Clearlane CRA

Skript zur Funktionsqualifizierung (OQ)

In einem Test-Projekt in Jira mit mindestens zwei Testbenutzern durchführen. Vor Beginn die App-Version (Apps verwalten) und Ihre Site notieren. Jedem Test einen Screenshot beifügen. Diese Fassung zitiert die Bezeichnungen der englischen Oberfläche: Stellen Sie die Sprache von Jira für den Test auf Englisch. Benutzer A: Jira-Administrator (immer im Sicherheitsteam). Benutzer B: zweiter Testbenutzer, nicht im Sicherheitsteam, der das Testprojekt einsehen und bearbeiten kann. Clearlane CRA unterstützt Sie bei den Meldepflichten des Cyber Resilience Act (Artikel 14, gültig seit dem 11. September 2026); die App übermittelt nichts an die zentrale Meldeplattform der ENISA.

App-Version	
Site	
Durchgeführt von	
Datum	
Freigegeben von	

Test	Schritte	Erwartetes Ergebnis	Ergebnis (bestanden / nicht bestanden)	Tester, Datum
OQ-01 Einstellungen und Signaturpasswort	Als Benutzer A (Jira-Administrator) Apps > Clearlane CRA > „Settings“ öffnen. Unter „Manufacturer“ „Name“, „Website (https)“ und „Security contact“ ausfüllen; das Erinnerungskästchen („Send each case owner one reminder e-mail a day…“) angekreuzt lassen; unter „Signing password policy“ „Attempts before lock“ auf 3 und „Lock (minutes)“ auf 5 setzen; auf „Save“ klicken. In „Signing password“ ein Passwort mit 7 Zeichen in „New password“ eingeben und auf „Save the password“ klicken, dann ein Passwort mit 8 oder mehr Zeichen.	„Settings saved“ erscheint. Das Passwort mit 7 Zeichen wird mit „The password is too short.“ abgewiesen; das längere wird angenommen („Saved“), und „Change the password“ wird angeboten. Benutzer B (kein Jira-Administrator, nicht in „Security team“ genannt) hat keinen Tab „Settings“.		
OQ-02 Ein Produkt und seinen Supportzeitraum erfassen	In „Products“ auf „Add a product“ klicken: „Product name“ = Gateway Console, „Type“ = Software, „CRA class“ = Default, kein Mitgliedstaat ausgewählt; auf „Save“ klicken. Dann auf „All 27“ klicken, das Testprojekt in „Jira projects“ hinzufügen und auf „Save“ klicken. Im Produkt auf „Add a version“ klicken: „Version“ = 2.4.1, „On the market since“ = vor einem Jahr, „Support until“ wie vorgeschlagen belassen, auf „Save“ klicken. Version 2.4.0 mit „Support until“ zwei Jahre nach ihrem Datum des Inverkehrbringens hinzufügen und auf „Save“ klicken; dann „Why a shorter support period“ ausfüllen und erneut auf „Save“ klicken.	Ohne Mitgliedstaat wird das Speichern mit „Some fields are missing or not valid. (Member States)“ abgewiesen. Für 2.4.1 wird „Support until“ fünf Jahre nach dem Datum des Inverkehrbringens vorgeschlagen („Proposed: 5 years after it went on the market.“), und der Status ist „Supported“. Version 2.4.0 wird abgewiesen, bis die Begründung angegeben ist („reason for a shorter support“), und dann mit ihr gespeichert. Beide Versionen zeigen „No SBOM“.		

Test	Schritte	Erwartetes Ergebnis	Ergebnis (bestanden / nicht bestanden)	Tester, Datum
OQ-03 SBOM importieren und eine Komponente suchen	Bei Version 2.4.1 auf „Import SBOM“ klicken und eine als XML exportierte SBOM ablegen. Dann über „choose a file“ eine JSON-SBOM im Format CycloneDX (1.x) oder SPDX (2.x oder 3.0) dieser Version auswählen, die lodash 4.17.20 enthält, und auf „Save this SBOM“ klicken. Die SBOM mit „View“ öffnen und lodash in „Filter components…“ eingeben. In „Products“ unter „Which products contain…“ lodash < 4.17.21 eingeben und auf „Search“ klicken. Unter „History of this product“ auf „Show“ klicken.	Die XML-Datei wird mit „This is an XML file. Export the SBOM as JSON (CycloneDX or SPDX).“ abgewiesen. Die JSON-Datei wird mit Format, Version und Anzahl der Komponenten erkannt (zum Beispiel „CycloneDX 1.5 · 312 components (25 direct)“), mit Dateiname, Größe und dem beschriebenen Produkt (eine Warnung, falls sie eine andere Version beschreibt); „SBOM saved: N components“ erscheint. Die SBOM-Ansicht listet lodash mit Version, Typ und „Direct“ auf und zeigt den „SHA-256 of the file“. Die Suche liefert „1 match in 1 version“ (Gateway Console 2.4.1), gekennzeichnet als „In range“, mit „Open a case for 1 version“. Der Verlauf zeigt „SBOM imported“ mit Version, Format und Anzahl.		
OQ-04 Einen Fall aus einem Vorgang eröffnen	Im Testprojekt einen Vorgang mit der Zusammenfassung „[Snyk] High severity - Prototype Pollution in lodash“ und der Beschreibung „CVE-2020-8203. Vulnerable versions: < 4.17.21“ erstellen. Dessen Panel „CRA“ öffnen und auf „Open a case“ klicken. Unter „Products and versions affected“ auf „Add them“ klicken (oder 2.4.1 manuell auswählen); „Owner“ = Benutzer A beibehalten; auf „Open the case“ klicken. Den Vorgang neu laden.	Das Panel bietet „Open a CRA case on [key]“ an, und das Formular zeigt „Read from the Snyk work item: check before saving.“, mit vorausgefüllten Feldern „Title“, „Identifiers“ (CVE-2020-8203), „Severity“ High, „Component“ lodash und „Vulnerable versions“ < 4.17.21, „1 version contains this component: Gateway Console 2.4.1“ und einem „Fix target date“ mit „Proposed: 30 days for this severity.“. „CRA-0001 opened“ erscheint; das Panel zeigt nun den Fall im Schritt „Qualification“ mit „Qualify it“ und bietet nicht mehr an, einen weiteren Fall zu eröffnen. „Vulnerabilities“ listet CRA-0001 auf.		
OQ-05 Qualifizieren, signieren und die Fristen starten	Als Benutzer A bei CRA-0001 unter „Qualification“: „Are the products listed affected?“ = „Affected“; „Is it actively exploited?“ = „Yes“; in „When did you become aware of it?“ ein Datum und eine Uhrzeit 30 Stunden vor jetzt eingeben; „Why“ ausfüllen; auf „Qualify and sign“ klicken. Die Erklärung lesen, das richtige Passwort in „Signing password“ eingeben und auf „Sign“ klicken.	Vor dem Signieren erscheint „Reportable under Article 14: the clocks start.“, und der Hinweis zeigt Early warning = Kenntnisnahme + 24 h und Notification = Kenntnisnahme + 72 h. Nach dem Signieren zeigt die Qualifizierung die Signatur: Name von Benutzer A, „Qualification“, Datum und Uhrzeit, die Erklärung „I qualify CRA-0001 as an actively exploited vulnerability in the products listed. It is reported under Article 14 of the Cyber Resilience Act.“ und den SHA-256-Fingerabdruck. Drei Fristen erscheinen: „Early warning“ „Late“ (fällig Kenntnisnahme + 24 h, mit UTC-Zeit), „Notification“ „Open“ (fällig Kenntnisnahme + 72 h, noch etwa 42 h), „Final report“ „Not started“ („Starts when the fix or mitigation is available.“). „History“ zeigt „Qualified (signed) · Art. 14“.		
OQ-06 Falsches Signaturpasswort und Sperre	Bei CRA-0001 auf „Qualify again“ klicken, die Antworten beibehalten, ein neues „Why“ schreiben und auf „Qualify and sign“ klicken. Zweimal mit einem falschen Passwort auf „Sign“ klicken, dann ein drittes Mal; dann mit dem richtigen Passwort. 5 Minuten warten (die in Test 1 eingestellte Sperre) und erneut mit dem richtigen Passwort signieren.	Die ersten beiden Versuche zeigen „Wrong signing password.“, und nichts wird aufgezeichnet. Der dritte zeigt „Signing is locked for a few minutes after too many attempts.“, und das richtige Passwort wird mit derselben Meldung abgewiesen, solange die Sperre andauert. Nach 5 Minuten wird die Signatur angenommen: „History“ zeigt „Qualified again (signed) · Art. 14“, die Qualifizierung zeigt „1 earlier qualification“, und die drei Fälligkeitszeitpunkte sind unverändert.		
OQ-07 ENISA-Felder und als übermittelt erfasste Meldungen	Bei CRA-0001 unter „Reporting to ENISA“ den Tab „Notification“ öffnen, dann den Tab „Early warning“. Die Pflichtfelder prüfen, „+ … optional fields“ öffnen, „Summary“ bearbeiten und auf „Save the text“ klicken. Bei einem Feld auf „Copy“ und auf „Copy all fields“ klicken und in einen Texteditor einfügen. „Submitted on the platform at“ auf jetzt setzen, „Platform reference“ ausfüllen und auf „Record as submitted“ klicken. Die	Bevor die Frühwarnung erfasst ist, zeigt der Tab Notification „Record the early warning first.“. Die Pflichtfelder tragen die Bezeichnungen der ENISA und sind aus dem Fall und dem Produkt vorausgefüllt: „Notification type“ (Vulnerability), „Title“, „Summary“, „Member States where the product is available“, „Product name“, „Product version“ (2.4.1) und „Date and time when you become aware (UTC)“; jedes zeigt verwendete Zeichen / Limit. „Text saved“ erscheint; der eingefügte Text enthält jede Bezeichnung und jeden		

Test	Schritte	Erwartetes Ergebnis	Ergebnis (bestanden / nicht bestanden)	Tester, Datum
	„Notification“ auf dieselbe Weise erfassen. Auf „Show the text sent“ klicken.	Wert. Nach dem Erfassen: „Submitted [date time] ([UTC]) · recorded by User A · [reference]“ mit „… late“ für die Frühwarnung und „on time“ für die Meldung, sowie ein SHA-256; die Fristen zeigen „Submitted late“ und „Submitted“. „History“ zeigt „Report submitted · Early warning (submitted late)“ und „Report submitted · Notification“; „Show the text sent“ zeigt genau die erfassten Felder.		
OQ-08 Korrektur, Abschlussbericht und Information der Nutzer	Bei CRA-0001 den Tab „Final report“ öffnen. Unter „Fix or mitigation“ auf „Record the fix“ klicken: „What is available“ = „Security update“, „Fixed version“ = 2.4.2, „Available to users since“ = jetzt, „What it changes“ und „Link for users“ ausfüllen, auf „Record the fix“ klicken. Ohne den Tab „Final report“ zu verlassen, „Date when corrective or mitigating measure has been available“ und „Details about the security update or corrective measure available“ ansehen. Nur „Date and time when it occurred (UTC)“ ausfüllen, „Full description of the impact“ leer lassen und „Record as submitted“ ansehen; dann „Full description of the impact“ ausfüllen und auf „Record as submitted“ klicken. Unter „Users and advisory“ › „Users informed“ auf „Record“ klicken, „Informed at“ und „How“ ausfüllen, „What they were told“ lesen, auf „Record“ klicken.	Vor der Korrektur zeigt der Tab Final report „Record the fix first: the final report describes it.“. Danach: „Fix recorded“, Schritt „Disclosure“, und die Frist „Final report“ ist genau 14 Tage nach „Available to users since“ fällig; im geöffneten Tab werden die Felder aus der Korrektur sofort ausgefüllt (das Datum in UTC, „Version 2.4.2. …“). Solange ein Pflichtfeld leer ist, erscheint „1 required field is empty or too long.“ und „Record as submitted“ ist ausgegraut (eine Meldung mit leerem Pflichtfeld lehnt auch der Server der App ab). Nach dem Erfassen zeigt die Frist „Submitted“, und die Korrektur zeigt „The final report was submitted with this fix: it can no longer change.“ (kein „Edit“). „What they were told“ ist mit dem Produkt, der Version, „Update to version 2.4.2 or later.“ und dem Sicherheitskontakt vorausgefüllt; der Eintrag zeigt Datum, Kanal und „recorded by User A“. „History“ zeigt „Fix available“, „Report submitted · Final report“ und „Users informed“.		
OQ-09 Fristen bei schwerwiegendem Vorfall und Erinnerung an den Verantwortlichen	Als Benutzer A auf „New case“ klicken: „Kind“ = „Incident“, „Work item“ = „Create one“ (Testprojekt, beliebiger „Work item type“), „Title“ und „What is known“ ausfüllen, Gateway Console 2.4.1 auswählen, „Owner“ = Benutzer B; auf „Open the case“ klicken. Qualifizieren: „Affected“, „Is the incident severe?“ = „Yes“, „Is it suspected to come from unlawful or malicious acts?“ = „Unknown“, Kenntnisnahme vor 30 Stunden, „Why“; signieren. Keine Meldung erfassen. Am nächsten Tag nach 09:00 UTC das Postfach von Benutzer B und die „History“ des Falls prüfen. Dann als Benutzer B die „Early warning“ und die „Notification“ als jetzt übermittelt erfassen.	Bevor die Meldung erfasst ist, zeigt die Frist „Final report“ „Not started“ („Starts when the notification is submitted.“); die Felder der Frühwarnung enthalten „Incident is suspected of unlawful or malicious acts“ = Unknown. Benutzer B erhält eine E-Mail von Jira, „Clearlane CRA: 1 case needs you“, die den Fall mit „Early warning late since [date] UTC“ und einem Link nennt; am Vorgang wird nichts veröffentlicht, und an diesem Tag kommt keine zweite Erinnerung. „History“ zeigt „Reminder e-mail sent · early warning late“. Nachdem die Meldung erfasst ist, ist der Abschlussbericht genau einen Kalendermonat nach dem Übermittlungszeitpunkt der Meldung fällig.		
OQ-10 CSAF-Sicherheitshinweis	Bei CRA-0001 unter „Users and advisory“ › „Security advisory“ „EN“ als „Advisory language“ wählen und auf „Preview“ klicken. Auf „Record a publication“ klicken, „What changed“ und „Where it is published“ ausfüllen, auf „Record the publication“ klicken, dann auf „Download the CSAF file“. Die Anhänge des Vorgangs und die heruntergeladene Datei öffnen (optional in einem CSAF-2.0-Validator).	Die Vorschau zeigt das betroffene Produkt und die Versionen, die korrigierte Version, Schweregrad, Kennungen, „This vulnerability is actively exploited.“, die zu ergreifenden Maßnahmen und den Kontakt. „Revision 1 published on [date] · Attached to [key]“ erscheint; der Vorgang hat cra-0001.json; die Revisionszeile zeigt die Zusammenfassung, die URL, Benutzer A und ein SHA-256. Die Datei ist ein CSAF-2.0-Sicherheitshinweis („csaf_version“: „2.0“, Tracking-ID CRA-0001, Herausgeber = Name und Website des Herstellers), der 2.4.1 als bekannt betroffen und 2.4.2 als behoben aufführt, mit einer Herstellerkorrektur und dem Ausnutzungsstatus. „History“ zeigt „Advisory published“.		
OQ-11 Berechtigungen	Als Benutzer A auf „New case“ klicken, „Use an existing one“ wählen, einen Vorgang aus einem Projekt auswählen, das Benutzer B nicht einsehen kann, und auf „Open the case“ klicken. Als Benutzer B (nicht im Sicherheitsteam) Apps › Clearlane CRA › „Vulnerabilities“ öffnen, „All“ wählen und diese	Benutzer B sieht den Fall zum verborgenen Vorgang nicht: Er wird nicht aufgeführt, und die Suche zeigt „No case matches these filters.“. Bei CRA-0001 sieht Benutzer B „Read only: the owner and the security team change this case.“, ohne „Qualify again“, ohne „Close and sign“ und ohne		

Test	Schritte	Erwartetes Ergebnis	Ergebnis (bestanden / nicht bestanden)	Tester, Datum
	Fallnummer in das Suchfeld eingeben. Als Benutzer B CRA-0001 und dann „Products“ öffnen.	bearbeitbares Feld. In „Products“ hat Benutzer B kein „Add a product“ und sieht „SBOMs are only visible to the security team.“.		
OQ-12 Abschluss, Nachweisdatei und Prüfpfad	Als Benutzer A bei CRA-0001 die Liste „Closure“ prüfen, auf „Close and sign“ klicken, „Note“ ausfüllen und mit dem richtigen Passwort signieren. Auf „Evidence file (PDF)“ klicken und die Datei öffnen. Auf „Attach PDF to the work item“ klicken. In „History“ auf „Show all“ klicken.	Jeder Punkt der Liste ist abgehakt („Fix or mitigation“, „Early warning“, „Notification“, „Final report“, „Users informed“, „Advisory published (or delay recorded)“). Nach dem Signieren: „Fixed · closed on [date]“, und die Abschlusssignatur zeigt Name, „Closure“, Datum und Uhrzeit, die Erklärung „I confirm that the handling of CRA-0001 is complete as recorded: corrective or mitigating measure, reports, information of users and advisory. I close this case.“ und ihren SHA-256; nichts kann mehr bearbeitet werden. Das PDF „CRA case evidence file“ enthält die Falldaten, Produkte und Versionen mit Datum des Inverkehrbringens, Supportende und Mitgliedstaaten, die Qualifizierung, jede Meldung (fällig und übermittelt in UTC, Referenz, Fristeinhaltung, SHA-256, übermittelter Text), Korrektur, Information der Nutzer, Revisionen des Sicherheitshinweises, elektronische Signaturen, Anhänge des Vorgangs und Prüfpfad, mit „Generated … by … · Clearlane CRA“ und Seitenzahlen. „Attached to [key]“ erscheint. „History“ listet jeden bei CRA-0001 erfassten Schritt (Tests 4 bis 8, 10 und 12) mit Datum, Uhrzeit und Person auf; kein Eintrag kann bearbeitet oder gelöscht werden.		