desplaçades a l'alfabet. Per exemple, amb un decalatge de 3, la A se substituiria per la D, la B esdevindria E, i així. El mètode deu el seu nom a en Juli Cèsar, qui el feia servir per comunicar-se amb els seus generals.




Exemple amb clau de xifratge 4:

```
Text clar:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Text xifrat: EFGHIJKLMNOPQRSTUVWXYZABCD

Text clar:   SETZE JUTGES MENGEN FETGE
Text xifrat: WIXDI NYXKIW QIRKIR JIXKI
```

Exemple amb clau de xifratge 6:

```
Text clar:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Text xifrat: GHIJKLMNOPQRSTUVWXYZABCDEF

Text clar:   WIKIPEDIA, LA ENCICLOPEDIA LIBRE
Text xifrat: COQOVKJOG, RG KTIOIRUVKJOG ROHXK
```

És a dir, per xifrar o desxifrar emprant Cèsar el primer a aconseguir és el nombre que fa de clau de xifratge. "Cèsar n", on n és el nombre de transposicions.