Anlage – Profilbögen Los 2 – Security-Tests

Name Bieter:

Kriterienkatalog – Erfahrung und Qualifikation des verbindlich anzubietenden Personals – Personalprofil und Zuschlagskriterien

Die untenstehende Profiltabelle nennt die konkreten Anforderungen an das Personenprofil für Los 2 – Security-Tests gemäß der Leistungsbeschreibung. Der Bieter muss zu diesen Anforderungen entsprechende Angaben machen. Dazu sind in der Spalte „Angaben des Bieters“ die entsprechenden Eintragungen vorzunehmen.

Füllen Sie das Personenprofil direkt im elektronischen Formular aus, indem Sie die Formularfelder benutzen. Falls dies aus technischen Gründen nicht möglich sein sollte, werden auch handschriftliche Eintragungen akzeptiert.

Die maximal erreichbare Wertungspunktzahl beträgt 365 WP.

Legende

A = A-Kriterium (Mindestanforderung)

B = B-Kriterium (bewertet)

I = Informativ

WP = Wertungspunkte

Hinweis zur Teamzusammensetzung:

Für Los 2 – Security-Tests wird angesichts der Leistungsdauer von 2 Monaten sowie des Prüfgegenstands (Webanwendung inkl. UI, APIs, Authentifizierungs-/Autorisierungsmechanismen, Rollen- und Berechtigungskonzepte, Datenverarbeitung/-übertragung, Konfigurationen, Anbindungen an externe Dienste) ein dreiköpfiges Security-Test-Team als realistisch und auskömmlich angesehen:

- 1x Lead Penetration Tester/in (Security Test Lead) für Methodik, Koordination, Testkonzept, Berichtswesen und Retest-Steuerung,
- 1x Senior Penetration Tester/in mit Schwerpunkt Web-Anwendung und APIs (inkl. KI-/LLM-spezifischer Schwachstellen wie Prompt Injection),
- 1x Penetration Tester/in mit Schwerpunkt Infrastruktur, Rollen-/Berechtigungskonzepte und datenschutzrelevante Sicherheitsaspekte.

Teammitglied 1 – Lead Penetration Tester/in (Security Test Lead)

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
1	A	Name (ggf. anstelle dessen eindeutiges Kennzeichen)	
2	I	Funktion beim Bieter *Sofern die Person bei einem Unterauftragnehmer beschäftigt ist, ist dieser hier zusätzlich anzugeben.*	Funktion: Ggf. Unterauftragnehmer:
3	A	Einsatzumfang während der Leistungsdauer von maximal 70 Tagen (40 Tage initialer Test sowie voraussichtlich 30 Tage für Nachtestungen) *Mindestanforderung: 75% (6 Stunden pro Tag)*	Einsatzumfang:
4	A	Der/Die Lead Penetration Tester/in (Security Test Lead) verfügt über gute deutsche Sprachkenntnisse (mind. B2 nach europ. Referenzrahmen)	☐ muttersprachlich ☐ B2-Zertifizierung o. vergleichbar Nachweis als Anlage Nr. ___ beigefügt
5	A	Der/Die Lead Penetration Tester/in (Security Test Lead) erklärt sich bereit, auf Anforderung des Auftraggebers ein aktuelles polizeiliches Führungszeugnis (nicht älter als 6 Monate) vorzulegen *Aufgrund des sicherheitskritischen Charakters der Leistung (Zugriff auf sicherheitsrelevante Systeminformationen, Schwachstellen und ggf. personenbezogene Daten) wird eine Erklärung zur Zuverlässigkeit vorausgesetzt.*	☐ Erklärung zur Vorlage eines Führungszeugnisses auf Anforderung liegt bei
6	B	Der/Die Lead Penetration Tester/in (Security Test Lead) verfügt über einen akkreditierten Master- oder gleichwertigen Studienabschluss der (Wirtschafts-)Informatik, IT-Sicherheit oder vergleichbaren Studiengang, alternativ eine vergleichbare einschlägige Berufserfahrung *Bei Vorlage eines Nachweises einmalig: 5 WP*	☐ Master- oder gleichwertiger Studienabschluss (Wirtschafts-)Informatik, IT-Sicherheit oder vergleichbar ☐ vergleichbare einschlägige Berufserfahrung Nachweis als Anlage Nr. ___ beigefügt
7	A/B	Der/Die Lead Penetration Tester/in (Security Test Lead) verfügt über Berufserfahrung im Bereich Penetrationstests/IT-Security-Testing: *Mindestanforderung: mind. 6 Jahre Erfahrung* über 10 Jahre: 5 WP **Maximale Wertungspunkte: 5 WP** *Hinweis: Es darf maximal eine Box angekreuzt werden.*	☐ mind. 6 Jahre (Mindestanforderung) ☐ über 10 Jahre

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
8	B	**Der/Die Lead Penetration Tester/in (Security Test Lead) verfügt über praktische Berufserfahrung in den folgenden Bereichen:** **Steuerung und Koordination von Security-Test-/Penetrationstestprojekten** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Anwendung anerkannter Methoden (OWASP Testing Guide, OWASP Top 10, OWASP API Security Top 10)** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Erstellung von Testkonzepten, Penetrationstestberichten, Risikobewertungen und Management-Zusammenfassungen** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Steuerung von Nachtests (Retests) nach Schwachstellenbehebung** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Security-Testing von KI-/LLM-basierten Anwendungen einschließlich Adversarial und Red Team Testing von KI-Funktionalitäten und Agentic Harnesses bzw. agentischen Systemen** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Maximale Wertungspunkte: 75 WP** *Hinweis: Eine Eigenerklärung ohne eine aussagekräftige Begründung wird nicht bewertet.* **** Bedeutung der Erfahrungsstufen zur Orientierung:***	Steuerung und Koordination von Security-Test-/Penetrationstestprojekten ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Anwendung anerkannter Methoden (OWASP Testing Guide, OWASP Top 10, OWASP API Security Top 10) ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Erstellung von Testkonzepten, Penetrationstestberichten, Risikobewertungen und Management-Zusammenfassungen ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Steuerung von Nachtests (Retests) nach Schwachstellenbehebung ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Security-Testing von KI-/LLM-basierten Anwendungen einschließlich Adversarial und Red Team Testing von KI-Funktionalitäten und Agentic Harnesses bzw. agentischen Systemen ☐ relevante Grundkenntnisse

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
		relevante Grundkenntnisse: theoretische Grundlagen und professionelle Anwendungserfahrung in relevantem Umfang (>3 Monate) *umfangreiche Projekterfahrung: tiefere Fach- und Anwendungskenntnisse aus mehreren Projekten (>3 Jahre); kann andere einarbeiten* *Expertenkenntnisse: sehr tiefe Kenntnisse; hat an der Weiterentwicklung der Methodik/des Tools mitgewirkt oder hält Vorträge/Workshops dazu*	☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung:
9	I	Der/Die Lead Penetration Tester/in (Security Test Lead) verfügt über einschlägige Zertifizierungen (z. B. OSCP, CISSP, CEH, GWAPT oder vergleichbar)	Zertifizierung/Beschreibung: Nachweis als Anlage Nr. ___ beigefügt
10	B	Der/Die Lead Penetration Tester/in (Security Test Lead) verfügt über praktische Erfahrung im Umgang mit Pentest-/Security-Testing-Werkzeugen (z. B. Burp Suite, OWASP ZAP, Nmap, Metasploit) sowie mit der Klassifizierung von Schwachstellen nach anerkannten Standards (z. B. CVSS) - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP **Maximale Wertungspunkte: 10 WP**	☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung Eingesetzte Werkzeuge:
11		**Projektreferenzen**	
11.1	A	Es muss mindestens eine persönliche Projektreferenz eingereicht werden, in der die Person Tätigkeiten im Bereich Leitung von Penetrationstests/Security-Testprojekten für größere Softwaresysteme wahrgenommen hat. **Mindestanforderungen:** - Referenz nicht älter als 3 Jahre (laufende Projekte sind zulässig) - Der Projekteinsatz des/der MitarbeiterIn in dieser Rolle betrug mindestens 3 Monate	Der/Die MitarbeiterIn hatte in dem Referenzprojekt eine dem hier abgefragten Profil entsprechende Funktion (Mindestanforderung) Persönliche Einsatzzeit (Monat/Jahr von/bis): Von: Bis: Auftraggeber und Ansprechpartner (Adresse, Telefonnummer):
11.2	B	**Soweit die Tätigkeiten der Person im/in den vorzulegenden Referenzprojekt/en auch die folgenden Aspekte umfasst haben, werden die folgenden Bewertungskriterien einmalig gewertet:** - Leitung eines Pentest-Projekts für ein System mit mehr als 100.000 Nutzenden: 10 WP - Steuerung eines Security-Testteams von mind. 2 Personen: 10 WP	☐ Leitung eines Pentest-Projekts für ein System mit mehr als 100.000 Nutzenden Kurze Beschreibung: ☐ Steuerung eines Security-Testteams von mind. 2 Personen Kurze Beschreibung: ☐ Security-Testung im öffentlichen/behördlichen Kontext

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
		- Security-Testung im öffentlichen/behördlichen Kontext: 5 WP - Security-Testung von Systemen mit personenbezogenen Daten (DSGVO-relevant): 5 WP - Leitung eines Pentest-Projekts für eine KI-/LLM-basierte Anwendung einschließlich Adversarial und Red Team Testing von KI-Funktionalitäten und Agentic Harnesses bzw. agentischen Systemen: 10 WP **Maximale Wertungspunkte: 40 WP** *Hinweis: Eigenerklärungen ohne eine aussagekräftige Darstellung werden nicht bewertet.*	Kurze Beschreibung: ☐ Security-Testung von Systemen mit personenbezogenen Daten (DSGVO-relevant) Kurze Beschreibung: ☐ Leitung eines Pentest-Projekts für eine KI-/LLM-basierte Anwendung einschließlich Adversarial und Red Team Testing von KI-Funktionalitäten und Agentic Harnesses bzw. agentischen Systemen Kurze Beschreibung:
			Mögliche Gesamtpunktzahl Der/Die Lead Penetration Tester/in (Security Test Lead): 135 WP

Teammitglied 2 – Senior Penetration Tester/in (Web & API)

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
1	A	Name (ggf. anstelle dessen eindeutiges Kennzeichen)	
2	I	Funktion beim Bieter *Sofern die Person bei einem Unterauftragnehmer beschäftigt ist, ist dieser hier zusätzlich anzugeben.*	Funktion: Ggf. Unterauftragnehmer:
3	A	Einsatzumfang während der Leistungsdauer von maximal 70 Tagen (40 Tage initialer Test sowie voraussichtlich 30 Tage für Nachtestungen) *Mindestanforderung: 100% (8 Stunden pro Tag)*	Einsatzumfang:
4	A	Der/Die Senior Penetration Tester/in (Web & API) verfügt über gute deutsche Sprachkenntnisse (mind. B2 nach europ. Referenzrahmen)	☐ muttersprachlich ☐ B2-Zertifizierung o. vergleichbar Nachweis als Anlage Nr. ___ beigefügt
5	A	Der/Die Senior Penetration Tester/in (Web & API) erklärt sich bereit, auf Anforderung des Auftraggebers ein aktuelles polizeiliches Führungszeugnis (nicht älter als 6 Monate) vorzulegen *Aufgrund des sicherheitskritischen Charakters der Leistung (Zugriff auf sicherheitsrelevante Systeminformationen, Schwachstellen und ggf. personenbezogene Daten) wird eine Erklärung zur Zuverlässigkeit vorausgesetzt.*	☐ Erklärung zur Vorlage eines Führungszeugnisses auf Anforderung liegt bei
6	B	Der/Die Senior Penetration Tester/in (Web & API) verfügt über einen akkreditierten Master- oder gleichwertigen Studienabschluss der (Wirtschafts-)Informatik, IT-Sicherheit oder vergleichbaren Studiengang, alternativ eine vergleichbare einschlägige Berufserfahrung *Bei Vorlage eines Nachweises einmalig: 5 WP*	☐ Master- oder gleichwertiger Studienabschluss (Wirtschafts-)Informatik, IT-Sicherheit oder vergleichbar ☐ vergleichbare einschlägige Berufserfahrung Nachweis als Anlage Nr. ___ beigefügt
7	A/B	Der/Die Senior Penetration Tester/in (Web & API) verfügt über Berufserfahrung im Bereich Penetrationstests/IT-Security-Testing: *Mindestanforderung: mind. 4 Jahre Erfahrung* über 6 Jahre: 5 WP **Maximale Wertungspunkte: 5 WP** *Hinweis: Es darf maximal eine Box angekreuzt werden.*	☐ mind. 4 Jahre (Mindestanforderung) ☐ über 6 Jahre

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
8	B	**Der/Die Senior Penetration Tester/in (Web & API) verfügt über praktische Berufserfahrung in den folgenden Bereichen:** **Web-Application-Penetrationstests nach OWASP Top 10** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **API-Penetrationstests nach OWASP API Security Top 10 (inkl. Schnittstellenverträge, Authentifizierung, Fehlerbehandlung)** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Prüfung von Authentifizierungs-, Sitzungs- und Autorisierungsmechanismen (Broken Access Control, Privilege Escalation)** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Testen von KI-/LLM-basierten Funktionen einschließlich Agentic Harness auf sicherheitsrelevante Schwachstellen (z. B. Prompt Injection, Datenlecks über Modellantworten, Missbrauch von Assistenz-/Tutorfunktionen, unzulässige Tool-Aufrufe, Manipulation des Agentenverhaltens)** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Maximale Wertungspunkte: 60 WP** *Hinweis: Eine Eigenerklärung ohne eine aussagekräftige Begründung wird nicht bewertet.* **** Bedeutung der Erfahrungsstufen zur Orientierung:*** *relevante Grundkenntnisse: theoretische Grundlagen und professionelle Anwendungserfahrung in relevantem Umfang (>3 Monate)* *umfangreiche Projekterfahrung: tiefere Fach- und Anwendungskenntnisse aus mehreren*	Web-Application-Penetrationstests nach OWASP Top 10 ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: API-Penetrationstests nach OWASP API Security Top 10 (inkl. Schnittstellenverträge, Authentifizierung, Fehlerbehandlung) ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Prüfung von Authentifizierungs-, Sitzungs- und Autorisierungsmechanismen (Broken Access Control, Privilege Escalation) ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Testen von KI-/LLM-basierten Funktionen einschließlich Agentic Harness auf sicherheitsrelevante Schwachstellen (z. B. Prompt Injection, Datenlecks über Modellantworten, Missbrauch von Assistenz-/Tutorfunktionen, unzulässige Tool-Aufrufe, Manipulation des Agentenverhaltens) ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung:

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
		Projekten (>3 Jahre); kann andere einarbeiten *Expertenkenntnisse: sehr tiefe Kenntnisse; hat an der Weiterentwicklung der Methodik/des Tools mitgewirkt oder hält Vorträge/Workshops dazu*	
9	I	Der/Die Senior Penetration Tester/in (Web & API) verfügt über einschlägige Zertifizierungen (z. B. OSCP, eWPT/eWPTX, GWAPT oder vergleichbar)	Zertifizierung/Beschreibung: Nachweis als Anlage Nr. ___ beigefügt
10	B	Der/Die Senior Penetration Tester/in (Web & API) verfügt über praktische Erfahrung im Umgang mit Pentest-/Security-Testing-Werkzeugen (z. B. Burp Suite, OWASP ZAP, Nmap, Metasploit) sowie mit der Klassifizierung von Schwachstellen nach anerkannten Standards (z. B. CVSS) - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP **Maximale Wertungspunkte: 10 WP**	☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung Eingesetzte Werkzeuge:
11		**Projektreferenzen**	
11.1	A	Es muss mindestens eine persönliche Projektreferenz eingereicht werden, in der die Person Tätigkeiten im Bereich Web-Application- und/oder API-Penetrationstests wahrgenommen hat. **Mindestanforderungen:** - Referenz nicht älter als 3 Jahre (laufende Projekte sind zulässig) - Der Projekteinsatz des/der MitarbeiterIn in dieser Rolle betrug mindestens 3 Monate	Der/Die MitarbeiterIn hatte in dem Referenzprojekt eine dem hier abgefragten Profil entsprechende Funktion (Mindestanforderung) Persönliche Einsatzzeit (Monat/Jahr von/bis): Von: Bis: Auftraggeber und Ansprechpartner (Adresse, Telefonnummer):
11.2	B	**Soweit die Tätigkeiten der Person im/in den vorzulegenden Referenzprojekt/en auch die folgenden Aspekte umfasst haben, werden die folgenden Bewertungskriterien einmalig gewertet:** - Penetrationstest einer Webanwendung mit mehr als 100.000 Nutzenden: 10 WP - Identifikation kritischer Schwachstellen (z. B. IDOR, Broken Access Control, Injection): 10 WP - Security-Testung im schulischen/öffentlichen Bildungskontext: 5 WP - Penetrationstest einer KI-/LLM-basierten Anwendung einschließlich Agentic Harness (z. B. Prompt Injection, Model-Abuse,	☐ Penetrationstest einer Webanwendung mit mehr als 100.000 Nutzenden Kurze Beschreibung: ☐ Identifikation kritischer Schwachstellen (z. B. IDOR, Broken Access Control, Injection) Kurze Beschreibung: ☐ Security-Testung im schulischen/öffentlichen Bildungskontext Kurze Beschreibung: ☐ Penetrationstest einer KI-/LLM-basierten Anwendung einschließlich Agentic Harness (z. B. Prompt Injection, Model-Abuse, unzulässige

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
		unzulässige Tool-Aufrufe, Manipulation des Agentenverhaltens): 10 WP **Maximale Wertungspunkte: 35 WP** *Hinweis: Eigenerklärungen ohne eine aussagekräftige Darstellung werden nicht bewertet.*	Tool-Aufrufe, Manipulation des Agentenverhaltens) Kurze Beschreibung:
			Mögliche Gesamtpunktzahl Der/Die Senior Penetration Tester/in (Web & API): 115 WP

Teammitglied 3 – Penetration Tester/in (Infrastruktur, Rollen & Datenschutz)

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
1	A	Name (ggf. anstelle dessen eindeutiges Kennzeichen)	
2	I	Funktion beim Bieter *Sofern die Person bei einem Unterauftragnehmer beschäftigt ist, ist dieser hier zusätzlich anzugeben.*	Funktion: Ggf. Unterauftragnehmer:
3	A	Einsatzumfang während der Leistungsdauer von maximal 70 Tagen (40 Tage initialer Test sowie voraussichtlich 30 Tage für Nachtestungen) *Mindestanforderung: 100% (8 Stunden pro Tag)*	Einsatzumfang:
4	A	Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz) verfügt über gute deutsche Sprachkenntnisse (mind. B2 nach europ. Referenzrahmen)	☐ muttersprachlich ☐ B2-Zertifizierung o. vergleichbar Nachweis als Anlage Nr. ___ beigefügt
5	A	Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz) erklärt sich bereit, auf Anforderung des Auftraggebers ein aktuelles polizeiliches Führungszeugnis (nicht älter als 6 Monate) vorzulegen *Aufgrund des sicherheitskritischen Charakters der Leistung (Zugriff auf sicherheitsrelevante Systeminformationen, Schwachstellen und ggf. personenbezogene Daten) wird eine Erklärung zur Zuverlässigkeit vorausgesetzt.*	☐ Erklärung zur Vorlage eines Führungszeugnisses auf Anforderung liegt bei
6	B	Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz) verfügt über einen akkreditierten Master- oder gleichwertigen Studienabschluss der (Wirtschafts-)Informatik, IT-Sicherheit oder vergleichbaren Studiengang, alternativ eine vergleichbare einschlägige Berufserfahrung *Bei Vorlage eines Nachweises einmalig: 5 WP*	☐ Master- oder gleichwertiger Studienabschluss (Wirtschafts-)Informatik, IT-Sicherheit oder vergleichbar ☐ vergleichbare einschlägige Berufserfahrung Nachweis als Anlage Nr. ___ beigefügt
7	A/B	Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz) verfügt über Berufserfahrung im Bereich Penetrationstests/IT-Security-Testing: *Mindestanforderung: mind. 3 Jahre Erfahrung* über 5 Jahre: 5 WP **Maximale Wertungspunkte: 5 WP** *Hinweis: Es darf maximal eine Box angekreuzt werden.*	☐ mind. 3 Jahre (Mindestanforderung) ☐ über 5 Jahre

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
8	B	**Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz) verfügt über praktische Berufserfahrung in den folgenden Bereichen:** **Netzwerk- und Infrastruktur-Penetrationstests (inkl. Konfigurationsprüfung, Hardening, Cloud-Security)** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Prüfung von Rollen- und Berechtigungskonzepten (horizontale/vertikale Rechteausweitung)** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Prüfung der Datenübertragung und Verschlüsselung sowie datenschutzrelevanter Sicherheitsaspekte (DSGVO)** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Prüfung von Anbindungen an externe Dienste und Drittsysteme sowie der sicherheitsrelevanten Interaktion mit KI-/LLM-Diensten und Agentic Harnesses** - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP - Expertenkenntnisse: 15 WP **Maximale Wertungspunkte: 60 WP** *Hinweis: Eine Eigenerklärung ohne eine aussagekräftige Begründung wird nicht bewertet.* **** Bedeutung der Erfahrungsstufen zur Orientierung:*** *relevante Grundkenntnisse: theoretische Grundlagen und professionelle Anwendungserfahrung in relevantem Umfang (>3 Monate)* *umfangreiche Projekterfahrung: tiefere Fach- und Anwendungskenntnisse aus mehreren Projekten (>3 Jahre); kann andere einarbeiten*	Netzwerk- und Infrastruktur-Penetrationstests (inkl. Konfigurationsprüfung, Hardening, Cloud-Security) ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Prüfung von Rollen- und Berechtigungskonzepten (horizontale/vertikale Rechteausweitung) ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Prüfung der Datenübertragung und Verschlüsselung sowie datenschutzrelevanter Sicherheitsaspekte (DSGVO) ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung: Prüfung von Anbindungen an externe Dienste und Drittsysteme sowie der sicherheitsrelevanten Interaktion mit KI-/LLM-Diensten und Agentic Harnesses ☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung ☐ Expertenkenntnisse Kurze Beschreibung:

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
		Expertenkenntnisse: sehr tiefe Kenntnisse; hat an der Weiterentwicklung der Methodik/des Tools mitgewirkt oder hält Vorträge/Workshops dazu	
9	I	Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz) verfügt über einschlägige Zertifizierungen (z. B. OSCP, CEH, CCSP oder vergleichbar)	Zertifizierung/Beschreibung: Nachweis als Anlage Nr. ___ beigefügt
10	B	Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz) verfügt über praktische Erfahrung im Umgang mit Pentest-/Security-Testing-Werkzeugen (z. B. Burp Suite, OWASP ZAP, Nmap, Metasploit) sowie mit der Klassifizierung von Schwachstellen nach anerkannten Standards (z. B. CVSS) - relevante Grundkenntnisse: 5 WP - umfangreiche Projekterfahrung: 10 WP **Maximale Wertungspunkte: 10 WP**	☐ relevante Grundkenntnisse ☐ umfangreiche Projekterfahrung Eingesetzte Werkzeuge:
11		**Projektreferenzen**	
11.1	A	Es muss mindestens eine persönliche Projektreferenz eingereicht werden, in der die Person Tätigkeiten im Bereich Infrastruktur-Penetrationstests und/oder Prüfung von Rollen-/Berechtigungskonzepten wahrgenommen hat. **Mindestanforderungen:** - Referenz nicht älter als 3 Jahre (laufende Projekte sind zulässig) - Der Projekteinsatz des/der MitarbeiterIn in dieser Rolle betrug mindestens 3 Monate	Der/Die MitarbeiterIn hatte in dem Referenzprojekt eine dem hier abgefragten Profil entsprechende Funktion (Mindestanforderung) Persönliche Einsatzzeit (Monat/Jahr von/bis): Von: Bis: Auftraggeber und Ansprechpartner (Adresse, Telefonnummer):
11.2	B	**Soweit die Tätigkeiten der Person im/in den vorzulegenden Referenzprojekt/en auch die folgenden Aspekte umfasst haben, werden die folgenden Bewertungskriterien einmalig gewertet:** - Penetrationstest einer Cloud-Infrastruktur: 10 WP - Sicherheitsrelevante Prüfung der Verarbeitung personenbezogener Daten (DSGVO-Kontext): 10 WP - Security-Testung im schulischen/öffentlichen Bildungskontext: 5 WP - Sicherheitsprüfung von Schnittstellen zu externen KI-/LLM-Diensten einschließlich der Anbindung und sicherheitsrelevanten Funktionen eines Agentic Harness: 10 WP	☐ Penetrationstest einer Cloud-Infrastruktur Kurze Beschreibung: ☐ Sicherheitsrelevante Prüfung der Verarbeitung personenbezogener Daten (DSGVO-Kontext) Kurze Beschreibung: ☐ Security-Testung im schulischen/öffentlichen Bildungskontext Kurze Beschreibung: ☐ Sicherheitsprüfung von Schnittstellen zu externen KI-/LLM-Diensten einschließlich der Anbindung und sicherheitsrelevanten Funktionen eines Agentic Harness

Lfd. Nr.	A/B/I	Anforderungen	Angaben des Bieters
		Maximale Wertungspunkte: 35 WP *Hinweis: Eigenerklärungen ohne eine aussagekräftige Darstellung werden nicht bewertet.*	Kurze Beschreibung:
			Mögliche Gesamtpunktzahl Der/Die Penetration Tester/in (Infrastruktur, Rollen & Datenschutz): 115 WP