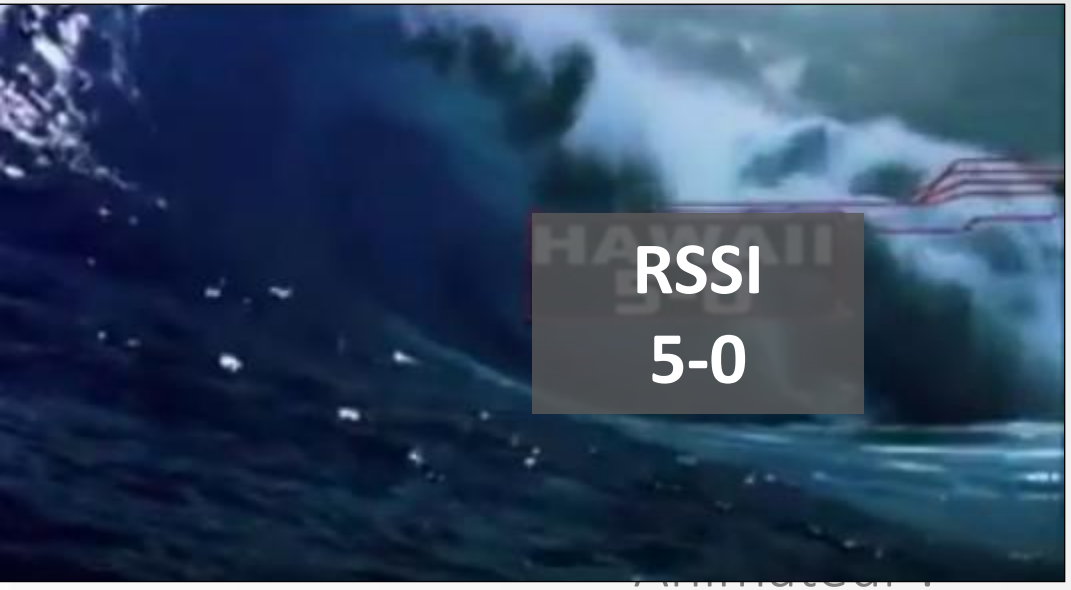
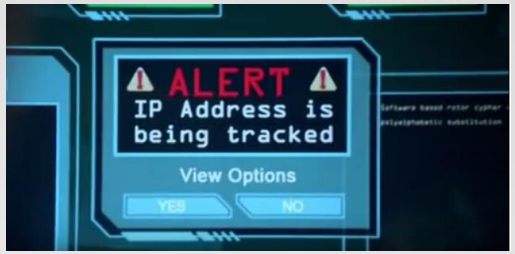
CYBER BATTLE
RSSI 5.0





Philippe TOURRON

Licence Creative Commons BY-NC-SA

P. Tourron – Tous droits réservés

Principe

- **3 équipes**
- **Une cible : un « bien ou service » à protéger**
- **Une équipe attaque : choix d'un scénario (et angle d'attaque DIC), préparation (4 min), les équipes de défense se préparent (en prenant en connaissance les mesures proposées)**
- **Lancement de l'attaque : description du scénario par l'équipe attaquante**

Les 2 équipes défendent : 4 min pour choisir 5 mesures de sécurité .

Choisir 4 mesures parmi celles proposées plus une « inventée » avec au moins 1 parmi chaque catégorie :

- **Prévention (avant l'attaque pour limiter la réalisation)**
- **Protection (pendant l'attaque pour empêcher ou réduire la progression, alerter)**
- **Récupération/Réparation (après l'attaque pour minimiser l'impact)**

- **Les équipes de défense doivent récupérer ces mesures (en concurrence) en temps limité(30s)**
- **Les équipes de défense expliquent leurs choix et leurs difficultés et la salle commente**

P. Tourron – Tous droits réservés

CONTEXTE

Contexte : la cible

LE DOSSIER PATIENT INFORMATISE

Critères de sécurité

Disponibilité
Intégrité
Confidentialité

P. Tourron – Tous droits réservés

PREMIERE ATTAQUE

ATTAQUE

CHOIX DU CRITERE D'ATTAQUE : D I C

CHOIX DU SCENARIO :

1. **DENI DE SERVICE**
2. **DEPASSEMENT DE CAPACITE DES MOYENS TECHNIQUES**
3. **USURPATION D'IDENTITE**
4. **INTRUSION PHYSIQUE DANS LES BUREAUX DES ADMINISTRATEURS**
5. **INTRUSION PHYSIQUE DANS UN DATACENTER HEBERGEANT LES DONNEES ET APPLI**
6. **INTRUSION LOGIQUE CHEZ LE MAINTENEUR AYANT ACCES A DISTANCE SUR LA CIBLE**
7. **CAPTURE DU TRAFFIC SUR LE RESEAU LOCAL**
8. **INJECTION D'UN VIRUS DE CRYPTAGE**
9. **INJECTION D'UN VIRUS DE COLLECTE DE DONNEES**

EXPLICATION PAR LES ATTAQUANTS

P. Tourron – Tous droits réservés

SELON EBIOS

M1. MAT-USG – Détournement de l'usage prévu d'un matériel
M2. MAT-ESP – Espionnage d'un matériel
M3. MAT-DEP – Dépassement des limites de fonctionnement d'un matériel
M4. MAT-DET – Détérioration d'un matériel
M5. MAT-MOD – Modification d'un matériel
M6. MAT-PTE – Perte d'un matériel

MENACES SUR LES LOGICIELS
M7. LOG-USG – Détournement de l'usage prévu d'un logiciel
M8. LOG-ESP – Analyse d'un logiciel
M9. LOG-DEP – Dépassement des limites d'un logiciel
M10. LOG-DET – Suppression de tout ou partie d'un logiciel
M11. LOG-MOD – Modification d'un logiciel
M12. LOG-PTE – Disparition d'un logiciel

MENACES SUR LES CANAUX INFORMATIQUES ET DE TÉLÉPHONIE
M13. RSX-USG – Attaque du milieu sur un canal informatique ou de téléphoı
M14. RSX-ESP – Écoute passive d'un canal informatique ou de téléphonie
M15. RSX-DEP – Saturation d'un canal informatique ou de téléphonie
M16. RSX-DET – Dégradation d'un canal informatique ou de téléphonie
M17. RSX-MOD – Modification d'un canal informatique ou de téléphonie
M18. RSX-PTE – Disparition d'un canal informatique ou de téléphonie

MENACES SUR LES PERSONNES
M19. PER-USG – Dissipation de l'activité d'une personne
M20. PER-ESP – Espionnage d'une personne à distance
M21. PER-DEP – Surcharge des capacités d'une personne
M22. PER-DET – Dégradation d'une personne
M23. PER-MOD – Influence sur une personne
M24. PER-PTE – Départ d'une personne

MENACES SUR LES SUPPORTS PAPIER
M25. PAP-USG – Détournement de l'usage prévu d'un support papier
M26. PAP-ESP – Espionnage d'un support papier
M27. PAP-DET – Détérioration d'un support papier
M28. PAP-PTE – Perte d'un support papier

MENACES SUR LES CANAUX INTERPERSONNELS
M29. CAN-USG – Manipulation via un canal interpersonnel
M30. CAN-ESP – Espionnage d'un canal interpersonnel
M31. CAN-DEP – Saturation d'un canal interpersonnel
M32. CAN-DET – Dégradation d'un canal interpersonnel
M33. CAN-MOD – Modification d'un canal interpersonnel
M34. CAN-PTE – Disparition d'un canal interpersonnel

P. Tourron – Tous droits réservés

DEFENSE

MESURES DE SECURITE

1. AUTHENTIFICATION FORTE
2. CONSIGNES DE FERMETURE DES LOCAUX
3. RANGEMENT / PROTECTION DES INFORMATIONS CONFIDENTIELLES
4. SALLE DE SECOURS
5. ANTIVOL POUR ORDINATEURS
6. MISE A JOUR ANTIVIRUS ET SYSTEMES
7. ALARME DANS LES LOCAUX
8. MOTS DE PASSES COMPLEXES
9. VIDEO-PROTECTION DES LOCAUX
10. CONTROLE D'ACCES PAR BADGE
11. BARREAUX AUX FENÊTRE EN RDC
12. CONTRAT DE MAINTENANCE 24/7
13. BROYEUR PAPIER
14. ANTIVIRUS
15. AUTHENTIFICATION FORTE (CPS, OTP)
16. COMPTES DISTINCTS POUR L'ADMINISTRATION DES SYSTEMES
17. ORGANISER UNE COMMUNICATION
18. INTERDIRE INSTALLATION LOGICIEL PAR LES UTILISATEURS
19. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT SUR LES POSTES
20. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT DANS LES MEL
21. WAF : PARE-FEU APPLICATION WEB
22. PARE-FEU RESEAU
23. SAUVEGARDE HORS LIGNE SUR SITE EXTERNE
24. ASSURANCE POUR LES DEGATS MATERIELS
25. ASSURANCE POUR LES DEGATS D'IMAGE
26. INTERVENTION PC SECURITE SUR ALARME
27. CHIFFREMENT DES POSTES
28. GESTION DE CRISE ET ENTRAINEMENT
29. PROCEDURE DE COUPURE INTERNET
30. HTTPS POUR ACCES APPLICATION
31. DISPOSITIF DE PROTECTION INCENDIE
32. SENSIBILISATION A LA SECURITE
33. CHARTE ET ENGAGEMENT DE CONFIDENTIALITE
34. SEGMENTATION DU RESEAU ET FILTRAGE LAN
35. COLLECTE ET CORRELATION DES TRACES (ALERTE, RAPPORTS, AUDIT/ANALYSE)
36. PCA/PRA
37. TEST ET ENTRAINEMENT A LA RECUPERATION DES SAUVEGARDES
38. BASTION D'ADMINISTRATION FILTRANT ET ENREGISTRANT MAINTENEUR
39. DOUBLE PARE-FEU DE MARQUE DIFFERENTES
40. OPTION IPS EVOLUEE
41. MODE DEGRADE POUR LES APPLICATIONS CRITIQUES
42. ELIMINER OU PROTEGER EN PERIMETRIE LES SYTEMES OBSOLETES
43. DEPOT DE PLAINTE
44. PROXY INTERNET ET REGLES ADAPTABLE
45. REVERSE PROXY POUR ACCES DEPUIS INTERNET
46. SYSTÈME DE DETECTION DE VULNERABILITE
47. PORTES ANTI-EFFRACTION

P. Tourron – Tous droits réservés

DEUXIEME ATTAQUE

Contexte : la cible

SITE WEB DE DEMANDE DE RDV PATIENT

Critères de sécurité

Disponibilité
Intégrité
Confidentialité

P. Tourron – Tous droits réservés

ATTAQUE

CHOIX DU CRITERE D'ATTAQUE : D I C

CHOIX DU SCENARIO :

1. **DENI DE SERVICE (saturation pour ralentir/interrompre un service)**
2. **DEPASSEMENT DE CAPACITE DES MOYENS TECHNIQUES**
3. **USURPATION D'IDENTITE**
4. **INTRUSION PHYSIQUE DANS LES BUREAUX DES ADMINISTRATEURS**
5. **INTRUSION PHYSIQUE DANS UN DATACENTER HEBERGEANT LES DONNEES ET APPLI**
6. **CAPTURE DU TRAFFIC SUR LE RESEAU LOCAL**
7. **INJECTION D'UN VIRUS DE CRYPTAGE**
8. **INJECTION D'UN VIRUS DE COLLECTE DE DONNEES**

EXPLICATION PAR LES ATTAQUANTS

P. Tourron – Tous droits réservés

SELON EBIOS

M1. MAT-USG – Détournement de l'usage prévu d'un matériel
M2. MAT-ESP – Espionnage d'un matériel
M3. MAT-DEP – Dépassement des limites de fonctionnement d'un matériel
M4. MAT-DET – Détérioration d'un matériel
M5. MAT-MOD – Modification d'un matériel
M6. MAT-PTE – Perte d'un matériel

MENACES SUR LES LOGICIELS
M7. LOG-USG – Détournement de l'usage prévu d'un logiciel
M8. LOG-ESP – Analyse d'un logiciel
M9. LOG-DEP – Dépassement des limites d'un logiciel
M10. LOG-DET – Suppression de tout ou partie d'un logiciel
M11. LOG-MOD – Modification d'un logiciel
M12. LOG-PTE – Disparition d'un logiciel

MENACES SUR LES CANAUX INFORMATIQUES ET DE TÉLÉPHONIE
M13. RSX-USG – Attaque du milieu sur un canal informatique ou de téléphoı
M14. RSX-ESP – Écoute passive d'un canal informatique ou de téléphonie
M15. RSX-DEP – Saturation d'un canal informatique ou de téléphonie
M16. RSX-DET – Dégradation d'un canal informatique ou de téléphonie
M17. RSX-MOD – Modification d'un canal informatique ou de téléphonie
M18. RSX-PTE – Disparition d'un canal informatique ou de téléphonie

MENACES SUR LES PERSONNES
M19. PER-USG – Dissipation de l'activité d'une personne
M20. PER-ESP – Espionnage d'une personne à distance
M21. PER-DEP – Surcharge des capacités d'une personne
M22. PER-DET – Dégradation d'une personne
M23. PER-MOD – Influence sur une personne
M24. PER-PTE – Départ d'une personne

MENACES SUR LES SUPPORTS PAPIER
M25. PAP-USG – Détournement de l'usage prévu d'un support papier
M26. PAP-ESP – Espionnage d'un support papier
M27. PAP-DET – Détérioration d'un support papier
M28. PAP-PTE – Perte d'un support papier

MENACES SUR LES CANAUX INTERPERSONNELS
M29. CAN-USG – Manipulation via un canal interpersonnel
M30. CAN-ESP – Espionnage d'un canal interpersonnel
M31. CAN-DEP – Saturation d'un canal interpersonnel
M32. CAN-DET – Dégradation d'un canal interpersonnel
M33. CAN-MOD – Modification d'un canal interpersonnel
M34. CAN-PTE – Disparition d'un canal interpersonnel

P. Tourron – Tous droits réservés

DEFENSE

MESURES DE SECURITE

1. AUTHENTIFICATION FORTE
2. CONSIGNES DE FERMETURE DES LOCAUX
3. RANGEMENT / PROTECTION DES INFORMATIONS CONFIDENTIELLES
4. SALLE DE SECOURS
5. ANTIVOL POUR ORDINATEURS
6. MISE A JOUR ANTIVIRUS ET SYSTEMES
7. ALARME DANS LES LOCAUX
8. MOTS DE PASSES COMPLEXES
9. VIDEO-PROTECTION DES LOCAUX
10. CONTROLE D'ACCES PAR BADGE
11. BARREAUX AUX FENÊTRE EN RDC
12. CONTRAT DE MAINTENANCE 24/7
13. BROYEUR PAPIER
14. ANTIVIRUS
15. AUTHENTIFICATION FORTE (CPS, OTP)
16. COMPTES DISTINCTS POUR L'ADMINISTRATION DES SYSTEMES
17. ORGANISER UNE COMMUNICATION
18. INTERDIRE INSTALLATION LOGICIEL PAR LES UTILISATEURS
19. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT SUR LES POSTES
20. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT DANS LES MEL
21. WAF : PARE-FEU APPLICATION WEB
22. PARE-FEU RESEAU
23. SAUVEGARDE HORS LIGNE SUR SITE EXTERNE
24. ASSURANCE POUR LES DEGATS MATERIELS
25. ASSURANCE POUR LES DEGATS D'IMAGE
26. INTERVENTION PC SECURITE SUR ALARME
27. CHIFFREMENT DES POSTES
28. GESTION DE CRISE ET ENTRAINEMENT
29. PROCEDURE DE COUPURE INTERNET
30. HTTPS POUR ACCES APPLICATION
31. DISPOSITIF DE PROTECTION INCENDIE
32. SENSIBILISATION A LA SECURITE
33. CHARTE ET ENGAGEMENT DE CONFIDENTIALITE
34. SEGMENTATION DU RESEAU ET FILTRAGE LAN
35. COLLECTE ET CORRELATION DES TRACES (ALERTE, RAPPORTS, AUDIT/ANALYSE)
36. PCA/PRA
37. TEST ET ENTRAINEMENT A LA RECUPERATION DES SAUVEGARDES
38. BASTION D'ADMINISTRATION FILTRANT ET ENREGISTRANT MAINTENEUR
39. DOUBLE PARE-FEU DE MARQUE DIFFERENTES
40. OPTION IPS EVOLUEE
41. MODE DEGRADE POUR LES APPLICATIONS CRITIQUES
42. ELIMINER OU PROTEGER EN PERIMETRIE LES SYTEMES OBSOLETES
43. DEPOT DE PLAINTE / ALERTE AUTORITES, (INFO DES PERSONNES/RGPD)
44. PROXY INTERNET ET REGLES ADAPTABLE
45. REVERSE PROXY POUR ACCES DEPUIS INTERNET
46. SYSTÈME DE DETECTION DE VULNERABILITE
47. PORTES ANTI-EFFRACTION

P. Tourron – Tous droits réservés

TROISIEME ATTAQUE

Contexte : la cible

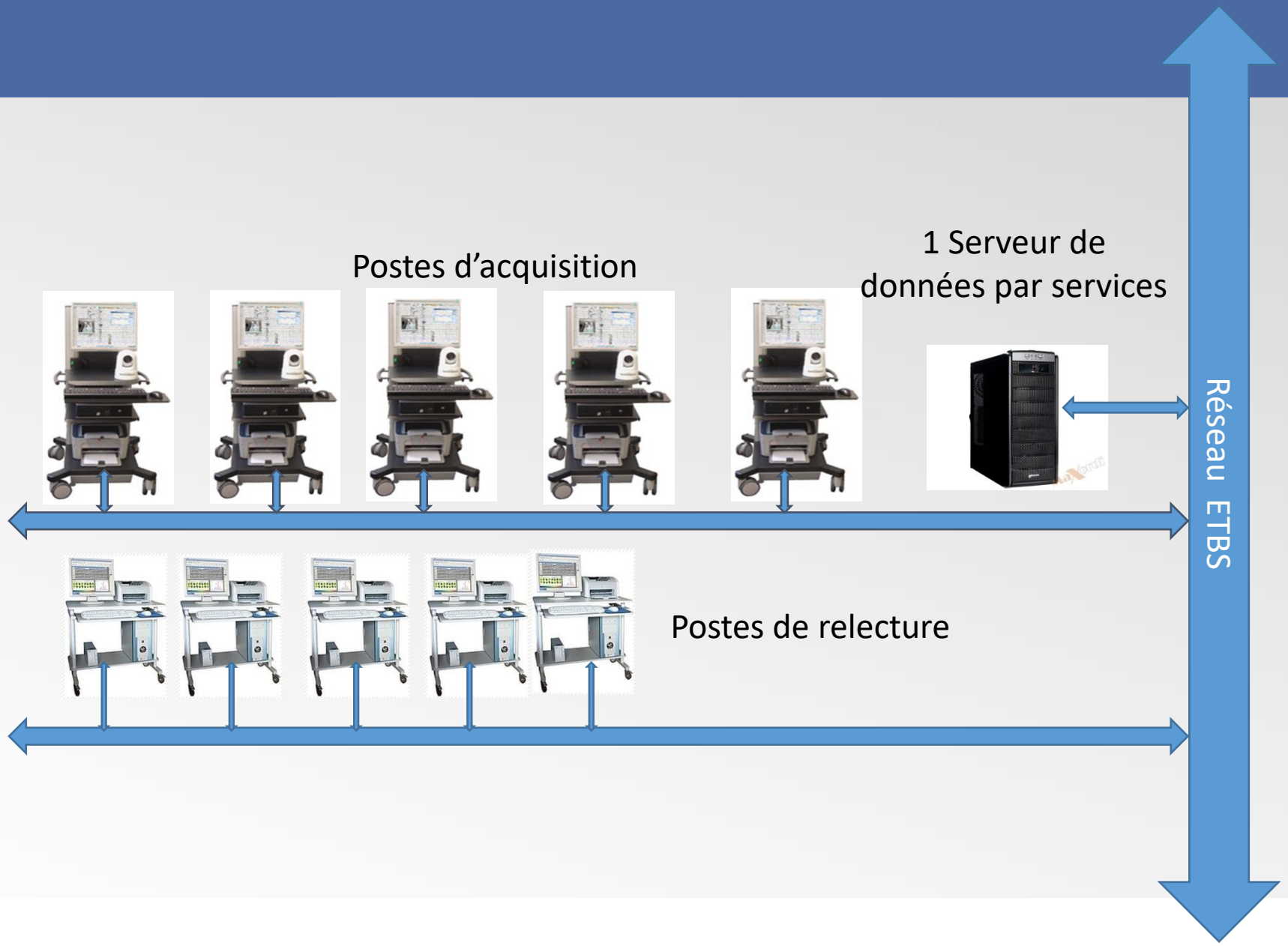
PLATEAU TECHNIQUE BIOMEDICAL : EEG
(OS plus supporté)

Critères de sécurité

Disponibilité
Intégrité
Confidentialité

P. Tourron – Tous droits réservés

EEG



P. Tourron – Tous droits réservés

ATTAQUE

CHOIX DU CRITERE D'ATTAQUE : D I C

CHOIX DU SCENARIO :

1. **DENI DE SERVICE**
2. **DEPASSEMENT DE CAPACITE DES MOYENS TECHNIQUES**
3. **USURPATION D'IDENTITE**
4. **INTRUSION PHYSIQUE DANS LES BUREAUX DES ADMINISTRATEURS**
5. **INTRUSION PHYSIQUE DANS UN DATACENTER HEBERGEANT LES DONNEES ET APPLI**
6. **INTRUSION LOGIQUE CHEZ LE MAINTENEUR AYANT ACCES A DISTANCE SUR LA CIBLE**
7. **CAPTURE DU TRAFFIC SUR LE RESEAU LOCAL**
8. **INJECTION D'UN VIRUS DE CRYPTAGE**
9. **INJECTION D'UN VIRUS DE COLLECTE DE DONNEES**

EXPLICATION PAR LES ATTAQUANTS

P. Tourron – Tous droits réservés

SELON EBIOS

M1. MAT-USG – Détournement de l'usage prévu d'un matériel
M2. MAT-ESP – Espionnage d'un matériel
M3. MAT-DEP – Dépassement des limites de fonctionnement d'un matériel
M4. MAT-DET – Détérioration d'un matériel
M5. MAT-MOD – Modification d'un matériel
M6. MAT-PTE – Perte d'un matériel

MENACES SUR LES LOGICIELS
M7. LOG-USG – Détournement de l'usage prévu d'un logiciel
M8. LOG-ESP – Analyse d'un logiciel
M9. LOG-DEP – Dépassement des limites d'un logiciel
M10. LOG-DET – Suppression de tout ou partie d'un logiciel
M11. LOG-MOD – Modification d'un logiciel
M12. LOG-PTE – Disparition d'un logiciel

MENACES SUR LES CANAUX INFORMATIQUES ET DE TÉLÉPHONIE
M13. RSX-USG – Attaque du milieu sur un canal informatique ou de téléphoı
M14. RSX-ESP – Écoute passive d'un canal informatique ou de téléphonie
M15. RSX-DEP – Saturation d'un canal informatique ou de téléphonie
M16. RSX-DET – Dégradation d'un canal informatique ou de téléphonie
M17. RSX-MOD – Modification d'un canal informatique ou de téléphonie
M18. RSX-PTE – Disparition d'un canal informatique ou de téléphonie

MENACES SUR LES PERSONNES
M19. PER-USG – Dissipation de l'activité d'une personne
M20. PER-ESP – Espionnage d'une personne à distance
M21. PER-DEP – Surcharge des capacités d'une personne
M22. PER-DET – Dégradation d'une personne
M23. PER-MOD – Influence sur une personne
M24. PER-PTE – Départ d'une personne

MENACES SUR LES SUPPORTS PAPIER
M25. PAP-USG – Détournement de l'usage prévu d'un support papier
M26. PAP-ESP – Espionnage d'un support papier
M27. PAP-DET – Détérioration d'un support papier
M28. PAP-PTE – Perte d'un support papier

MENACES SUR LES CANAUX INTERPERSONNELS
M29. CAN-USG – Manipulation via un canal interpersonnel
M30. CAN-ESP – Espionnage d'un canal interpersonnel
M31. CAN-DEP – Saturation d'un canal interpersonnel
M32. CAN-DET – Dégradation d'un canal interpersonnel
M33. CAN-MOD – Modification d'un canal interpersonnel
M34. CAN-PTE – Disparition d'un canal interpersonnel

P. Tourron – Tous droits réservés

DEFENSE

MESURES DE SECURITE

1. AUTHENTIFICATION FORTE
2. CONSIGNES DE FERMETURE DES LOCAUX
3. RANGEMENT / PROTECTION DES INFORMATIONS CONFIDENTIELLES
4. SALLE DE SECOURS
5. ANTIVOL POUR ORDINATEURS
6. MISE A JOUR ANTIVIRUS ET SYSTEMES
7. ALARME DANS LES LOCAUX
8. MOTS DE PASSES COMPLEXES
9. VIDEO-PROTECTION DES LOCAUX
10. CONTROLE D'ACCES PAR BADGE
11. BARREAUX AUX FENÊTRE EN RDC
12. CONTRAT DE MAINTENANCE 24/7
13. BROYEUR PAPIER
14. ANTIVIRUS
15. AUTHENTIFICATION FORTE (CPS, OTP)
16. COMPTES DISTINCTS POUR L'ADMINISTRATION DES SYSTEMES
17. ORGANISER UNE COMMUNICATION
18. INTERDIRE INSTALLATION LOGICIEL PAR LES UTILISATEURS
19. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT SUR LES POSTES
20. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT DANS LES MEL
21. WAF : PARE-FEU APPLICATION WEB
22. PARE-FEU RESEAU
23. SAUVEGARDE HORS LIGNE SUR SITE EXTERNE
24. ASSURANCE POUR LES DEGATS MATERIELS
25. ASSURANCE POUR LES DEGATS D'IMAGE
26. INTERVENTION PC SECURITE SUR ALARME
27. CHIFFREMENT DES POSTES
28. GESTION DE CRISE ET ENTRAINEMENT
29. PROCEDURE DE COUPURE INTERNET
30. HTTPS POUR ACCES APPLICATION
31. DISPOSITIF DE PROTECTION INCENDIE
32. SENSIBILISATION A LA SECURITE
33. CHARTE ET ENGAGEMENT DE CONFIDENTIALITE
34. SEGMENTATION DU RESEAU ET FILTRAGE LAN
35. COLLECTE ET CORRELATION DES TRACES (ALERTE, RAPPORTS, AUDIT/ANALYSE)
36. PCA/PRA
37. TEST ET ENTRAINEMENT A LA RECUPERATION DES SAUVEGARDES
38. BASTION D'ADMINISTRATION FILTRANT ET ENREGISTRANT MAINTENEUR
39. DOUBLE PARE-FEU DE MARQUE DIFFERENTES
40. OPTION IPS EVOLUEE
41. MODE DEGRADE POUR LES APPLICATIONS CRITIQUES
42. ELIMINER OU PROTEGER EN PERIMETRIE LES SYTEMES OBSOLETES
43. DEPOT DE PLAINTE
44. PROXY INTERNET ET REGLES ADAPTABLE
45. REVERSE PROXY POUR ACCES DEPUIS INTERNET
46. SYSTÈME DE DETECTION DE VULNERABILITE
47. PORTES ANTI-EFFRACTION

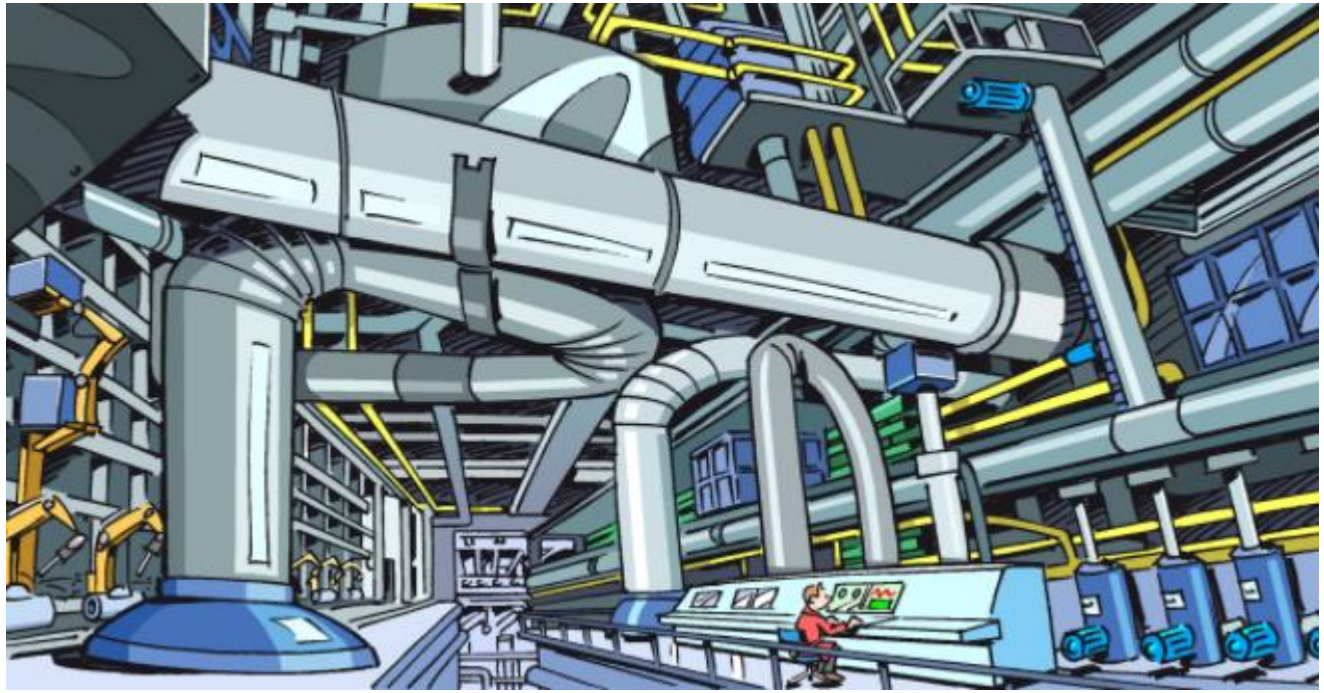
P. Tourron – Tous droits réservés

QUATRIEME ATTAQUE

Contexte : la cible

USINE DE FABRICATION ROBOTISEE

(SYSTEMES SCADA)



Critères de sécurité

Disponibilité
Intégrité
Confidentialité

P. Tourron – Tous droits réservés

ATTAQUE

CHOIX DU CRITERE D'ATTAQUE : D I C

CHOIX DU SCENARIO :

1. **DENI DE SERVICE**
2. **DEPASSEMENT DE CAPACITE DES MOYENS TECHNIQUES**
3. **USURPATION D'IDENTITE**
4. **INTRUSION PHYSIQUE DANS LES BUREAUX DES ADMINISTRATEURS**
5. **INTRUSION PHYSIQUE DANS UN DATACENTER HEBERGEANT LES DONNEES ET APPLI**
6. **INTRUSION LOGIQUE CHEZ LE MAINTENEUR AYANT ACCES A DISTANCE SUR LA CIBLE**
7. **CAPTURE DU TRAFFIC SUR LE RESEAU LOCAL**
8. **INJECTION D'UN VIRUS DE CRYPTAGE**
9. **INJECTION D'UN VIRUS DE COLLECTE DE DONNEES**

EXPLICATION PAR LES ATTAQUANTS

P. Tourron – Tous droits réservés

SELON EBIOS

M1. MAT-USG – Détournement de l'usage prévu d'un matériel
M2. MAT-ESP – Espionnage d'un matériel
M3. MAT-DEP – Dépassement des limites de fonctionnement d'un matériel
M4. MAT-DET – Détérioration d'un matériel
M5. MAT-MOD – Modification d'un matériel
M6. MAT-PTE – Perte d'un matériel

MENACES SUR LES LOGICIELS
M7. LOG-USG – Détournement de l'usage prévu d'un logiciel
M8. LOG-ESP – Analyse d'un logiciel
M9. LOG-DEP – Dépassement des limites d'un logiciel
M10. LOG-DET – Suppression de tout ou partie d'un logiciel
M11. LOG-MOD – Modification d'un logiciel
M12. LOG-PTE – Disparition d'un logiciel

MENACES SUR LES CANAUX INFORMATIQUES ET DE TÉLÉPHONIE
M13. RSX-USG – Attaque du milieu sur un canal informatique ou de téléphoı
M14. RSX-ESP – Écoute passive d'un canal informatique ou de téléphonie
M15. RSX-DEP – Saturation d'un canal informatique ou de téléphonie
M16. RSX-DET – Dégradation d'un canal informatique ou de téléphonie
M17. RSX-MOD – Modification d'un canal informatique ou de téléphonie
M18. RSX-PTE – Disparition d'un canal informatique ou de téléphonie

MENACES SUR LES PERSONNES
M19. PER-USG – Dissipation de l'activité d'une personne
M20. PER-ESP – Espionnage d'une personne à distance
M21. PER-DEP – Surcharge des capacités d'une personne
M22. PER-DET – Dégradation d'une personne
M23. PER-MOD – Influence sur une personne
M24. PER-PTE – Départ d'une personne

MENACES SUR LES SUPPORTS PAPIER
M25. PAP-USG – Détournement de l'usage prévu d'un support papier
M26. PAP-ESP – Espionnage d'un support papier
M27. PAP-DET – Détérioration d'un support papier
M28. PAP-PTE – Perte d'un support papier

MENACES SUR LES CANAUX INTERPERSONNELS
M29. CAN-USG – Manipulation via un canal interpersonnel
M30. CAN-ESP – Espionnage d'un canal interpersonnel
M31. CAN-DEP – Saturation d'un canal interpersonnel
M32. CAN-DET – Dégradation d'un canal interpersonnel
M33. CAN-MOD – Modification d'un canal interpersonnel
M34. CAN-PTE – Disparition d'un canal interpersonnel

P. Tourron – Tous droits réservés

DEFENSE

MESURES DE SECURITE

1. AUTHENTIFICATION FORTE
2. CONSIGNES DE FERMETURE DES LOCAUX
3. RANGEMENT / PROTECTION DES INFORMATIONS CONFIDENTIELLES
4. SALLE DE SECOURS
5. ANTIVOL POUR ORDINATEURS
6. MISE A JOUR ANTIVIRUS ET SYSTEMES
7. ALARME DANS LES LOCAUX
8. MOTS DE PASSES COMPLEXES
9. VIDEO-PROTECTION DES LOCAUX
10. CONTROLE D'ACCES PAR BADGE
11. BARREAUX AUX FENÊTRE EN RDC
12. CONTRAT DE MAINTENANCE 24/7
13. BROYEUR PAPIER
14. ANTIVIRUS
15. AUTHENTIFICATION FORTE (CPS, OTP)
16. COMPTES DISTINCTS POUR L'ADMINISTRATION DES SYSTEMES
17. ORGANISER UNE COMMUNICATION
18. INTERDIRE INSTALLATION LOGICIEL PAR LES UTILISATEURS
19. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT SUR LES POSTES
20. SYSTEME DE DETECTION DE COMPORTEMENT MALVEILLANT DANS LES MEL
21. WAF : PARE-FEU APPLICATION WEB
22. PARE-FEU RESEAU
23. SAUVEGARDE HORS LIGNE SUR SITE EXTERNE
24. ASSURANCE POUR LES DEGATS MATERIELS
25. ASSURANCE POUR LES DEGATS D'IMAGE
26. INTERVENTION PC SECURITE SUR ALARME
27. CHIFFREMENT DES POSTES
28. GESTION DE CRISE ET ENTRAINEMENT
29. PROCEDURE DE COUPURE INTERNET
30. HTTPS POUR ACCES APPLICATION
31. DISPOSITIF DE PROTECTION INCENDIE
32. SENSIBILISATION A LA SECURITE
33. CHARTE ET ENGAGEMENT DE CONFIDENTIALITE
34. SEGMENTATION DU RESEAU ET FILTRAGE LAN
35. COLLECTE ET CORRELATION DES TRACES (ALERTE, RAPPORTS, AUDIT/ANALYSE)
36. PCA/PRA
37. TEST ET ENTRAINEMENT A LA RECUPERATION DES SAUVEGARDES
38. BASTION D'ADMINISTRATION FILTRANT ET ENREGISTRANT MAINTENEUR
39. DOUBLE PARE-FEU DE MARQUE DIFFERENTES
40. OPTION IPS EVOLUEE
41. MODE DEGRADE POUR LES APPLICATIONS CRITIQUES
42. ELIMINER OU PROTEGER EN PERIMETRIE LES SYTEMES OBSOLETES
43. DEPOT DE PLAINTE
44. PROXY INTERNET ET REGLES ADAPTABLE
45. REVERSE PROXY POUR ACCES DEPUIS INTERNET
46. SYSTÈME DE DETECTION DE VULNERABILITE
47. PORTES ANTI-EFFRACTION

P. Tourron – Tous droits réservés

RETEX des équipes : exprimez-vous

- Vous devez compter avec la pression
- Vous devez anticiper l’organisation
- Préparez-vous aux crises

Et … la GTC-GTB

MERCI DE VOTRE PARTICIPATION

DEBAT / QUESTIONS

Détail licence

- Mode de licence du document : Il est sous licence Creative Commons BY-NC-SA, c’est-à-dire que vous pouvez reproduire cette création, la diffuser ou encore la modifer sous les conditions suivantes :
- Paternité : vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'oeuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'oeuvre)
- Pas d’utilisation commerciale : vous n'avez pas le droit d'utiliser cette création à des fins commerciales
- Partage des conditions initiales à l’identique : si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

P. Tourron – Tous droits réservés