Clearlane CRA

Protocole de qualification opérationnelle (OQ)

À dérouler dans un projet Jira de test, avec au moins deux utilisateurs de test. Noter la version de l'appli (Gérer les applis) et votre site avant de commencer. Joindre une capture à chaque test. Utilisateur A : administrateur Jira (toujours dans l'équipe sécurité). Utilisateur B : second utilisateur de test, hors équipe sécurité, qui peut parcourir et modifier le projet de test. Clearlane CRA aide à répondre aux obligations de signalement du Cyber Resilience Act (article 14, applicables depuis le 11 septembre 2026) ; l'appli n'envoie rien à la plateforme unique de signalement de l'ENISA.

Version de l'appli	
Site	
Exécuté par	
Date	
Approuvé par	

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
OQ-01 Réglages et mot de passe de signature	En tant qu'utilisateur A (administrateur Jira), ouvrir Applications › Clearlane CRA › « Réglages ». Sous « Fabricant », renseigner « Nom », « Site web (https) » et « Contact sécurité » ; laisser cochée la case des rappels (« Envoyer à chaque responsable un seul e-mail de rappel par jour… ») ; sous « Règles du mot de passe de signature », mettre « Essais avant blocage » à 3 et « Blocage (minutes) » à 5 ; cliquer sur « Enregistrer ». Dans « Mot de passe de signature », saisir un mot de passe de 7 caractères dans « Nouveau mot de passe » et cliquer sur « Enregistrer le mot de passe », puis un mot de passe de 8 caractères ou plus.	« Réglages enregistrés » s'affiche. Le mot de passe de 7 caractères est refusé avec « Mot de passe trop court. » ; le second est accepté (« Enregistré ») et « Changer le mot de passe » est proposé. L'utilisateur B (ni administrateur Jira, ni nommé dans « Équipe sécurité ») n'a pas d'onglet « Réglages ».		
OQ-02 Enregistrer un produit et sa période de support	Dans « Produits », cliquer sur « Ajouter un produit » : « Nom du produit » = Gateway Console, « Type » = Logiciel, « Classe CRA » = Par défaut, aucun État membre coché ; cliquer sur « Enregistrer ». Cliquer ensuite sur « Les 27 », ajouter le projet de test dans « Projets Jira » et cliquer sur « Enregistrer ». Dans le produit, cliquer sur « Ajouter une version » : « Version » = 2.4.1, « Sur le marché depuis » = il y a un an, laisser « Support jusqu'au » proposé, cliquer sur « Enregistrer ». Ajouter la version 2.4.0 avec « Support jusqu'au » deux ans après sa mise sur le marché et cliquer sur « Enregistrer » ; puis remplir « Pourquoi une période de support plus courte » et cliquer de nouveau sur « Enregistrer ».	Sans État membre, l'enregistrement est refusé avec « Des champs manquent ou ne sont pas valides. (États membres) ». Pour 2.4.1, « Support jusqu'au » est proposé cinq ans après la mise sur le marché (« Proposé : 5 ans après la mise sur le marché. ») et le statut est « Supportée ». La version 2.4.0 est refusée tant que la raison manque (« raison d'un support plus court »), puis enregistrée avec elle. Les deux versions affichent « Pas de SBOM ».		
OQ-03 Importer un SBOM et chercher	Sur la version 2.4.1, cliquer sur « Importer le SBOM » et déposer un SBOM exporté en XML. Puis, avec « choisissez un fichier », sélectionner un SBOM	Le fichier XML est refusé avec « C'est un fichier XML. Exportez le SBOM en JSON (CycloneDX ou SPDX). ». Le fichier JSON est lu : format, version et		

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
un composant	CycloneDX (1.x) ou SPDX (2.x ou 3.0) en JSON de cette version contenant lodash 4.17.20, et cliquer sur « Enregistrer ce SBOM ». Ouvrir le SBOM avec « Voir » et taper lodash dans « Filtrer les composants… ». Dans « Produits », sous « Quels produits contiennent… », taper lodash < 4.17.21 et cliquer sur « Rechercher ». Sous « Historique de ce produit », cliquer sur « Afficher ».	nombre de composants (par exemple « CycloneDX 1.5 · 312 composants (25 directs) »), nom et taille du fichier, produit décrit (avertissement s'il décrit une autre version) ; « SBOM enregistré : N composants » s'affiche. La vue du SBOM liste lodash avec sa version, son type et « Direct », et affiche le « SHA-256 du fichier ». La recherche renvoie « 1 résultat dans 1 version » (Gateway Console 2.4.1) marqué « Dans la plage », avec « Ouvrir un dossier pour 1 version ». L'historique affiche « SBOM importé » avec version, format et nombre.		
OQ-04 Ouvrir un dossier depuis un ticket	Dans le projet de test, créer un ticket de résumé « [Snyk] High severity - Prototype Pollution in lodash » et de description « CVE-2020-8203. Vulnerable versions: < 4.17.21 ». Ouvrir son panneau « CRA » et cliquer sur « Ouvrir un dossier ». Sous « Produits et versions concernés », cliquer sur « Les ajouter » (ou choisir 2.4.1 à la main) ; garder « Responsable » = utilisateur A ; cliquer sur « Ouvrir le dossier ». Recharger le ticket.	Le panneau propose « Ouvrir un dossier CRA sur [clé] » et le formulaire affiche « Lu dans le ticket Snyk : vérifiez avant d'enregistrer. », avec « Titre », « Identifiants » (CVE-2020-8203), « Gravité » Élevée, « Composant » lodash et « Versions vulnérables » < 4.17.21 prérempli, « 1 version contient ce composant : Gateway Console 2.4.1 », et une « Date cible du correctif » avec « Proposée : 30 jours pour cette gravité. ». « CRA-0001 ouvert » s'affiche ; le panneau montre le dossier à l'étape « Qualification » avec « À qualifier » et ne propose plus d'en ouvrir un autre. « Vulnérabilités » liste CRA-0001.		
OQ-05 Qualifier, signer et démarrer les horloges	En tant qu'utilisateur A, sur CRA-0001 sous « Qualification » : « Les produits listés sont-ils affectés ? » = « Affectés » ; « Est-elle activement exploitée ? » = « Oui » ; dans « Quand en avez-vous eu connaissance ? », saisir une date et une heure 30 heures avant maintenant ; remplir « Pourquoi » ; cliquer sur « Qualifier et signer ». Lire la déclaration, saisir le bon mot de passe dans « Mot de passe de signature » et cliquer sur « Signer ».	Avant la signature, « À signaler au titre de l'article 14 : les horloges démarrent. » s'affiche et l'aide indique Alerte précoce = connaissance + 24 h et Notification = connaissance + 72 h. Après la signature, la qualification affiche la signature : le nom de l'utilisateur A, « Qualification », la date et l'heure, la déclaration « Je qualifie CRA-0001 de vulnérabilité activement exploitée dans les produits listés. Elle est signalée au titre de l'article 14 du Cyber Resilience Act. » et l'empreinte SHA-256. Trois horloges apparaissent : « Alerte précoce » « En retard » (échéance connaissance + 24 h, avec l'heure UTC), « Notification » « En cours » (échéance connaissance + 72 h, environ 42 h restantes), « Rapport final » « Pas encore » (« Démarre quand le correctif ou l'atténuation est disponible. »). L'« Historique » affiche « Qualifié (signé) · Art. 14 ».		
OQ-06 Mauvais mot de passe de signature et blocage	Sur CRA-0001, cliquer sur « Requalifier », garder les réponses, écrire un nouveau « Pourquoi » et cliquer sur « Qualifier et signer ». Cliquer sur « Signer » avec un mauvais mot de passe deux fois, puis une troisième fois ; puis avec le bon mot de passe. Attendre 5 minutes (le blocage réglé au test 1) et signer de nouveau avec le bon mot de passe.	Les deux premiers essais affichent « Mot de passe de signature incorrect. » et rien n'est enregistré. Le troisième affiche « Signature bloquée quelques minutes après trop d'essais. », et le bon mot de passe est refusé avec le même message tant que dure le blocage. Après 5 minutes, la signature est acceptée : l'« Historique » affiche « Requalifié (signé) · Art. 14 », la qualification affiche « 1 qualification antérieure », et les trois échéances sont inchangées.		
OQ-07 Champs ENISA et signalements enregistrés comme envoyés	Sur CRA-0001, sous « Signalement à l'ENISA », ouvrir l'onglet « Notification », puis l'onglet « Alerte précoce ». Vérifier les champs obligatoires, ouvrir « + … champs facultatifs », modifier « Summary » et cliquer sur « Enregistrer le texte ». Cliquer sur « Copier » sur un champ puis sur « Copier tous les champs », et coller dans un éditeur de texte. Mettre « Envoyé sur la plateforme le » à maintenant, remplir « Référence de la plateforme » et cliquer sur « Enregistrer l'envoi ». Enregistrer la « Notification » de la même façon. Cliquer sur « Voir le texte envoyé ».	Avant l'enregistrement de l'alerte précoce, l'onglet Notification affiche « Enregistrez d'abord l'alerte précoce. ». Les champs obligatoires portent les libellés de l'ENISA (en anglais) et sont préremplis à partir du dossier et du produit : « Notification type » (Vulnerability), « Title », « Summary », « Member States where the product is available », « Product name », « Product version » (2.4.1) et « Date and time when you become aware (UTC) » ; chacun affiche caractères utilisés / limite. « Texte enregistré » s'affiche ; le texte collé contient chaque libellé et sa valeur. Après l'enregistrement : « Envoyé le [date heure] ([UTC]) · enregistré par utilisateur A · [référence] » avec « … de retard »		

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
		pour l'alerte précoce et « dans les délais » pour la notification, et une empreinte SHA-256 ; les horloges affichent « Envoi tardif » et « Envoi fait ». L'« Historique » affiche « Signalement envoyé · Alerte précoce (envoi tardif) » et « Signalement envoyé · Notification » ; « Voir le texte envoyé » montre exactement les champs enregistrés.		
OQ-08 Correctif, rapport final et utilisateurs informés	Sur CRA-0001, ouvrir l'onglet « Rapport final ». Sous « Correctif ou atténuation », cliquer sur « Enregistrer le correctif » : « Ce qui est disponible » = « Mise à jour de sécurité », « Version corrigée » = 2.4.2, « Disponible pour les utilisateurs depuis » = maintenant, remplir « Ce que ça change » et « Lien pour les utilisateurs », cliquer sur « Enregistrer le correctif ». Sans quitter l'onglet « Rapport final », regarder « Date when corrective or mitigating measure has been available » et « Details about the security update or corrective measure available ». Remplir seulement « Date and time when it occurred (UTC) », en laissant « Full description of the impact » vide, et regarder « Enregistrer l'envoi » ; puis remplir « Full description of the impact » et cliquer sur « Enregistrer l'envoi ». Sous « Utilisateurs et avis de sécurité » > « Utilisateurs informés », cliquer sur « Enregistrer », remplir « Informés le » et « Comment », lire « Ce qui leur a été dit », cliquer sur « Enregistrer ».	Avant le correctif, l'onglet Rapport final affiche « Enregistrez d'abord le correctif : le rapport final le décrit. ». Ensuite : « Correctif enregistré », étape « Divulgation », et l'horloge « Rapport final » échoit exactement 14 jours après « Disponible pour les utilisateurs depuis » ; dans l'onglet ouvert, les champs tirés du correctif se remplissent aussitôt (la date en UTC, « Version 2.4.2. … »). Tant qu'un champ obligatoire est vide, « 1 champ obligatoire est vide ou trop long. » s'affiche et « Enregistrer l'envoi » reste grisé (un signalement avec un champ obligatoire vide est aussi refusé par le serveur de l'appli). Une fois l'envoi enregistré, l'horloge affiche « Envoi fait » et le correctif affiche « Le rapport final a été envoyé avec ce correctif : il ne peut plus changer. » (plus de « Modifier »). « Ce qui leur a été dit » est prérempli avec le produit, la version, « Mettez à jour vers la version 2.4.2 ou ultérieure. » et le contact sécurité ; l'enregistrement affiche la date, le canal et « enregistré par utilisateur A ». L'« Historique » affiche « Correctif disponible », « Signalement envoyé · Rapport final » et « Utilisateurs informés ».		
OQ-09 Horloges d'un incident grave et rappel au responsable	En tant qu'utilisateur A, cliquer sur « Nouveau dossier » : « Type » = « Incident », « Ticket » = « En créer un » (projet de test, « Type de ticket » au choix), remplir « Titre » et « Ce que l'on sait », choisir Gateway Console 2.4.1, « Responsable » = utilisateur B ; cliquer sur « Ouvrir le dossier ». Qualifier : « Affectés », « L'incident est-il grave ? » = « Oui », « Est-il soupçonné de venir d'actes illicites ou malveillants ? » = « Inconnu », connaissance il y a 30 heures, « Pourquoi » ; signer. N'enregistrer aucun signalement. Le lendemain après 9 h UTC, vérifier la boîte mail de l'utilisateur B et l'« Historique » du dossier. Puis, en tant qu'utilisateur B, enregistrer l'« Alerte précoce » et la « Notification » comme envoyées maintenant.	Avant l'enregistrement de la notification, l'horloge « Rapport final » affiche « Pas encore » (« Démarre à l'envoi de la notification. ») ; les champs de l'alerte précoce comprennent « Incident is suspected of unlawful or malicious acts » = Unknown. L'utilisateur B reçoit un seul e-mail de Jira, « Clearlane CRA : 1 dossier vous attend », qui cite le dossier avec « Alerte précoce en retard depuis le [date] UTC » et un lien ; rien n'est publié sur le ticket, et aucun second rappel n'arrive ce jour-là. L'« Historique » affiche « E-mail de rappel envoyé · alerte précoce en retard ». Après l'enregistrement de la notification, le rapport final échoit exactement un mois calendaire après l'heure d'envoi de la notification.		
OQ-10 Avis de sécurité CSAF	Sur CRA-0001, sous « Utilisateurs et avis de sécurité » > « Avis de sécurité », choisir « FR » dans « Langue de l'avis » et cliquer sur « Aperçu ». Cliquer sur « Enregistrer une publication », remplir « Ce qui change » et « Où il est publié », cliquer sur « Enregistrer la publication », puis sur « Télécharger le fichier CSAF ». Ouvrir les pièces jointes du ticket et le fichier téléchargé (éventuellement dans un validateur CSAF 2.0).	L'aperçu affiche le produit et les versions concernés, la version corrigée, la gravité, les identifiants, « Cette vulnérabilité est activement exploitée. », que faire et le contact. « Révision 1 publiée le [date] · Joint à [clé] » s'affiche ; le ticket a la pièce jointe cra-0001.json ; la ligne de révision affiche le résumé, l'URL, l'utilisateur A et une empreinte SHA-256. Le fichier est un avis de sécurité CSAF 2.0 (« csaf_version » : « 2.0 », identifiant de suivi CRA-0001, éditeur = nom et site web du fabricant) qui donne 2.4.1 comme affectée et 2.4.2 comme corrigée, un correctif éditeur et le statut d'exploitation. L'« Historique » affiche « Avis publié ».		
OQ-11 Droits d'accès	En tant qu'utilisateur A, cliquer sur « Nouveau dossier », choisir « Utiliser un ticket existant », choisir un ticket d'un projet que l'utilisateur B ne peut pas parcourir et cliquer sur « Ouvrir le dossier ». En tant qu'utilisateur B (hors équipe sécurité), ouvrir Applications > Clearlane CRA > « Vulnérabilités »,	L'utilisateur B ne voit pas le dossier du ticket masqué : il n'est pas listé et la recherche affiche « Aucun dossier ne correspond à ces filtres. ». Sur CRA-0001, l'utilisateur B voit « Lecture seule : le responsable et l'équipe sécurité modifient ce dossier. », sans « Requalifier », sans « Clôturer et signer » et sans		

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
	choisir « Tous » et taper le numéro de ce dossier dans le champ de recherche. En tant qu'utilisateur B, ouvrir CRA-0001 puis « Produits ».	champ modifiable. Dans « Produits », l'utilisateur B n'a pas « Ajouter un produit » et voit « Les SBOM ne sont visibles que par l'équipe sécurité. ».		
OQ-12 Clôture, dossier de preuve et piste d'audit	En tant qu'utilisateur A, sur CRA-0001, vérifier la liste « Clôture », cliquer sur « Clôturer et signer », remplir « Remarque » et signer avec le bon mot de passe. Cliquer sur « Dossier de preuve (PDF) » et ouvrir le fichier. Cliquer sur « Joindre le PDF au ticket ». Dans « Historique », cliquer sur « Tout afficher ».	Chaque élément de la liste est coché (« Correctif ou atténuation », « Alerte précoce », « Notification », « Rapport final », « Utilisateurs informés », « Avis publié (ou report enregistré) »). Après la signature : « Corrigé · clôturé le [date] », et la signature de clôture affiche le nom, « Clôture », la date et l'heure, la déclaration « Je confirme que le traitement de CRA-0001 est complet tel qu'enregistré : mesure corrective ou d'atténuation, signalements, information des utilisateurs et avis de sécurité. Je clôture ce dossier. » et son empreinte SHA-256 ; plus rien n'est modifiable. Le PDF « Dossier de preuve CRA » contient les données du dossier, les produits et versions avec mise sur le marché, fin de support et États membres, la qualification, chaque signalement (échéance et envoi en UTC, référence, délai, empreinte SHA-256, texte envoyé), le correctif, les utilisateurs informés, les révisions de l'avis, les signatures électroniques, les pièces jointes du ticket et la piste d'audit, avec « Généré le … par … · Clearlane CRA » et la numérotation des pages. « Joint à [clé] » s'affiche. L'« Historique » liste chaque étape enregistrée sur CRA-0001 (tests 4 à 8, 10 et 12) avec date, heure et personne ; aucune entrée ne peut être modifiée ni supprimée.		