

MODELE
STORMSHIELD – outil de sécurisation du poste de travail

Date de mise en œuvre	Mars 2015
Finalité principale	Afin de renforcer la sécurité du poste de travail (en dehors des locaux et dans le cadre du télétravail) en complément de l'offre existante et de protéger les données hautement sensibles que l'Assurance Maladie et la CNAMTS détiennent, la CNAMTS dispose d'un outil de protection, STORMSHIELD. Ce serveur assure une protection contre les accès illégitimes au réseau, les tentatives d'attaques inconnues, l'utilisation illégitime des applications.
Service chargé de la mise en œuvre	CNAMTS / Direction des maîtrises d'ouvrage métier / Département études, conception, sécurité des environnements de travail
Catégories de personnes concernées par le traitement	Agents de l'organisme de l'Assurance Maladie
Catégories des données traitées	<p><u>Les logs Agent</u></p> <ul style="list-style-type: none"> - Date et identification agent : date, heure, nom utilisateur, code agent. - PMF : nom de la machine, adresse IP, nom ADN du poste. - Données Stormshield : identifiant interne Stormshield, type d'enregistrement, actions effectuées, détail de l'action effectuée. <p><u>Les logs Réseau</u></p> <ul style="list-style-type: none"> - Date et identification agent : date, heure, nom utilisateur, code agent. - PMF : nom de la machine, adresse IP, nom ADN du poste. - Données Stormshield : identifiant interne Stormshield, action réseau du PMF, sens de l'action réseau, résultat de l'action, adresse de contact du PMF, N° port, statuts fonctionnels de l'agent Stormshield. <p><u>Les logs Serveurs</u></p> <ul style="list-style-type: none"> - Date et identification agent : date, heure, nom utilisateur, code agent. - PMF : nom de la machine, adresse IP, nom ADN du poste. - Données Stormshield : identifiant interne Stormshield, action du programme sur PMF, avertissement, action, adresse IP de destination, N° port, statuts fonctionnels de l'agent Stormshield.
Destinataire des données	Personnel habilité de l'organisme de l'Assurance Maladie CRIP et administrateurs locaux
Droit d'accès	Le Directeur de l'organisme
Durée de conservation	Les enregistrements sont stockés d'une part sur des serveurs et d'autre part sur les PMF pendant une durée de 30 jours correspondant au délai minimum permettant d'analyser avec suffisamment de recul les dysfonctionnements. Une fois ce temps écoulé, les données sont supprimées.
	Les fichiers logs enregistrés permettent d'analyser les comportements anormaux des postes de travail et n'ont pas pour finalité le contrôle de l'activité de l'agent.