

DISPONIBILITÉ **INTÉGRITÉ** CONFIDENTIALITÉ

Présenté par Mr Alix

# STRATÉGIE RÉACTIVE EN CYBERSÉCURITÉ



# STRATÉGIE RÉACTIVE

La stratégie réactive désigne l'ensemble des mesures prises après la détection d'un incident de sécurité. Elle vise à limiter l'impact, comprendre l'incident, et restaurer un état normal sécurisé.

Objectifs de la stratégie réactive :

- Réagir rapidement et méthodiquement
- Identifier la source et la portée de l'incident
- Contenir la menace pour éviter sa propagation
- Appliquer des correctifs (remédiation)
- Documenter et améliorer les processus



# OUTILS ET TECHNIQUES

## DÉTECTION D'INTRUSION (IDS/IPS)

Identifier et bloquer les activités malveillantes ou anormales sur un réseau ou un système, en temps réel (IPS) ou a posteriori (IDS).

### OUTILS PRINCIPAUX

Outil	Fonction	Application
<b>Snort</b>	IDS basé sur signatures	Détection de scans, SQLi, menaces connues
<b>Suricata</b>	IDS/IPS multi-thread, performant	Analyse de flux complexes (ex : IPv6, HTTP2)
<b>Zeek</b>	IDS comportemental + logs détaillés	Surveillance HTTP, DNS, SSL, génération de logs

### EXEMPLE PRATIQUE : SURICATA

```
sudo suricata -c /etc/suricata/suricata.yaml -i eth0
```

- Fonction : Surveillance en temps réel sur l'interface eth0.
- Résultat : Alertes stockées dans /var/log/suricata/fast.log.



# OUTILS ET TECHNIQUES

## RÉPONSE AUX INCIDENTS

Structurer et automatiser les réactions face aux incidents de sécurité pour minimiser leur impact. Une réponse efficace suit des procédures claires (playbooks) et peut être accélérée par des outils SOAR (Security Orchestration, Automation and Response).

### Playbooks d'Incidents

Les playbooks sont des guides détaillant les étapes à suivre pour chaque type d'incident. Ils standardisent la réponse et évitent les oubli critiques.

Exemple : “PC compromis → isoler → analyser → nettoyer → réinitialiser comptes”



### SOAR (Automatisation de la réponse)

Les outils SOAR permettent d'automatiser les tâches répétitives et d'accélérer la réponse.

Outil	Fonction	Exemple d'Utilisation
TheHive	Gestion centralisée des incidents	Crée un ticket automatiquement à partir d'une alerte SIEM.
Cortex	Analyse automatisée (fichiers, IP...)	Enrichit un ticket TheHive avec des indicateurs de compromission (
Splunk SOAR	Orchestration des actions de réponse	Isole un endpoint ou bloque un hash malveillant sur l'EDR.

### Exemple de Flux Automatisé

- Alerte dans SIEM → Ticket dans TheHive
- Cortex analyse le hash d'un fichier joint
- Si malveillant → Splunk SOAR déclenche l'isolement automatique du poste

# OUTILS ET TECHNIQUES

## FORENSIQUE

Analyser un incident de sécurité en profondeur pour identifier son origine, son impact et recueillir des preuves exploitables juridiquement.

### Playbooks d'Incidents

Outil	Fonction Principale
Autopsy	Examiner une image disque, récupérer des fichiers supprimés, analyser les métadonnées.
FTK Imager	Créer une copie forensique (bit-for-bit) d'un disque sans altérer l'original.
Volatility	Analyser la mémoire RAM (processus malveillants, injections, clés de chiffrement).
Sysinternals Suite	Surveiller les processus, les connexions réseau et les exécutables auto-démarrables.



### Méthodologie d'Investigation

- Analyse des Logs
  - Outils : grep, Logwatch, Splunk, ELK.
- Timeline Analysis
  - Autopsy : Visualiser les horodatages des fichiers (création/modification).
- Vérification des Hashes
  - Comparer les empreintes (SHA256/MD5) avec des bases comme VirusTotal ou NSRL.

# OUTILS ET TECHNIQUES

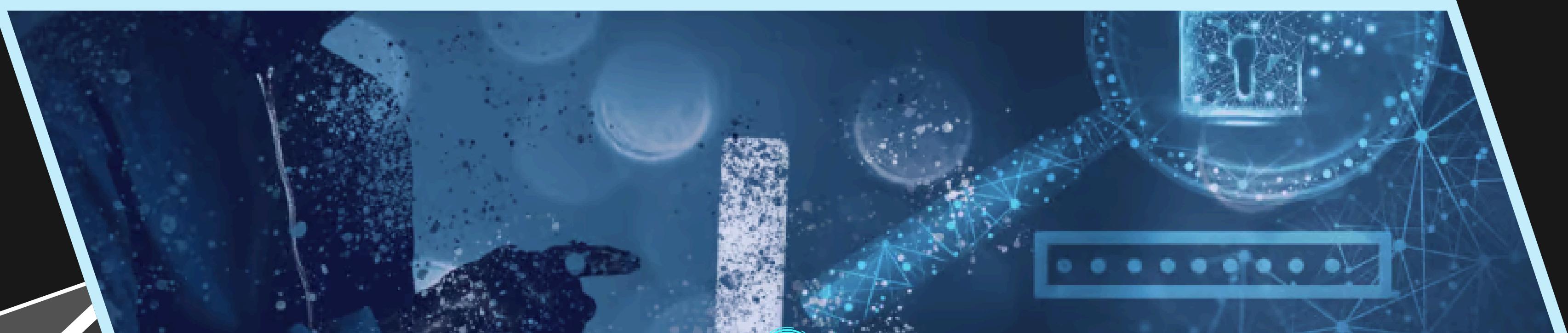
## CONTAINMENT ET REMÉDIATION

Stopper la propagation d'une attaque, sécuriser les données critiques et restaurer les systèmes dans un état sain.



### Actions pratiques

- Isolation réseau : via EDR, script, ou désactivation de l'interface
- Réinitialisation des mots de passe sur tous les comptes liés
- Suppression des backdoors trouvées
- Restauration depuis backup vérifié (ex: Veeam, Timeshift...)



# GESTION DE CRISE

## PLAN DE RÉPONSE AUX INCIDENTS (IRP)

Contenu clé :

- Rôles de chaque intervenant
- Procédures documentées
- Canaux de communication
- Niveau de criticité et priorités

Exemple :

*En cas de ransomware, l'équipe SOC isole le système en 15 min max, le juridique contacte l'assurance cyber dans l'heure.*



## COMMUNICATION

- Interne : notification à la DSI, au RSSI, à la direction
- Externe : communication au CERT, à l'ANSSI, aux clients si besoin

## COORDINATION

- CERT-MG à Madagascar, ou CERT-FR
- Fournir rapport technique et indicateurs de compromission
- Collaboration pour alerter d'autres entités menacées

# GESTION DE CRISE

## INTRUSION VIA PIÈCE JOINTE MALVEILLANTE

Contenu clé :

- Rôles de chaque intervenant
- Procédures documentées
- Canaux de communication
- Niveau de criticité et priorités

Exemple :

*En cas de ransomware, l'équipe SOC isole le système en 15 min max, le juridique contacte l'assurance cyber dans l'heure.*



## Procédure Détailnée

Étape	Action	Outil/Technique
1. Détection	Alerte Suricata sur connexion suspecte (port 4444)	Règle ET CNC ShadowPad C2 Traffic
2. Ticketing	Création automatique d'un ticket	TheHive + intégration SIEM
3. Enrichissement	Analyse du hash (ef3d8...)	Cortex + VirusTotal (90/95 AV détectent)
4. Isolation	Blocage du poste via l'EDR	Splunk SOAR → Script PowerShell Disable-NetAdapter
5. Analyse	Dump RAM → Détection de mimikatz.exe	Volatility (pslist, cmdscan)
6. Logs	Identification des mouvements latéraux (RDP)	ELK (requête : event.code:4624 AND user.name:admin)
7. Remédiation	Suppression du malware + reset des mots de passe	GPO + EDR (ex : CrowdStrike Falcon)
8. Rapport	Synthèse technique + recommandations	Template PDF exporté depuis TheHive



DISPONIBILITÉ **INTÉGRITÉ** CONFIDENTIALITÉ



# ISO/IEC 27005

## ANALYSE DE RISQUES EN CYBERSÉCURITÉ

# ISO/IEC 27005

## Analyse de risques en cybersécurité



### Origine :

Norme internationale dérivée de la famille ISO/IEC 27000, spécifiquement conçue pour accompagner la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) selon ISO 27001.

### Approche : Normative & proactive

ISO/IEC 27005 fournit un cadre méthodologique permettant d'analyser, évaluer et traiter les risques de manière structurée, cyclique et conforme aux exigences des entreprises souhaitant se certifier ISO 27001.

Proactivité : elle repose sur le principe de prévention par anticipation continue des vulnérabilités et des menaces, et sur l'amélioration constante de la sécurité via la boucle PDCA.



# ISO/IEC 27005

## Analyse de risques en cybersécurité

# LES ÉTAPES TECHNIQUES DÉTAILLÉES

1. Définir le contexte
  - Organisationnel : rôles, responsabilités, objectifs de sécurité
  - Environnement légal : conformité RGPD, lois sectorielles
  - Périmètre : SI concerné, processus, actifs métier
2. Identifier les risques
  - Actifs : matériels, logiciels, données, humains
  - Menaces : malwares, phishing, attaques internes, DDOS...
  - Vulnérabilités : absence de firewall, personnel non formé, logiciel obsolète

# ISO/IEC 27005

## Analyse de risques en cybersécurité

# LES ÉTAPES TECHNIQUES DÉTAILLÉES

3. Analyser les risques
  - Calculer l'impact potentiel (financier, réputation, légal)
  - Estimer la probabilité de survenance
  - Exemples d'outils : matrices de risques, arbres de défaillance
4. Évaluer les risques
  - Comparer les résultats aux seuils d'acceptabilité
  - Classer les risques en acceptables / non acceptables
  - Prioriser les risques à traiter

DISPONIBILITÉ **INTÉGRITÉ** CONFIDENTIALITÉ

# ISO/IEC 27005

## Analyse de risques en cybersécurité

# LES ÉTAPES TECHNIQUES DÉTAILLÉES

### 5. Traiter les risques

- Réduction : mise en place de mesures techniques (EDR, segmentation)
- Transfert : assurance cyber, externalisation
- Acceptation : risque jugé mineur
- Évitement : modification du processus métier

### 6. Surveiller et améliorer (PDCA)

- Plan : définir politiques et objectifs de sécurité
- Do : mettre en œuvre les mesures
- Check : auditer, surveiller les incidents
- Act : corriger, améliorer le système

# ISO/IEC 27005

## Analyse de risques en cybersécurité



Exemple Appliqué : Sécurisation d'une Plateforme E-Santé

### Contexte

- Périmètre : Hébergement cloud, back-office, API.
- Actifs critiques : Dossiers médicaux (RGPD), serveurs patients.
- Menaces :
  - Phishing ciblé (accès admin)
  - Exploits RCE (ex : Log4j)
  - Vol de données (darkweb)

### Analyse des Risques

Critère	Évaluation
Impact	Élevé (secret médical + amendes RGPD)
Probabilité	Moyenne (cible attractive)
Conclusion	<b>Risque inacceptable</b> → Action immédiate requise

### Mesures de Traitement

#### Protections :

- WAF (règles OWASP)
- Authentification forte (MFA + certificats)
- EDR (détection comportementale)
- Segmentation réseau (VLANS + microsegmentation)

### Surveillance Continue

- *Dashboard : Supervision SIEM (logs API + accès admin).*
- *Audits : Trimestriels (compliance HIPAA/RGPD).*
- *Tests : Pentest annuel + exercices de crise.*

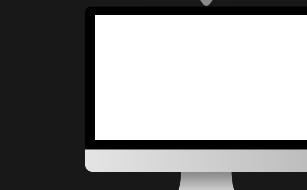
# PROJET M1

Mise en œuvre d'un système intégré de cybersécurité basé sur la norme ISO/IEC 27001 pour la détection, la réponse et la remédiation d'une attaque par ver (Silver C2) et post-exploitation (Mimikatz) sur Active Directory, à l'aide de Suricata, ELK Stack, TheHive et Windows Defender EDR”



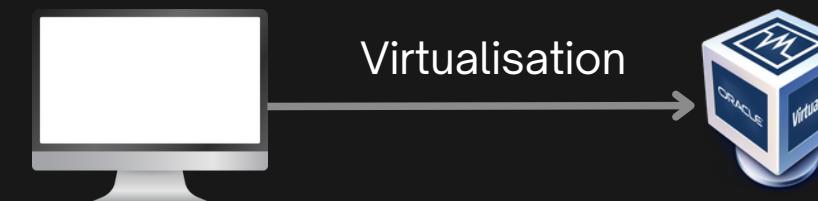
**VM1**

Active Directory  
Windows Server  
2019 DC



**VM2**

User Windows  
Vulnerable Host



Machine physique,  
SIEM, TheHive,  
VirtualBox



**Attacker**

Kali Linux / Parrot  
Worm g.  
Mimikatz



ISO/IEC  
27001

**VirtualBox**



**VM4**

IDS / IPS  
Ubuntu



**SIEM+SO**

Ubuntu