[Date]

Xavier Martin

CHU Ynov

Configuration IPS/IDS

CHU Ynov

Table des matières

[1. Objectifs de la solution IPS/IDS 2](#_Toc202340351)

[2. Portée et périmètre 4](#_Toc202340352)

[3. Architecture cible 7](#_Toc202340353)

[4. Choix des technologies 11](#_Toc202340354)

[5. Configuration des règles IPS/IDS 15](#_Toc202340355)

[6. Intégration réseau 19](#_Toc202340356)

[7. Surveillance et alerting 23](#_Toc202340357)

[8. Processus de réponse aux alertes 27](#_Toc202340358)

[9. Tests et validation 31](#_Toc202340359)

[10. Conformité et gouvernance 34](#_Toc202340360)

[11. Formation et sensibilisation 38](#_Toc202340361)

[12. Amélioration continue 42](#_Toc202340362)

# 1. Objectifs de la solution IPS/IDS

La mise en place d’une solution IPS/IDS (Intrusion Prevention System / Intrusion Detection System) au sein du CHU Ynov s’inscrit dans la stratégie globale de sécurisation des systèmes d’information hospitaliers. Son objectif principal est de renforcer la posture de défense en profondeur et de répondre aux exigences réglementaires et métiers en matière de sécurité des données de santé.

**1.1 Garantir la détection et la prévention des intrusions**

Surveiller en temps réel le trafic réseau interne et externe pour identifier toute activité malveillante, anormale ou suspecte.

Bloquer automatiquement les attaques connues et les patterns de menace grâce à des signatures mises à jour.

Identifier des attaques « zero-day » ou des comportements anormaux par des mécanismes d’analyse heuristique ou comportementale.

Couvrir les vecteurs d’attaque classiques : scans de ports, brute-force, exploits applicatifs, tentatives d’escalade de privilèges, exfiltration de données.

**1.2 Protéger les systèmes d’information critiques hospitaliers**

Défendre les flux sensibles : Dossier Patient Informatisé (DPI), systèmes de laboratoire (LIMS), pharmacie, radiologie (RIS/PACS), portails métiers.

Empêcher la compromission de serveurs applicatifs, bases de données ou hyperviseurs hébergeant des données de santé à caractère personnel.

Surveiller les interconnexions avec des prestataires, partenaires ou autres établissements (GHT).

Maintenir la disponibilité des services face aux attaques par déni de service (DoS/DDoS).

**1.3 Réduire la surface d’attaque et contenir les incidents**

Segmenter et contrôler les flux réseau entre les différentes zones (DMZ, LAN administratif, VLAN médicaux).

Mettre en place des barrières techniques pour isoler un segment en cas de compromission.

Limiter la propagation latérale d’un malware ou d’un ransomware.

Faciliter les actions de confinement immédiat en cas d’alerte critique.

**1.4 Améliorer la visibilité et la traçabilité des événements de sécurité**

Collecter et analyser les logs de détection et de prévention des intrusions.

Fournir une visibilité complète sur le trafic réseau en clair et chiffré (avec inspection SSL si nécessaire).

Contribuer à l’alimentation du SIEM régional ou du SOC GHT pour corrélation multi-sources.

Assurer la journalisation horodatée et signée des événements de sécurité pour les besoins d’enquête, de forensique et de conformité RGPD.

**1.5 Renforcer la conformité réglementaire et les exigences sectorielles**

Répondre aux exigences de la PGSSI-S sur le « contrôle des accès et journalisation » et la « détection des incidents de sécurité ».

Contribuer au respect des obligations RGPD, notamment la détection et la notification des violations de données à caractère personnel.

Respecter les exigences des hébergeurs HDS et des prestataires certifiés, notamment en matière de journalisation et de traçabilité des accès.

S’inscrire dans la démarche globale de mise en œuvre du SMSI (ISO 27001), en intégrant l’IPS/IDS comme mesure de sécurité documentée et auditable.

**1.6 Soutenir la gestion des incidents et la continuité des soins**

Fournir des alertes en temps réel permettant une réaction rapide et coordonnée.

Supporter la cellule de crise SSI lors des incidents graves, avec des données précises sur la nature et la portée de l’attaque.

Limiter l’impact potentiel sur la prise en charge des patients en permettant un confinement efficace et une continuité en mode dégradé.

Contribuer aux exercices PRA/PCA en simulant des scénarios d’attaque et en validant les plans de réponse.

**1.7 Favoriser l’amélioration continue et la maturité cyber**

Alimenter les exercices de sensibilisation et de formation des équipes (DSI, RSSI, administrateurs réseaux).

Permettre l’analyse des tendances et des menaces émergentes via les rapports consolidés.

Servir de base à la mise à jour de la PSSI et des plans directeurs SI.

Garantir l’adaptabilité du dispositif de sécurité face à l’évolution des infrastructures (cloud, IoT médical, mobilité).

# 2. Portée et périmètre

Cette section définit les contours techniques et organisationnels de la solution IPS/IDS. Elle précise les zones du réseau concernées, les flux couverts, les types de données protégées et les priorités métier. En clarifiant ce périmètre, le CHU Ynov s’assure d’une couverture adaptée aux risques et d’une allocation optimale des ressources de sécurité.

**2.1 Périmètre fonctionnel**

Cette sous-partie décrit les objectifs fonctionnels précis que le périmètre doit adresser.

Couvrir la détection et la prévention des intrusions sur les segments réseau les plus critiques pour le soin.

Protéger les applications métier hospitalières : Dossier Patient Informatisé (DPI), laboratoire (LIMS), imagerie (RIS/PACS), pharmacie, systèmes de prescription.

Surveiller les flux intersites entre les établissements AP-HM et le GHT via VPN ou liaisons dédiées.

Inclure les accès Internet (patients, visiteurs, prestataires) et la DMZ exposant des services externes.

Garantir la journalisation et la traçabilité des événements de sécurité sur l’ensemble de ces périmètres.

**2.2 Périmètre technique réseau**

Cette sous-partie détaille les segments réseau où l’IPS/IDS sera déployé et actif.

**2.2.1 Zones critiques incluses :**

LAN médical : VLAN des unités de soins, postes cliniques, équipements biomédicaux connectés.

VLAN administratifs : services RH, facturation, achats.

DMZ : serveurs exposés aux accès externes (portails patients, interopérabilité GHT).

Liaisons VPN intersites : tunnels chiffrés reliant le site principal au PRA et aux autres établissements du GHT.

Interfaces Internet : sorties Internet générales et accès invités.

**2.2.2 Segmentation et isolation :**

Identification des VLAN et sous-réseaux via cartographie réseau validée.

Définition des points d’insertion pour les capteurs IPS (inline) et IDS (sniffer).

Segmentation logique et physique permettant le filtrage et la surveillance différenciée des flux métiers et techniques.

**2.3 Périmètre applicatif**

Cette sous-partie précise les applications et services hospitaliers qui seront protégés et surveillés.

Dossier Patient Informatisé (DPI) : flux API, connexions client-serveur, interopérabilité HL7.

Applications métiers hospitalières : gestion des lits, rendez-vous, facturation, identito-vigilance.

Systèmes de laboratoire (LIMS) et d’imagerie médicale (RIS/PACS) : connexions DICOM, HL7, FTP/SFTP.

Plateformes de prescription et pharmacie : flux sécurisés entre pharmacie et services cliniques.

Systèmes tiers et interopérabilité : flux EAI, ESB, échanges avec le GHT.

**2.4 Périmètre des données protégées**

Cette sous-partie décrit le type de données dont la sécurité sera améliorée grâce à la surveillance IPS/IDS.

Données de santé à caractère personnel (DCP) : dossier médical, résultats de laboratoire, imagerie.

Données administratives sensibles : informations RH, données financières.

Journalisation des accès : logs applicatifs, journaux système.

Flux inter-applicatifs critiques : échanges internes entre bases de données, serveurs applicatifs, systèmes analytiques.

Données d’authentification : flux LDAP/AD, RADIUS, SSO hospitalier.

**2.5 Flux réseau surveillés**

Cette sous-partie précise la granularité des flux réseau inclus dans la surveillance.

Flux Nord-Sud : trafic entrant/sortant Internet (menaces externes).

Flux Est-Ouest : communications inter-VLAN au sein du SI hospitalier (lateral movement potentiel).

Flux Inter-sites : liaisons sécurisées avec le PRA ou d’autres hôpitaux du GHT.

Flux DMZ : requêtes externes vers les portails exposés.

Flux prestataires : connexions VPN partenaires pour télémaintenance ou services HDS.

**2.6 Priorités métier et criticité**

Cette sous-partie définit la priorisation des ressources IPS/IDS selon les risques métier.

Priorité 1 (Critique) :

DPI, prescriptions, systèmes de laboratoire et d’imagerie.

Flux de synchronisation intersites (PRA).

Interfaces exposées sur Internet (DMZ).

Priorité 2 (Importante) :

Applications administratives RH, finances.

Accès invités/visiteurs.

Flux inter-VLAN non critiques.

Priorité 3 (Surveillance opportuniste) :

Supervision technique interne.

Flux backup internes (hors PRA).

**2.7 Limitations et exclusions**

Cette sous-partie clarifie ce qui est volontairement exclu ou limité pour des raisons techniques ou de politique.

Flux de sauvegarde hors site chiffrés avec bande passante dédiée (pour éviter les faux positifs massifs).

Réplications internes des SAN/VM hyperviseurs (non inspectées inline pour performance).

Flux SNMP de supervision technique.

Trafic intra-hôte (loopback) sur serveurs virtualisés (surveillé par autres outils).

**2.8 Gouvernance du périmètre**

Cette sous-partie définit les mécanismes de mise à jour et de validation du périmètre.

Cartographie réseau et applicative validée semestriellement par la DSI et le RSSI.

Processus de changement contrôlé (CAB) pour l’ajout/retrait de segments ou de flux surveillés.

Documentation formalisée dans la GED sécurisée.

Suivi via tableaux de bord SIEM intégrant la couverture IPS/IDS.

Intégration des mises à jour dans la PSSI et le SMSI.

# 3. Architecture cible

Cette section présente l’architecture technique de déploiement des composants IPS/IDS du CHU Ynov. L’architecture cible repose sur un équilibre entre couverture maximale, performance réseau, tolérance aux pannes et intégration dans l’écosystème de sécurité existant (pare-feux, SIEM, SOC, PRA). Elle distingue les modes de fonctionnement (inline vs passif), les zones réseau surveillées, et les mécanismes de redondance.

**3.1 Objectifs d’architecture**

Cette sous-partie précise les objectifs stratégiques et opérationnels visés par l’architecture IPS/IDS.

Surveillance active du trafic critique sans introduire de point de défaillance unique (SPOF).

Couverture complète des segments critiques, avec granularité adaptée au niveau de sensibilité.

Déploiement hybride : mix entre composants inline (prévention) et en miroir (détection passive).

Haute disponibilité (HA) : garantir la continuité de la surveillance même en cas de défaillance matérielle.

Facilité de maintenance et de montée en charge, pour intégrer de nouveaux flux ou systèmes sans refonte majeure.

**3.2 Composants de l’architecture**

Cette sous-partie détaille les briques techniques qui composent le système IPS/IDS.

Capteurs IPS inline : équipements physiques ou virtuels (ex : Fortinet FortiGate, Palo Alto, Stormshield), insérés directement sur les liaisons critiques (LAN médical → cœur de réseau).

Sondes IDS passives : capteurs en mode miroir/monitor (ex : Suricata, Snort), reliés à des ports SPAN sur les switchs cœur.

Console de management centralisée (NMS) : interface d’administration pour la gestion des politiques, des journaux, des signatures et des alertes.

Serveur de journalisation / collecteur de logs : intégré au SIEM régional ou local (ELK, Splunk, Wazuh).

Lien vers le SOC régional : transmission temps réel des alertes critiques, supervision étendue.

**3.3 Mode de déploiement : hybride IPS/IDS**

Cette sous-partie présente les choix techniques entre prévention (inline) et détection (passif).

Mode IPS Inline (préventif)

Positionné en amont des systèmes critiques (DPI, PACS, LIMS).

Capable de bloquer activement les paquets malveillants selon des signatures ou heuristiques.Fonctionnalités d’inspection SSL, inspection DNS, filtrage protocolaire, signature personnalisée.

Support HA avec bypass matériel ou logique en cas de défaillance (fail-open configurable).

Mode IDS Sniffer (passif)

Positionné sur les ports SPAN des switchs cœur et des routeurs de bordure.

Permet une surveillance sans impact sur le trafic (pas de coupure possible).

Dédié à l’analyse comportementale (lateral movement, brute-force interne, anomalies métier).

Alimente le SIEM pour corrélation inter-outils.

**3.4 Localisation des sondes**

Cette sous-partie localise physiquement et logiquement les équipements dans l’infrastructure réseau.

Site principal (CHU) :

IPS entre firewall interne et routeurs de distribution.

IDS sur segments LAN métiers sensibles.

Datacenter PRA distant :

IDS passif sur l’entrée des flux de réplication.

IPS sur les flux sortants vers le PRA (via tunnels VPN).

DMZ et internet :

IPS inline en frontal sur les interfaces exposées (portails patients, accès partenaires).

IDS sur les flux entrants sortants (reverse proxy, accès prestataires).

Postes critiques isolés (ex : radiologie, bloc opératoire connecté) :

Capteurs légers type Suricata mini-appliance ou agent logiciel.

**3.5 Résilience et haute disponibilité**

Cette sous-partie décrit les mécanismes garantissant la continuité de la surveillance et la non-interruption des soins.

Redondance active/passive des capteurs IPS (cluster HA, VRRP, heartbeat).

Fail-open configurables pour garantir le passage des paquets en cas de panne.

Double alimentation, double carte réseau pour chaque capteur inline.

Supervision continue des sondes par les outils Zabbix / Centreon.

Journalisation persistante hors bande vers un collecteur tiers (éviter perte d’alertes).

**3.6 Intégration au SIEM et au SOC**

Cette sous-partie décrit comment les sondes s’intègrent dans l’écosystème de cybersurveillance.

Transmission temps réel des alertes vers le SIEM régional (Elastic, Splunk, Graylog).

Corrélation avec les logs AD, firewall, antivirus et proxies.

Classement automatique des alertes (informative / suspecte / critique).

Interface web de tableaux de bord personnalisés pour la DSI et le RSSI.

Journalisation signée et horodatée selon les exigences PSSI-S.

**3.7 Schéma réseau de référence (à annexer)**

Un schéma réseau est associé à cette section et comprend :

La localisation logique et physique de chaque capteur.

Le routage et le VLAN tagging des flux inspectés.

Les flux mirroring configurés sur les switchs cœur.

Les flux montants vers la console d’administration et le SIEM.

Le chemin de secours activé en cas de panne ou de bascule PRA.

**3.8 Gouvernance de l’architecture**

Cette sous-partie encadre la gestion de l’architecture dans la durée.

Architecture validée par le comité de pilotage SSI et intégrée au plan directeur SI.

Révision annuelle avec mise à jour des emplacements physiques, règles de segmentation, équipements déployés.

Documentation complète dans la GED sécurisée (schémas, configurations, procédures).

Recette technique à chaque nouvelle intégration ou migration de services critiques.

# 4. Choix des technologies

Cette section détaille les solutions logicielles et matérielles envisagées ou recommandées pour la mise en œuvre du dispositif IPS/IDS du CHU Ynov. Le choix des technologies doit répondre à des critères de robustesse, de compatibilité avec l’architecture hospitalière, de conformité réglementaire et d’évolutivité.

**4.1 Objectifs du choix technologique**

Cette sous-partie précise les exigences fonctionnelles et stratégiques qui guident la sélection des outils et équipements.

Garantir la détection et la prévention des menaces connues et inconnues, y compris les attaques ciblées sur des protocoles médicaux spécifiques (HL7, DICOM).

Offrir une administration centralisée et unifiée des politiques de sécurité et des logs.

Assurer la scalabilité pour accompagner la croissance des flux et des équipements réseau.

Permettre l’intégration avec le SIEM régional et le SOC du GHT.

Respecter les contraintes réglementaires (HDS, PGSSI-S, RGPD) en matière de journalisation et de confidentialité des données.

**4.2 Critères de sélection des solutions**

Cette sous-partie explicite les principaux critères techniques et organisationnels retenus.

Compatibilité réseau : support de hauts débits (1/10/40 Gbps), inspection SSL/TLS, VLAN tagging.

Capacités d’analyse : base de signatures mise à jour, inspection des protocoles applicatifs (HTTP/S, FTP/SFTP, DNS, SMB, HL7).

Haute disponibilité : modes actif/actif ou actif/passif, fail-open configurable.

Journalisation et traçabilité : logs signés et horodatés, export vers SIEM.

Administration sécurisée : accès restreint via bastion, MFA, chiffrement des communications.

Certification ou conformité sectorielle : ISO 27001, ANSSI CSPN/CC (si disponible), bonnes pratiques HDS.

**4.3 Équipements IPS recommandés**

Cette sous-partie décrit les choix matériels/logiciels pour la partie IPS (inline).

Fortinet FortiGate (version NGFW) :

Inspection en profondeur des paquets (DPI).

Filtrage applicatif (Layer 7), signatures AV/IPS régulièrement mises à jour.

Inspection SSL/TLS avec certificats internes.

Haute disponibilité (HA) actif/passif ou clustering.

Support des interfaces multiples (10 Gbps).

Palo Alto Networks :

Moteur d’analyse Threat Prevention.

Détection de zero-day via WildFire (sandboxing cloud).

Gestion centralisée via Panorama.

Analyse des protocoles médicaux spécifiques (via App-ID).

Stormshield Network Security :

Fabrication européenne, certification CSPN.

Inspection en profondeur personnalisable.

Support des environnements virtualisés (VMware, KVM).

**4.4 Logiciels IDS open source**

Pour les sondes passives, des solutions open source robustes sont envisagées.

Suricata :

Multi-threading, haute performance.

Détection signatures et anomalies.

Support de l’analyse TLS, HTTP, SMB.

Compatible avec Elasticsearch/Logstash/Kibana (ELK).

Snort :

Large communauté, signatures régulièrement mises à jour.

Simplicité de déploiement sur ports SPAN.

Extensible via règles personnalisées.

Intégrable avec l’écosystème SIEM/SOC.

**4.5 Plateformes de gestion centralisée**

Cette sous-partie décrit les outils pour piloter la politique de sécurité et centraliser les logs.

FortiAnalyzer :

Agrégation des logs FortiGate.

Rapports personnalisés.

Support pour RGPD (recherche sur données personnelles).

Panorama (Palo Alto) :

Administration centralisée des règles et signatures.

Gestion des mises à jour.

Historique des modifications (audit trail).

Graylog / ELK Stack :

Agrégation des logs IDS open source.

Dashboard personnalisés.

Intégration SIEM/SOC régional.

**4.6 Intégration avec le SIEM et le SOC**

Cette sous-partie précise les besoins d’interopérabilité avec les systèmes existants.

Export natif des logs au format syslog sécurisé (TCP/TLS).

Envoi des alertes temps réel vers le SIEM régional.

Corrélation des événements avec logs AD, firewall, antivirus.

Support des API REST pour enrichir les dashboards de supervision.Respect des exigences de journalisation longue durée (18-24 mois selon politique).

**4.7 Sécurité et conformité des outils**

Cette sous-partie détaille les mesures de sécurité imposées aux solutions choisies.

Chiffrement systématique des communications d’administration et de journalisation.

Authentification forte (MFA) pour l’accès aux consoles.

Journalisation des actions administrateurs : logs immuables, exportables pour audit.

Gestion des mises à jour : planification et test sur environnement préproduction.

Validation interne : revue des configurations avant mise en production.

Conformité RGPD :

Cartographie des données personnelles contenues dans les logs.

Analyse d’impact (PIA) si nécessaire.

**4.8 Support et maintenance**

Cette sous-partie aborde les engagements attendus des éditeurs et intégrateurs.

Contrat de support 24/7 pour les équipements IPS.

Accès aux mises à jour de signatures et firmware.

Engagements SLA en cas de panne critique.

Formation et transfert de compétences pour les équipes DSI/RSSI.

Documentation complète en français ou anglais avec mises à jour régulières.

# 5. Configuration des règles IPS/IDS

La configuration des règles de l’IPS/IDS est une étape critique : elle permet de définir avec précision ce qui doit être détecté ou bloqué, comment, et avec quel niveau de sévérité. Elle conditionne l’efficacité du dispositif, mais aussi sa pertinence opérationnelle (éviter les faux positifs paralysants) et sa conformité réglementaire.

Cette section formalise les principes de configuration adaptés au contexte d’un CHU, la structuration des politiques, la gestion des exceptions, et les bonnes pratiques de mise à jour.

**5.1 Objectifs de la configuration des règles**

Cette sous-partie rappelle les finalités stratégiques des règles IPS/IDS.

Détecter et bloquer les menaces connues et inconnues sur l’ensemble des flux critiques.

Prioriser la protection des services médicaux (DPI, LIMS, RIS/PACS) tout en garantissant la disponibilité.

Réduire les faux positifs grâce à une adaptation fine des règles au contexte applicatif hospitalier.

Garantir la traçabilité et l’auditabilité des règles et de leurs évolutions.

**5.2 Structuration des politiques**

Cette sous-partie détaille la manière d’organiser les règles selon la criticité des flux et des systèmes.

**5.2.1 Segmentation par criticité**

Règles strictes (blocage IPS) :

Flux Internet entrants.

Interfaces exposées en DMZ.

Accès VPN partenaires.

Règles équilibrées (détection + blocage sélectif) :

Flux inter-VLAN médicaux critiques (DPI, LIMS).

Flux intersites vers PRA.

Règles passives (IDS only) :

Flux internes bas criticité (logs, supervision technique).

Réplications SAN ou backups internes.

**5.2.2 Priorisation des signatures**

Signatures « Critical/High » :

Blocage automatique en IPS.

Alertes prioritaires envoyées au SIEM/SOC.

Signatures « Medium/Low » :

Détection uniquement.

Logs conservés pour analyse ultérieure.

**5.3 Gestion des exceptions et whitelists**

Cette sous-partie précise comment limiter les faux positifs tout en restant sécurisé.

Identification des flux légitimes entre systèmes internes (ex. DPI ↔ Laboratoire).

Maintien d’une liste blanche validée en comité SSI.

Exceptions documentées et justifiées (conservation dans la GED sécurisée).

Revue semestrielle des exceptions pour éviter la dérive ou l’obsolescence.

**5.4 Règles personnalisées et spécifiques métier**

Cette sous-partie insiste sur l’adaptation au contexte hospitalier.

Détection des anomalies sur protocoles médicaux spécifiques :

HL7 (formatage suspect, injection de commande).

DICOM (trafic inhabituel, payload excessif).

Règles spécifiques pour API internes entre applications métier.

Inspection des flux HTTPS internes avec SSL inspection :

Certificats internes gérés en PKI.

Analyse respectueuse de la confidentialité (limitation aux flux métiers identifiés).

**5.5 Mise à jour des signatures**

Cette sous-partie décrit le cycle de vie des signatures et la politique de maintien à jour.

Mises à jour quotidiennes des signatures éditeur (Fortinet, Palo Alto).

Revue hebdomadaire des logs pour identifier des patterns récurrents ou des faux positifs.

Tests sur environnement de préproduction avant déploiement en production des signatures majeures.

Maintien d’un plan de rollback en cas de mise à jour problématique.

**5.6 Journalisation et auditabilité des règles**

Cette sous-partie définit les obligations de traçabilité des changements.

Journalisation automatique des modifications de règles dans la console centralisée.

Enregistrement de l’auteur, date, motif du changement.

Export des logs de configuration vers le SIEM régional.

Revue trimestrielle en comité SSI pour validation des évolutions.

**5.7 Intégration avec le SIEM et le SOC**

Cette sous-partie précise comment les règles alimentent la supervision globale.

Envoi des alertes IPS/IDS au SIEM régional en temps réel (format syslog sécurisé).

Corrélation multi-sources :

Logs AD, firewall, antivirus.

Événements applicatifs (DPI, LIMS).

Scoring des alertes pour priorisation par le SOC.

Playbooks de réponse définis pour alertes critiques (blocage, isolation de segment, forensique).

**5.8 Gouvernance et cycle de vie des règles**

Cette sous-partie décrit le processus de gestion des règles sur la durée.

Définition et validation des règles par le RSSI et la DSI.

Documentation des règles actives dans la GED sécurisée.

Cycle de validation semestrielle des ensembles de règles.

Ajustement permanent en fonction des résultats des tests (Metasploit, Nmap) et des retours d’expérience des incidents.

Sensibilisation et formation des administrateurs réseau sur l’analyse des logs et la gestion des faux positifs.

# 6. Intégration réseau

L’intégration du dispositif IPS/IDS dans l’architecture réseau du CHU Ynov est un enjeu central : elle doit offrir une couverture maximale des flux critiques tout en préservant la performance, la résilience et la continuité de service. Cette section définit les choix techniques de positionnement, d’isolation logique, de redondance et de supervision réseau.

**6.1 Objectifs de l’intégration réseau**

Cette sous-partie précise les finalités stratégiques et opérationnelles de l’intégration.

Permettre la surveillance et la prévention des attaques sur l’ensemble des flux critiques (Internet, DMZ, intersites, intra-VLAN).

Assurer la segmentation entre zones de sécurité différentes (LAN médical, administratif, DMZ).

Garantir la haute disponibilité pour ne pas interrompre les soins même en cas de panne.

Optimiser les performances réseau avec un dimensionnement adapté et des chemins de secours.

Faciliter la maintenance et les évolutions sans refonte majeure.

**6.2 Principes d’architecture réseau**

Cette sous-partie décrit les choix de conception globaux.

Déploiement hybride : combinaison de sondes IPS inline et IDS passives.

Intégration en bridge transparent pour IPS : pas de modification des adresses IP ou du routage.

Utilisation de SPAN/mirroring pour IDS passif : observation des flux sans impact sur la production.

VLAN dédié pour l’administration sécurisée des équipements.

Interconnexion avec les pares-feux, proxies, routeurs et commutateurs cœur.

**6.3 Points d’insertion des capteurs**

Cette sous-partie détaille où seront placés les équipements dans le réseau.

**6.3.1 IPS Inline**

Entre le firewall interne et les switchs cœur pour contrôler les flux Nord-Sud (Internet ↔ LAN).

Sur les liaisons intersites (VPN/PRA) pour contrôler les flux critiques entre datacenters.

En frontal sur la DMZ pour bloquer les attaques avant exposition des portails patients ou services partenaires.

Option fail-open matériel pour garantir le passage du trafic même en cas de panne.

**6.3.2 IDS Passif**

Ports SPAN/mirror configurés sur les switchs cœur.

Surveillance des flux Est-Ouest entre VLAN médicaux.

Observation des flux intra-DC (serveur à serveur) pour détecter mouvement latéral.

Inspection des flux de supervision technique, logs et ordonnancement.

**6.4 Segmentation et isolation logique**

Cette sous-partie explique comment l’IPS/IDS s’inscrit dans la politique de segmentation réseau.

Identification des VLAN médicaux (DPI, imagerie, labo) versus VLAN administratifs.

Mise en place de politiques différenciées (règles strictes sur médicaux, plus souples sur administratifs).

Isolation des interfaces d’administration sur un VLAN sécurisé, limité aux bastions de la DSI.

Chiffrement des flux d’administration (SSH, HTTPS, VPN IPsec entre sites).

**6.5 Résilience et haute disponibilité**

Cette sous-partie décrit les mécanismes techniques garantissant la continuité du service.

Cluster actif/passif ou actif/actif sur les appliances IPS.

Fail-open matériel ou logiciel en cas de panne, pour éviter l’interruption des soins.

Redondance des alimentations électriques (double alimentation secourue).

Liens réseau redondants (double fibre avec bascule automatique).

Supervision de la disponibilité via Zabbix / Centreon, alerting en cas de défaillance.

**6.6 Qualité de service et performance**

Cette sous-partie aborde les aspects de performance réseau.

Dimensionnement des interfaces (1/10/40 Gbps selon segments).

Application de QoS pour prioriser les flux critiques (DPI, prescriptions).

Contrôle de la latence induite : benchmark avant production, validation des temps de passage.

Plan de capacity planning pour anticiper l’évolution du trafic.

**6.7 Sécurité des communications d’administration**

Cette sous-partie précise la sécurisation de l’accès aux consoles et équipements.

Interfaces d’administration isolées sur VLAN dédié, filtré par firewall.

Authentification forte (MFA) obligatoire pour tous les comptes admins.

Journalisation complète des actions d’administration (logs horodatés et signés).

Chiffrement des flux d’administration (SSH, HTTPS avec certificats internes).

**6.8 Intégration avec le PRA**

Cette sous-partie décrit l’alignement avec le Plan de Reprise d’Activité.

Déploiement de sondes IDS passives sur le site PRA.

Réplication des règles et des logs entre site principal et PRA.

Capacité à basculer les flux IPS vers la redondance PRA en cas de sinistre.

Tests annuels de restauration de configuration IPS/IDS sur PRA.

**6.9 Supervision et alerting réseau**

Cette sous-partie précise les dispositifs de surveillance continue.

Intégration des équipements IPS/IDS dans les consoles Zabbix ou Centreon.

Monitoring des états (up/down), CPU/mémoire, bande passante, latence.

Configuration d’alertes multi-niveaux (mail, SMS, webhook) vers DSI et RSSI.

Tableau de bord consolidé dans le SIEM régional pour corrélation globale.

**6.10 Documentation et gouvernance**

Cette sous-partie insiste sur la traçabilité des choix et des évolutions réseau.

Schémas réseau détaillés avec positionnement des capteurs IPS/IDS.

Documentation des ports SPAN configurés et des règles ACL associées.

Conservation des configurations versionnées dans la GED sécurisée.

Revue annuelle du schéma réseau en comité SSI, mise à jour systématique après tout changement majeur.

# 7. Surveillance et alerting

La capacité à surveiller en continu le dispositif IPS/IDS et à recevoir des alertes pertinentes est essentielle pour garantir la détection précoce des incidents et la réactivité des équipes de cybersécurité. Au CHU Ynov, la surveillance et l’alerting doivent être adaptés à la criticité des flux hospitaliers, intégrés dans l’écosystème SIEM/SOC régional, et gouvernés par des procédures formalisées.

**7.1 Objectifs de la surveillance et de l’alerting**

Cette sous-partie rappelle les finalités stratégiques et opérationnelles.

Assurer une visibilité temps réel sur l’ensemble des flux réseau critiques.

Détecter et qualifier toute tentative d’intrusion, qu’elle soit externe ou interne (lateral movement).

Réduire le délai de réaction en alertant immédiatement les équipes concernées.

Garantir la traçabilité et l’auditabilité des événements pour les enquêtes post-incidents.

Contribuer à l’amélioration continue via l’analyse des tendances et des récurrences.

**7.2 Sources de logs et d’événements**

Cette sous-partie décrit la nature des événements collectés.

Alertes IPS (blocages, détections en ligne).

Alertes IDS (détections passives sur flux internes).

Logs système des appliances (authentification, mises à jour).

Journaux d’administration (création/modification des règles).

Données de performance (latence, bande passante, état HA).

Signatures déclenchées (ID, niveau de sévérité, contexte).

**7.3 Niveau de criticité des alertes**

Cette sous-partie détaille la classification des alertes.

Critique : intrusion confirmée ou blocage d’attaque connue → notification immédiate, escalade SOC.

Élevé : tentative d’exploit, comportement fortement suspect → alerte mail/SMS, vérification manuelle.

Moyen : activité anormale, faux positif possible → log détaillé, revue hebdomadaire.

Bas : informationnel → journalisation pour audit et statistique.

**7.4 Intégration avec le SIEM régional**

Cette sous-partie détaille les mécanismes d’intégration.

Export natif des logs IPS/IDS en syslog sécurisé (TCP/TLS) vers le SIEM régional.

Normalisation des données pour corrélation multi-sources (AD, firewall, antivirus).

Enrichissement des alertes (géolocalisation IP, réputation IOC, contexte applicatif).

Tableaux de bord unifiés et filtrés pour les administrateurs CHU et le SOC régional.

**7.5 Dashboards et supervision en temps réel**

Cette sous-partie explique l’interface de pilotage opérationnelle.

Visualisation temps réel des alertes par niveau de criticité.

Cartographie des flux et des capteurs actifs.

Historique des alertes avec filtres multi-critères.

Indicateurs clés de performance :

Taux de détection.

Taux de blocage.

Temps moyen de réponse.

Volume de logs collectés.

**7.6 Alerting automatisé et notifications**

Cette sous-partie précise la gestion des notifications vers les équipes.

Alertes critiques :

Notifications temps réel par email et SMS.

Envoi vers la hotline SOC en astreinte.

Alertes élevées :

Mail de groupe RSSI/DSI.

Enrichissement automatique avec contexte (signature, flux concerné).

Alertes moyennes/basses :

Stockage dans le SIEM.

Intégration aux rapports hebdomadaires.

**7.7 Journalisation et conservation des logs**

Cette sous-partie définit les exigences de traçabilité et de conformité.

Conservation des logs 18 à 24 mois selon la politique PGSSI-S.

Stockage horodaté et signé numériquement pour assurer l’intégrité.

Redondance des journaux sur site PRA ou dans un cloud souverain HDS.

Export régulier des journaux dans la GED sécurisée.

**7.8 Analyse et qualification des alertes**

Cette sous-partie décrit le processus opérationnel de traitement des alertes.

Analyse quotidienne des alertes par les équipes DSI/RSSI.

Qualification des alertes :

Vérification du contexte réseau/applicatif.

Consultation des logs AD ou serveur.

Vérification sur les endpoints (EDR).

Escalade immédiate au SOC régional en cas d’alerte critique confirmée.

Documentation des incidents dans le registre de sécurité.

**7.9 Reporting et indicateurs**

Cette sous-partie précise les rapports générés et partagés.

Rapports hebdomadaires pour la DSI/RSSI :

Nombre d’alertes par criticité.

Fausse alerte / alerte confirmée.

Temps moyen de qualification.

Rapports mensuels consolidés pour le comité SSI :

Tendances et analyses globales.

État des correctifs appliqués.

Plans d’action en cours.

Intégration des indicateurs dans le tableau de bord cybersécurité institutionnel.

**7.10 Gouvernance et amélioration continue**

Cette sous-partie précise le pilotage stratégique.

Règles d’alerting validées par le RSSI en comité SSI.

Revue semestrielle des règles pour réduire faux positifs.

Mise à jour continue des signatures et des politiques d’alerte.

Formation des équipes sur les nouveaux vecteurs de menace.

Intégration des résultats dans le plan d’amélioration continue SSI.

# 8. Processus de réponse aux alertes

Le processus de réponse aux alertes est un élément clé de la stratégie de cybersécurité du CHU Ynov. Il permet de transformer les détections IPS/IDS en actions concrètes, rapides et coordonnées, afin de limiter les impacts, contenir les menaces et préserver la continuité des soins.

Cette section décrit les étapes structurées, les rôles impliqués, les circuits d’escalade et les bonnes pratiques pour garantir un traitement efficace et conforme des alertes de sécurité.

**8.1 Objectifs du processus de réponse**

Cette sous-partie explicite les finalités stratégiques et opérationnelles.

Identifier rapidement les tentatives d’intrusion ou de compromission.

Qualifier et prioriser les alertes selon leur criticité et leur impact potentiel.

Contenir la menace pour éviter la propagation sur le réseau hospitalier.

Eradiquer les causes et corriger les vulnérabilités exploitées.

Maintenir ou rétablir la disponibilité des services critiques pour le soin.

Assurer la traçabilité et respecter les obligations réglementaires (PGSSI-S, RGPD).

**8.2 Chaîne de traitement des alertes**

Cette sous-partie détaille le workflow général des alertes.

**Détection :**

Événement capté par IPS (blocage) ou IDS (alerte passive).

Transmission automatique au SIEM/SOC.

**Notification :**

Envoi immédiat d’alerte selon criticité :

Critique → email/SMS au RSSI/DSI + SOC régional.

Élevée → mail au RSSI/DSI.

Moyenne/basse → stockée pour analyse périodique.

**Qualification :**

Analyse des logs détaillés (flux réseau, AD, serveurs).

Vérification du contexte (équipement concerné, utilisateur, application).

Identification du vrai positif ou faux positif.

**Escalade si nécessaire :**

Transmission au SOC régional pour investigation poussée.

Mobilisation de la cellule de crise SSI en cas d’incident majeur.

**Réponse et remédiation :**

Blocage manuel/automatique des flux suspects.

Isolation du VLAN ou de l’équipement compromis.

Application de correctifs ou mises à jour.

Révocation des accès compromis.

**Clôture et documentation :**

Enregistrement complet de l’incident dans le registre de sécurité.

Rapport d’incident rédigé et archivé dans la GED sécurisée.

Notification CNIL si violation de données personnelles.

**8.3 Qualification des alertes**

Cette sous-partie précise les étapes d’analyse pour distinguer les vrais incidents des faux positifs.

Consultation des journaux réseau : flux concernés, ports/protocoles.

Vérification des logs applicatifs (DPI, LIMS, PACS) pour activité anormale.

Croisement avec logs AD/LDAP : tentatives d’authentification suspectes.

Analyse des postes ou serveurs concernés via outils EDR/antivirus.

Utilisation des IOC (Indicators of Compromise) actualisés.

**8.4 Containment et actions immédiates**

Cette sous-partie décrit les mesures de confinement disponibles.

Blocage automatique via IPS pour les signatures critiques.

Déconnexion manuelle d’un VLAN compromis.

Filtrage ACL d’urgence sur les switchs ou firewalls.

Restriction des accès VPN pour partenaires ou prestataires.

**8.5 Réponse technique et remédiation**

Cette sous-partie détaille les actions pour supprimer la menace et corriger les failles.

Analyse forensique des dumps réseau ou logs.

Suppression des malwares sur serveurs/postes impactés.

Mise à jour des signatures IPS/IDS.

Renforcement des règles firewall ou ACL.

Application des correctifs applicatifs ou OS concernés.

Vérification post-action avec test de non-régression.

**8.6 Coordination et gouvernance**

Cette sous-partie précise les rôles et responsabilités.

DSI : pilotage opérationnel des actions de confinement/remédiation.

RSSI : supervision globale, validation des étapes, communication direction.

SOC régional : investigation avancée, corrélation multi-établissements.

Référents métiers : validation des impacts applicatifs, support aux tests de reprise.

Cellule de crise SSI : mobilisation en cas d’incident majeur (Plan Blanc, PRA).

**8.7 Documentation et traçabilité**

Cette sous-partie garantit la conformité et l’auditabilité.

Création d’un ticket d’incident ou d’une fiche d’alerte dans l’outil ITSM.

Journalisation détaillée des étapes :

Heure de détection.

Analyses réalisées.

Décisions prises.

Mesures correctives appliquées.

Archivage des rapports d’incident dans la GED sécurisée.

Conservation des logs pertinents pendant 18 à 24 mois.

**8.8 Obligations réglementaires et notification**

Cette sous-partie couvre les aspects juridiques.

Notification interne immédiate de la direction en cas d’incident majeur.

Information de l’ARS et de la CNIL sous 72 heures si violation de données personnelles avérée.

Respect des obligations HDS en matière de journalisation et de reporting.

**8.9 Retour d’expérience et amélioration continue**

Cette sous-partie formalise la démarche qualité post-incident.

Organisation de RETEX systématique après incident majeur.

Analyse des causes racines.

Mise à jour des règles IPS/IDS pour réduire les faux négatifs.

Ajustement des procédures et des playbooks de réponse.

Intégration des leçons apprises dans la formation des équipes.

# 9. Tests et validation

Le déploiement et l’exploitation d’un dispositif IPS/IDS au CHU Ynov doivent s’accompagner d’une stratégie formalisée de tests et de validation. Cette section décrit les objectifs, les méthodes, les fréquences, les acteurs et la gouvernance des tests destinés à garantir l’efficacité, la performance et la pertinence des règles de détection/prévention, tout en minimisant les risques opérationnels (faux positifs ou blocages injustifiés).

**9.1 Objectifs des tests IPS/IDS**

Cette sous-partie définit les finalités stratégiques des campagnes de test.

Vérifier l’efficacité réelle des signatures et des règles de blocage/détection.

Valider la capacité de détection de nouveaux vecteurs d’attaque (zero-day, ransomware).

Confirmer la non-régression après mise à jour des signatures ou changements de configuration.

Mesurer l’impact sur la performance réseau (latence, bande passante).

Assurer la compatibilité avec les flux applicatifs hospitaliers critiques.

**9.2 Types de tests planifiés**

Cette sous-partie précise les différents types de tests réalisés.

**9.2.1 Tests unitaires de règles**

Simulation d’attaques spécifiques (exploits connus).

Vérification de la bonne détection / du blocage IPS.

Analyse des logs générés.

**9.2.2 Tests fonctionnels**

Vérification du parcours applicatif complet (DPI, LIMS, PACS).

Validation de la non-interruption des flux métiers.

Tests des flux intersites (VPN vers PRA).

**9.2.3 Tests de charge et de performance**

Simulation de trafic élevé (1/10/40 Gbps selon segments).

Mesure de la latence ajoutée.

Identification des goulots d’étranglement.

**9.2.4 Tests de scénarios réels (Red Team / Blue Team)**

Simulations contrôlées d’attaques internes et externes.

Enchaînement d’étapes (reconnaissance, lateral movement, exfiltration).

Validation des règles d’alerte et des temps de réaction.

**9.3 Outils et environnements de test**

Cette sous-partie décrit les moyens techniques utilisés.

Metasploit Framework pour exploits et payloads connus.

Nmap / NSE pour scans réseau.

Scapy pour tests de création de paquets personnalisés.

Iperf/Spirent pour simulation de bande passante élevée.

Environnements de préproduction ou de bac à sable pour tests à risque réduit.

**9.4 Planification et fréquence**

Cette sous-partie fixe la fréquence et la gouvernance des campagnes de test.

Tests unitaires : après chaque mise à jour majeure des signatures ou des règles.

Tests fonctionnels : trimestriels sur scénarios métiers critiques.

Tests de charge : semestriels ou après évolution du réseau.

Exercices Red Team / Blue Team : annuels, validés en comité SSI.

Intégration des tests IPS/IDS dans les exercices PRA/PCA.

**9.5 Processus de validation**

Cette sous-partie décrit les étapes de validation des résultats.

Plan de test validé en comité SSI avec objectifs et périmètres.

Exécution contrôlée par la DSI et le RSSI.

Analyse des résultats :

Taux de détection / blocage.

Faux positifs / faux négatifs.

Temps de traitement des alertes.

Impact sur performance.

Documentation détaillée dans un rapport de test versionné.

**9.6 Suivi des résultats et plans d’action**

Cette sous-partie précise comment les résultats sont exploités.

Analyse des écarts avec les objectifs fixés.

Identification des causes racines des échecs ou des alertes incorrectes.

Plan d’action technique :

Ajustement des règles.

Ajout de signatures personnalisées.

Optimisation des exceptions/whitelists.

Suivi des actions correctives en comité SSI.

**9.7 Documentation et archivage**

Cette sous-partie garantit la traçabilité et la conformité réglementaire.

Conservation des plans de test et des rapports complets dans la GED sécurisée.

Journalisation des modifications de règles suite aux tests.

Archivage des résultats pour audit interne/externe (HDS, PGSSI-S).

Accès restreint selon la matrice des habilitations SSI.

**9.8 Amélioration continue**

Cette sous-partie formelle la démarche qualité.

Intégration des résultats des tests dans la revue annuelle SSI.

Mise à jour des playbooks de réponse aux incidents en fonction des failles détectées.

Formation des équipes DSI/RSSI sur les nouveaux vecteurs d’attaque et les réponses adaptées.

Collaboration avec le SOC régional pour mutualiser les retours d’expérience et les indicateurs de menace.

# 10. Conformité et gouvernance

La mise en œuvre du dispositif IPS/IDS au CHU Ynov doit s’inscrire dans un cadre réglementaire strict, conforme aux exigences légales, sectorielles et normatives relatives à la sécurité des systèmes d’information traitant des données de santé à caractère personnel.

Cette section détaille les référentiels réglementaires applicables, les exigences spécifiques en matière de journalisation et de sécurité, ainsi que les mécanismes de gouvernance mis en place pour garantir la traçabilité, la cohérence, et l’évolution maîtrisée du dispositif.

**10.1 Objectifs de conformité et de gouvernance**

Cette sous-partie définit les finalités de la démarche.

S’assurer de la conformité réglementaire vis-à-vis des exigences nationales et européennes (PGSSI-S, RGPD, HDS).

Intégrer le dispositif IPS/IDS dans la gouvernance globale de la sécurité du SI hospitalier.

Garantir la traçabilité des décisions, des alertes, et des configurations dans une logique d’auditabilité.

Appuyer la démarche d’amélioration continue de la sécurité (SMSI, ISO 27001, ITIL SSI).

S’assurer que les décisions prises en matière de détection/prévention soient documentées, validées et suivies dans le temps.

**10.2 Référentiels réglementaires applicables**

Cette sous-partie dresse la liste des cadres juridiques et normatifs à respecter.

RGPD (UE 2016/679) : détection des violations de données personnelles, minimisation des données de journalisation, notification sous 72h en cas de compromission.

PGSSI-S (Politique Générale de Sécurité des SI de Santé) :

Volet 3 : surveillance de la sécurité des SI.

Volet 5 : traçabilité, auditabilité, maîtrise des accès.

HDS (Hébergeur de Données de Santé) :

Exigences en matière de détection d’intrusion, gestion des journaux, sécurité des flux réseau.

Code de la Santé Publique (art. L.1111-8) : obligations de sécurisation des données de santé traitées par les SIH.

ISO 27001 / 27002 / 27701 : sécurité des systèmes d’information, gouvernance de la sécurité, protection des données à caractère personnel.

**10.3 Exigences spécifiques de sécurité**

Cette sous-partie présente les obligations précises liées au déploiement IPS/IDS.

Journalisation horodatée et signée de tous les événements de sécurité.

Conservation des logs pendant une durée minimale de 18 mois (voire 24 en cas d'obligation HDS).

Traçabilité complète des actions d’administration (création/modification des règles, accès aux consoles).

Limitation des accès aux journaux et consoles par une politique de contrôle d’accès basée sur le principe du moindre privilège.

Chiffrement des communications (HTTPS, SSH, syslog sécurisé via TLS).

Politique de réversibilité pour restitution des journaux et configuration en cas de changement de fournisseur ou d’arrêt du service.

**10.4 Intégration dans la gouvernance SSI du CHU**

Cette sous-partie explique comment le dispositif s’inscrit dans les instances de sécurité en place.

Comité de pilotage SSI (RSSI, DSI, Direction Générale, représentants métiers) :

Valide les règles critiques, la stratégie de détection, les exceptions.

Supervise les alertes majeures, les incidents, les plans d’action correctifs.

Comité technique SSI :

Se réunit mensuellement pour suivre les indicateurs, les retours du SOC, les incidents IPS/IDS.

Gère les évolutions de configuration, les mises à jour de signature, les tests.

Intégration dans la PSSI institutionnelle comme mesure structurante de sécurité.

**10.5 Responsabilités et rôles**

Cette sous-partie précise la répartition des responsabilités dans le pilotage du dispositif.

Acteur Rôle :

RSSI Supervision globale, conformité, stratégie de surveillance.

DSI Implémentation technique, MCO, supervision des alertes.

SOC régional Analyse avancée, investigation, qualification des événements.

Référents métiers Validation des impacts métier lors de blocage ou test.

Prestataires sécurité Maintenance logicielle, support éditeur, mises à jour de signatures.

**10.6 Documentation et auditabilité**

Cette sous-partie définit les obligations de traçabilité et les pratiques d’audit.

Documentation centralisée dans la GED (règles en vigueur, configurations, exceptions validées).

Historisation des changements dans les consoles d’administration (horodatage, identifiant utilisateur, action réalisée).

Export régulier des rapports d’alerte et d’activité au format exploitable (CSV, PDF, JSON).

Participation aux audits internes SSI et aux audits externes HDS/RGPD.

Tenue à jour du registre des activités de traitement (conformément à l'article 30 du RGPD).

**10.7 Mises à jour, contrôles et revue**

Cette sous-partie précise les cycles de révision.

Revue semestrielle des règles IPS/IDS par le comité technique SSI.

Audit annuel de conformité du dispositif dans le cadre du SMSI (ou Plan Directeur SI).

Mise à jour après :

Évolution réglementaire ou normative.

Incidents critiques ou faux positifs récurrents.

Modification du périmètre fonctionnel ou technique (nouvelle application métier, migration, refonte réseau).

**10.8 Politique de confidentialité et données personnelles**

Cette sous-partie encadre les enjeux RGPD liés à la journalisation.

Les logs collectés ne doivent contenir que les données strictement nécessaires à la détection d’incidents.

Application de la minimisation et du principe de finalité.

Analyse d’impact (AIPD/PIA) réalisée pour le traitement des logs contenant des identifiants personnels (IP, login utilisateur).

Accès restreint aux journaux contenant des données personnelles : uniquement personnel habilité RSSI/SOC.

**10.9 Coordination avec le GHT et le SI régional**

Cette sous-partie précise les interfaces avec les dispositifs mutualisés.

Alignement du dispositif local IPS/IDS avec la politique de cybersurveillance du GHT.

Intégration au SIEM mutualisé régional pour partage des alertes et détection multi-établissement.

Participation aux exercices régionaux de réponse à incident.

Harmonisation des playbooks de réponse, des niveaux d’alerte et des flux d’information avec les hôpitaux partenaires.

# 11. Formation et sensibilisation

Le déploiement et l’exploitation efficaces d’un dispositif IPS/IDS au CHU Ynov exigent une montée en compétence structurée et continue des équipes techniques et des acteurs concernés. La réussite du projet dépend non seulement de la technologie, mais aussi de la capacité des personnes à l’administrer, à l’exploiter correctement et à intégrer ses alertes dans les processus de cybersécurité globaux.

Cette section formalise les objectifs pédagogiques, les publics visés, les contenus de formation, les modalités de sensibilisation et le pilotage global de ce volet stratégique.

**11.1 Objectifs stratégiques de la formation et de la sensibilisation**

Cette sous-partie décrit les buts généraux du programme de formation.

Permettre une exploitation efficace et sécurisée des outils IPS/IDS.

Réduire les erreurs humaines dans l’administration des règles, la gestion des alertes et la réaction aux incidents.

Renforcer la posture globale de cybersécurité du CHU via une approche défense en profondeur cohérente.

Favoriser la transversalité entre équipes DSI, RSSI, métiers et partenaires externes.

Satisfaire aux exigences de conformité (PGSSI-S, HDS, RGPD) en matière de compétence du personnel et de sensibilisation.

**11.2 Publics et cibles de la formation**

Cette sous-partie précise les groupes d’acteurs visés, avec une segmentation des niveaux de besoin.

Administrateurs réseau et systèmes DSI : paramétrage des règles IPS/IDS, supervision quotidienne, intégration réseau.

RSSI et équipe SSI : gouvernance des règles, suivi des alertes critiques, auditabilité.

Équipe SOC régional (partenaire GHT) : corrélation intersites, qualification avancée des alertes.

Référents métiers (DPI, LIMS, pharmacie) : compréhension des impacts métiers des blocages ou exceptions.

Direction Générale / DAF / Comité SSI : sensibilisation stratégique aux enjeux et arbitrages.

11.3 Contenus pédagogiques

Cette sous-partie détaille les thématiques de formation proposées.

**11.3.1 Formation technique avancée**

Concepts IPS vs IDS.

Administration des consoles Fortinet, Palo Alto, Suricata/Snort.

Gestion des politiques et des signatures.

Déploiement en mode inline / passif (SPAN/mirroring).

Inspection SSL/TLS et enjeux de confidentialité.

**11.3.2 Analyse des alertes et SOC**

Qualification des événements.

Réduction des faux positifs.

Corrélation avec les logs SIEM.

Escalade et notification des incidents critiques.

**11.3.3 Gouvernance et conformité**

Exigences PGSSI-S et HDS sur la surveillance réseau.

Journalisation, horodatage, conservation des logs.

RGPD et minimisation des données personnelles dans les logs.

Auditabilité et documentation des règles.

**11.3.4 Scénarios pratiques**

Exercices sur alertes réelles ou simulées.

Playbooks de réponse en cas d’incident.

Cas de blocage IPS justifié ou faux positif impactant le soin.

**11.4 Modalités de formation**

Cette sous-partie formalise les formats pédagogiques retenus.

Sessions présentielles ou distancielles animées par l’éditeur ou un prestataire qualifié.

Ateliers pratiques en environnement de préproduction ou bac à sable.

MOOC/vidéos internes pour révision autonome.

Guide d’administration et documentation versionnée.

Fiches réflexes pour les gestes critiques (blocage/déblocage, export de logs).

**11.5 Sensibilisation des autres publics**

Cette sous-partie décrit la démarche de sensibilisation plus large.

Sessions de sensibilisation SSI pour les cadres de santé et responsables de services cliniques :

Impact potentiel des blocages IPS sur le DPI et les applications métiers.

Importance de la coordination DSI/métiers en cas d’incident.

Formation courte pour prestataires partenaires (VPN, maintenance) :

Explications des contrôles IPS/IDS sur leurs accès.

Engagement sur la sécurité des flux.

**11.6 Planification et calendrier**

Cette sous-partie fixe les engagements et la temporalité.

**Formation initiale avant mise en production :**

2 jours minimum pour administrateurs réseaux.

1 journée pour RSSI / équipe SSI.

Sensibilisation courte (2h) pour métiers et direction.

Formations de recyclage / mise à jour :

Semestrielles ou annuelles selon évolutions des outils.

Après toute mise à jour majeure des signatures ou changement d’architecture.

Intégration au plan de formation global DSI.

**11.7 Documentation et supports**

Cette sous-partie détaille la production documentaire associée.

Guide d’administration IPS/IDS validé et versionné.

Procédures opérationnelles (création règles, export logs, intégration SIEM).

Playbooks de réponse aux alertes.

Présentations et supports pédagogiques archivés dans la GED sécurisée.

Historisation des participants aux sessions pour audit interne.

**11.8 Gouvernance et pilotage**

Cette sous-partie formalise le pilotage du programme.

Pilotage par le RSSI, en lien avec la DSI et la DRH formation.

Validation des contenus par le comité technique SSI.

Suivi du taux de couverture (pourcentage des équipes formées).

Intégration des retours d’expérience dans l’adaptation des formations.

**11.9 Suivi et amélioration continue**

Cette sous-partie insiste sur l’aspect itératif et évolutif.

Évaluation des sessions (questionnaires de satisfaction, quiz de validation).

Analyse des incidents ou alertes mal traitées pour identifier des besoins de formation supplémentaires.

Intégration des évolutions réglementaires (PGSSI-S, HDS, RGPD) dans le contenu pédagogique.

Mise à jour annuelle du plan de formation SSI dans le cadre du SMSI.

# 12. Amélioration continue

Le déploiement d’un dispositif IPS/IDS ne doit jamais être figé : face à l’évolution constante des menaces, des infrastructures, des usages métiers et des exigences réglementaires, il est indispensable d’inscrire ce dispositif dans une démarche formalisée et structurée d’amélioration continue.

Cette section décrit les objectifs, les processus, les acteurs et les livrables qui encadrent l’amélioration progressive et itérative de la stratégie IPS/IDS au CHU Ynov.

**12.1 Objectifs stratégiques de l’amélioration continue**

Cette sous-partie définit la finalité globale du dispositif.

Adapter en permanence la détection/prévention aux nouvelles menaces (APT, ransomware ciblés, exploits zero-day).

Améliorer la pertinence des alertes (réduction des faux positifs / faux négatifs).

Suivre l’évolution du SI hospitalier (nouveaux VLAN, applications, migrations cloud).

Aligner la configuration IPS/IDS sur les changements réglementaires ou contractuels (HDS, RGPD, PGSSI-S).

Renforcer la compétence des équipes par l’analyse des incidents et la capitalisation sur les retours d’expérience.

**12.2 Cycle d’amélioration continue**

Cette sous-partie formalise la méthode cyclique retenue, calquée sur le PDCA (Plan-Do-Check-Act).

**12.2.1 Plan**

Identification des risques émergents (veille cyber, CERT Santé, ANSSI).

Recensement des évolutions SI (nouveaux flux, nouvelles applications).

Définition d’objectifs d’amélioration (réduction faux positifs, couverture accrue).

**12.2.2 Do**

Implémentation des nouvelles signatures ou règles personnalisées.

Mise à jour des configurations (whitelists, inspection SSL).

Formation des équipes sur les changements apportés.

**12.2.3 Check**

Analyse des métriques : taux de détection, faux positifs, temps de réponse.

Revue des incidents récents et des tickets SOC.

Vérification de la couverture réseau effective des sondes IPS/IDS.

**12.2.4 Act**

Ajustement des règles, signatures et politiques.

Planification des évolutions techniques (mise à jour appliance, ajout de capteurs).

Intégration des résultats dans la PSSI, le SMSI et le Plan Directeur SI.

**12.3 Indicateurs de suivi**

Cette sous-partie précise les métriques surveillées pour piloter la qualité.

Taux de succès des détections critiques.

Nombre de faux positifs qualifiés.

Temps moyen de qualification des alertes par la DSI/SOC.

Temps moyen de réponse/containment.

Couverture réseau effective (%) des flux critiques.

Nombre de règles obsolètes ou inutilisées identifiées et retirées.

**12.4 Revues périodiques**

Cette sous-partie formalise la gouvernance régulière.

Revue trimestrielle technique :

Avec DSI/RSSI/SOC.

Analyse des logs et alertes.

Mise à jour des whitelists/blacklists.

Revue semestrielle stratégique :

En comité SSI.

Analyse des tendances.

Ajustement des priorités métier.

Évaluation de l’impact réglementaire.

Revue annuelle :

Alignement avec le SMSI et le Plan Directeur SI.

Bilan des formations effectuées.

Plan d’amélioration formalisé.

**12.5 Gestion des mises à jour et correctifs**

Cette sous-partie décrit la politique de maintien technique.

Mises à jour hebdomadaires des signatures (éditeurs ou communauté).

Tests de non-régression en préproduction.

Planification des mises à jour firmware/OS des appliances en fenêtre de maintenance validée.

Rétention des anciennes configurations pour rollback.

Documentation des changements dans la GED sécurisée.

**12.6 Capitalisation sur les incidents et retours d’expérience**

Cette sous-partie précise l’exploitation des incidents réels.

Analyse détaillée des incidents bloqués ou passés inaperçus.

Identification des causes racines (erreur de configuration, lacune dans la signature).

Ajustement immédiat des règles pour éviter la répétition.

Documentation des RETEX dans le registre SSI.

Partage des leçons apprises avec les autres établissements du GHT via le SOC régional.

**12.7 Implication des acteurs**

Cette sous-partie décrit la gouvernance humaine de l’amélioration.

RSSI : garant de la stratégie d’amélioration continue.

DSI : mise en œuvre technique, supervision des mises à jour.

SOC régional : détection avancée, conseil en signature, corrélation multi-sites.

Référents métiers : validation des impacts applicatifs (éviter les blocages injustifiés).

Comité SSI : validation des priorités et des arbitrages budgétaires.

**12.8 Documentation et auditabilité**

Cette sous-partie précise la traçabilité des évolutions.

Versionnage des configurations IPS/IDS.

Archivage des résultats de tests et de revues dans la GED sécurisée.

Historisation des décisions du comité SSI.

Préparation des éléments pour audits internes/externe (HDS, RGPD).

Alignement avec le registre de traitement des données personnelles.

**12.9 Alignement avec le SMSI et le Plan Directeur SI**

Cette sous-partie veille à la cohérence globale.

Intégration des plans d’action issus des revues dans le SMSI institutionnel.

Mise à jour des politiques de sécurité (PSSI) en conséquence.

Alignement avec le PCA/PRA pour garantir la reprise de la capacité de détection après sinistre.

Contribution aux plans directeurs numériques hospitaliers.