



**Université
de Rennes**



ENSSAT
L A N N I O N

Cahier des Clauses Techniques Particulières

Université de Rennes – IUT de Lannion – Enssat

Acquisition de deux environnements virtuels de formation et
simulation de type cyber-range, un pour l'IUT de Lannion et un pour
l'Enssat

Référence 2023026AOF

Contacts financiers : Tifenn Donguy (IUT) – Tifenn.Donguy@univ-rennes.fr
Carole Perrot (Enssat) – Carole.Perrot@enssat.fr

Contacts techniques : Mohamed-Aymen Chalouf (IUT) – Mohamed.Chalouf@univ-rennes.fr
Christophe Masson (Enssat) – Christophe.Masson@enssat.fr

A.	Objectif et contexte	4
A.1.	Objet de la consultation	4
A.2.	Présentation de l'IUT de Lannion	4
A.3.	Présentation de l'Enssat de Lannion	4
A.4.	Moyens actuellement utilisés pour les enseignements en Cyber à l'IUT	5
A.5.	Moyens actuellement utilisés pour les enseignements en Cyber à l'Enssat	5
B.	Objectifs	5
C.	Listes des contacts	6
C.1.	IUT	6
C.2.	Enssat	7
D.	Clauses techniques - Spécifications attendues	7
D.1.	Avant-propos	7
D.2.	Point particulier concernant le lot 2 – Enssat [Lot 2 – Enssat]	7
D.3.	Vocabulaire	8
D.4.	Dimensionnement de la solution	8
D.4.1.	[Lot 1 – IUT]	8
D.4.2.	[Lot 2 – Enssat]	8
D.5.	Accessibilité de la solution	9
D.6.	Description de l'infrastructure	9
D.7.	Authentification	9
D.8.	Gestion des droits	10
D.9.	Sauvegarde de la plateforme	10
D.10.	Mise à jour de la plateforme	10
D.11.	Constructions d'un environnement de formation et de simulation	10
D.12.	Déploiement d'un environnement de simulation	11
D.13.	Utilisation d'un environnement de simulation	11
D.14.	Scenarii pédagogiques	11
D.14.1.	Simulation de trafic réseau réaliste	11
D.14.2.	Surveillance des étudiants/apprenants et contrôle des scenarii	11
D.14.3.	Scenarii génériques de formation aux risques cyber	12
D.15.	Ouverture et coopération	12
D.16.	Extensibilité de la solution	13
E.	Garantie, contrat de maintenance, communauté d'utilisateurs	13
F.	Formations	13
G.	Modalités d'installation et de réception de la solution	14
G.1.	Installation de la solution	14

G.1.1.	[Lot 1 - IUT]	14
G.1.2.	[Lot2 – Enssat].....	14
G.1.3.	Adresses de livraison	15
G.2.	Délai de livraison – Date de facturation.....	15
G.3.	Phase de test et de recette	15
H.	Format de la réponse.....	16
I.	Développement durable et responsabilité sociétale	16
J.	Listes des prestations supplémentaires éventuelles.....	16
J.1.	[Lot2 – Enssat] PSE 2.1	17
J.2.	Solution de mobilité	17
J.2.1.	[Lot1 – IUT] PSE 1.1.....	17
J.2.2.	[Lot2 – Enssat] PSE 2.2.....	17
J.3.	Augmentation du dimensionnement de la solution	17
J.3.1.	[Lot 1 – IUT] PSE 1.2.....	17
J.3.2.	[Lot 2 – Enssat] PSE 2.3.....	17
J.3.3.	[Lot 2 – Enssat] PSE 2.4.....	17
J.4.	Connexion de matériel physique « délocalisé ».....	17
J.4.1.	[Lot 1 – IUT] PSE 1.3.....	17
J.4.2.	[Lot 2 – Enssat] PSE 2.5.....	17
J.5.	[Lot2 – Enssat] PSE 2.6	17
J.6.	Formation	18
J.6.1.	[Lot 1 – IUT] PSE 1.4.....	18
J.6.2.	[Lot 2 – Enssat] PSE 2.7.....	18
J.6.3.	PSE X.1	18
J.7.	Maintenance	18
J.7.1.	[Lot 1 – IUT] PSE 1.5.....	18
J.7.2.	[Lot 1 – IUT] PSE 1.6.....	18
J.7.3.	[Lot 1 – IUT] PSE 1.7	18
J.7.4.	[Lot 2 – Enssat] PSE 2.8.....	18
J.7.5.	[Lot 2 – Enssat] PSE 2.9.....	18
J.7.6.	[Lot 2 – Enssat] PSE 2.10.....	19

A. Objectif et contexte

A.1. Objet de la consultation

Cette consultation a pour objet la fourniture, la livraison, la mise en service et la formation à l'utilisation de deux « environnements virtuels de simulation et formation de type cyber-range », un pour l'IUT de Lannion et un pour L'Enssat.

Pour l'IUT, l'acquisition de cette plateforme de cybersécurité s'inscrit dans le cadre de développement des enseignements en cybersécurité avec l'arrivée du BUT (Bachelor Universitaire de Technologie) cybersécurité (en 2021) et du développement de nouvelles opportunités de formation autour de la sécurité numérique dans un contexte où : (i) un Campus des Métiers et des Qualifications (CMQ) d'excellence (Numérique, Photonique et Cybersécurité) a été labellisé à Lannion en 2020, et (ii) la structuration et le développement d'un écosystème de référence « cybersécurité des réseaux de communication » en Bretagne sur le territoire de Lannion ont commencé.

Pour l'Enssat, l'acquisition de cette plateforme s'inscrit dans le renforcement des parcours cyber dans ses formations en informatique (FISE et FISA) et en système numérique (cyber IoT/Réseaux). L'Enssat est également partenaire du master en cybersécurité de l'EUR Cyberschool¹. Cette formation en Master 1 et 2 a pour objectif de former à la recherche en cybersécurité. Dans le cadre d'un double diplôme d'ingénieur en Informatique Enssat d'une part et Master EUR CyberSchool d'autre part, des cours spécifiques liés à la sécurité des réseaux et virtualisation des infrastructures sont dispensés (et potentiellement ouverts aux étudiants autres que ceux de l'Enssat).

L'Enssat et l'IUT sont également partie prenante du consortium pour l'appel à projet CMA Cyberskill4All. Dans ce contexte et dans celui du CMQ d'excellence, les deux établissements Lannionnais doivent développer de nouveaux outils et moyens pour former les étudiants/apprenants à la cybersécurité et pouvoir proposer des blocs d'apprentissage pour les non spécialistes désirant se former à la cybersécurité. Les équipements seront donc largement utilisés dans ces cadres.

Par ailleurs, la structuration et le développement d'un écosystème de référence « cybersécurité des réseaux de communication » en Bretagne sur le territoire de Lannion qui a commencé en 2022 prévoit le recrutement d'un bon nombre (environ six) d'enseignants-chercheurs à partir de septembre 2023 qui seront rattachés à l'équipe SOTERN (Autoprotection de l'Internet du Futur) de l'IRISA (Institut de Recherche en Informatique et Systèmes Aléatoires) et qui viendront renforcer les activités de recherche en cybersécurité à l'IUT de Lannion et à l'Enssat.

A.2. Présentation de l'IUT de Lannion

L'Institut Universitaire de Technologie (IUT) de Lannion est une composante de l'Université de Rennes, localisée sur le site de Lannion. L'IUT de Lannion forme chaque année environ 850 étudiants. Il propose des formations de bac + 3 (Bachelor Universitaire de Technologie) dans plusieurs domaines : Information – Communication (InfoCom), Mesures Physiques (MP), Métiers du Multimédia et de l'Internet (MMI), Informatique (Info), Réseaux et Télécommunications (R&T). Trois de ces formations (MMI, Info et R&T) sont en lien direct avec les métiers du numérique avec une formation en cybersécurité (BUT R&T – Parcours Cybersécurité). La majorité de ces formations est orientée vers la pratique tout en étant accessible à l'alternance.

A.3. Présentation de l'Enssat de Lannion

L'École Nationale Supérieure des Sciences Appliquées et de Technologie (Enssat) est une école interne à l'Université de Rennes, situé également à Lannion.

¹ <https://cyberschool.univ-rennes.fr/>

L'Enssat délivre 5 diplômes d'ingénieur habilités par la Commission des Titres d'Ingénieur, en formation initiale et en formation continue :

- Informatique (cybersécurité, IA, science des données, développement logiciel) ;
- Photonique (technologies laser, biophotonique, photonique quantique, télécoms) ;
- Systèmes Numériques (objets communicants, systèmes embarqués, traitement du signal et des images, IA) ;

et par apprentissage :

- Informatique (cybersécurité, science des données et du multimédia, IA) ;
- Photonique & Électronique (technologies laser, systèmes électroniques, instrumentation et mesure).

Pour plus d'information, vous pouvez consulter la brochure "[chiffres clés 2022-2023](#)" ou le [site web](#).

Pour information l'Enssat est situé dans le centre-ville de Lannion, à 6 km de l'IUT.

A.4. Moyens actuellement utilisés pour les enseignements en Cyber à l'IUT

Pour les enseignements pratiques en cybersécurité, l'IUT de Lannion utilise deux types d'équipements :

- les salles banalisées de PC en double boot Linux/Windows (en général 14 postes par salle) sur lesquels on peut déployer des images virtuelles (de 1 à 3) de type VMWare ou VirtualBox ;
- 3 salles spécifiques de 7 environnements de Travaux Pratiques et une quatrième de 14. Un environnement "TP" est utilisé par un binôme d'étudiants. Il est composée de deux routeurs ISR Cisco, un commutateur Cisco, 3 PC en double boot Linux/Windows ainsi qu'un boîtier firewall stormshied. Le tout est complété par des machines virtuelles réparties sur les 3 PC.

Les salles sont raccordées sur un réseau commun de TP et s'appuient si besoin sur un serveur de TP fournissant divers services (DHCP, DNS, partages fichiers, proxy) et un serveur de clonage).

A.5. Moyens actuellement utilisés pour les enseignements en Cyber à l'Enssat

Pour les enseignements pratiques en cybersécurité, l'Enssat utilise deux types d'équipements :

- les salles banalisées de PC sous Linux (en général 16 postes par salle) sur lesquels sont déployés des images virtuelles (de 1 à 3) de type VirtualBox ;
- une salle spécifique "Réseaux" de 16 postes basés sur une infrastructure physique Cisco (commutateurs 2960 et routeurs 2811), ainsi que des machines virtuelles avec VirtualBox permettant de simuler une multiplication des postes. La capacité actuelle de la salle réseau est de 4 groupes banalisés permettant d'utiliser simultanément 1 routeur, 6 commutateurs et 16 terminaux (linux le plus souvent).

B. Objectifs

Les environnements virtuels de formation proposent d'immerger les étudiants/apprenants au sein de simulations visant à s'entraîner et à tester leurs compétences dans un environnement sécurisé. Ces environnements ont montré leur intérêt pour la formation dans plusieurs corps de métier. Dans notre cas, nous visons l'acquisition d'un tel dispositif pédagogique immersif, avec des interfaces qui sont celles réellement utilisées pour les métiers de la cybersécurité : principalement tactiles (clavier, souris) et audiovisuelles (écrans, micro et casque).

L'objectif est ainsi de disposer d'un environnement virtuel de formation et de simulation pour la gestion de la Sécurité des Systèmes d'Information (SSI), sous la forme d'une plateforme opérationnelle de type cyber-range destinée principalement à la formation dans les apprentissages et les usages de la cybersécurité, mais aussi pour la recherche en cybersécurité des réseaux et des systèmes d'information.

Du point de vue de la formation, cet environnement sera utilisé dans un objectif pédagogique auprès d'étudiants/apprenants et de professionnels, spécialistes ou non de la SSI, de la simple sensibilisation à l'hygiène informatique jusqu'à la simulation de cyberattaques ou l'élaboration de plans de crise pour des organisations ou entreprises. Il faudra donc un environnement virtuel apportant des outils pertinents pour plonger l'infrastructure hybride simulée-physique au sein d'un trafic réaliste, des outils pour le suivi pédagogique des étudiants/apprenants et des outils pour l'adaptation des scénarii à son appropriation par l'étudiant/apprenant.

Du point de vue de la recherche, cet environnement servira de plateforme de tests des solutions d'autoprotection conçues et développées dans le cadre des travaux des équipes de recherche Lannionaises. En effet, les données collectées via cette plateforme (alerte, journaux, etc.) permettront de mettre en place dynamiquement et automatiquement des actions et des politiques de sécurité dont l'efficacité sera évaluée.

Cet environnement devra ainsi apporter des outils facilitant l'acquisition des aspects métier de la SSI, permettant de comprendre et d'améliorer les prises de décision ; des possibilités de pause et de rejou seront particulièrement appréciées.

Il est important que nous puissions disposer dès le début d'un ensemble opérationnel de scénarii génériques couvrant les grands classiques de la cybersécurité et mettant en œuvre des exemples avec des équipes blue, red, purple, green, yellow et white. Une fois la plateforme prise en main, nous définirons des scénarii spécifiques répondant aux besoins particuliers de l'écosystème, puis nous apprendrons à les implanter et à les animer sur la plateforme. Par ailleurs, nous souhaitons renforcer la résilience cyber des organismes et entreprises installés sur le territoire de Lannion par la pratique d'exercices de crise cyber adaptés à leurs besoins spécifiques. Aussi, nous envisageons d'organiser des événements de cybersécurité de type CTF (Capture The Flag) à destination des étudiants/apprenants des deux établissements (IUT et Enssat). Nous sommes également prêts à partager nos expériences avec d'autres utilisateurs de telles plateformes et de coorganiser des exercices de crise cyber à l'échelle régionale et nationale en nous appuyant sur l'interopérabilité des environnements.

Au-delà de l'utilisation pour des besoins cyber, cette plateforme de déploiement rapide de VMs pourrait être également utilisée dans le cadre de TP classiques qui, pour différentes raisons, utilisent une solution à base de VMs autonomes (environnement préprogrammé par un enseignant par exemple).

C. Listes des contacts

C.1. IUT

- Référente financière :
 - Tifenn Donguy – Tifenn.Donguy@univ-rennes.fr
- Référent pédagogique :
 - Mohamed-Aymen Chalouf – Mohamed.Chalouf@univ-rennes.fr
- Référents techniques
 - Cédric Faron – Cedric.Faron@univ-rennes.fr
 - Annie Rouxel – Annie.Rouxel@univ-rennes.fr

C.2. Enssat

- Référente financière :
 - Carole Perrot – Carole.Perrot@enssat.fr
- Référent pédagogique :
 - Pierre Alain – Pierre.Alain@enssat.fr
- Référents techniques
 - Stéphane Chehayed – Stephane.Chehayed@enssat.fr
 - Christophe Masson – Christophe.Masson@enssat.fr

D. Clauses techniques - Spécifications attendues

D.1. Avant-propos

Le marché est composé de 2 lots distincts :

- lot 1 : Acquisition d'un environnement virtuel de formation et simulation de type cyber-range pour l'IUT de Lannion ;
- lot 2 : Acquisition d'un environnement virtuel de formation et simulation de type cyber-range pour l'Enssat.

et d'un ensemble de prestations supplémentaires éventuelles (PSE).

Les paragraphes suivants vont décrire les attendus de la prestation.

Comme les deux lots sont très proches, quand rien n'est précisé, cela indique que la demande concerne les deux lots. Quand il y aura spécificité sur un lot, cela sera explicité par le tag [Lot 1 – IUT] ou [Lot 2 – Enssat].

Le soumissionnaire sera autorisé à proposer des variantes. De même, si dans le cadre de son offre, le soumissionnaire considère que des PSE sont obligatoires, il sera autorisé à le faire (il devra préciser les raisons de cette obligation).

L'IUT et l'Enssat se réservent le droit de faire une audition des soumissionnaires. Cette audition se ferait après l'ouverture des plis. Elle se ferait, **au choix du soumissionnaire**, en présentiel ou en visioconférence (zoom ou teams via un lien défini par l'IUT/Enssat). La durée serait de 1h30 par soumissionnaire (30 min de présentation et 1h d'échange).

D.2. Point particulier concernant le lot 2 – Enssat [Lot 2 – Enssat]

La plupart des solutions de type cyber-range incluent un packaging comprenant à la fois les aspects matériels (serveurs/commutateurs/baies) et logiciels.

Pour des questions budgétaires mais aussi parce que l'Enssat dispose de ressources de calculs disponibles (infrastructure VmWare, infrastructure KVM), l'Enssat limite le lot 2 à juste l'offre logicielle. Une PSE comprenant l'offre matérielle sera bien évidemment prévue afin de compléter la solution. Vu que cette demande est particulière, le soumissionnaire est autorisé à :

- préciser qu'il ne peut répondre juste avec l'offre logicielle et que sa réponse inclut, de manière obligatoire, la PSE "matérielle" pour être valide ;
- indiquer des réserves, en précisant lesquelles, sur le bon fonctionnement selon la compatibilité de l'infrastructure physique.

Le soumissionnaire devra également préciser les contraintes sur l'infrastructure physique (configuration des serveurs, des commutateurs, systèmes/versions, etc.) afin de supporter son offre logicielle.

D.3. Vocabulaire

- par matériel informatique, nous entendons tout élément physique constitutif d'un système d'information : serveur, switch, routeur, câble Ethernet, Wifi, Bluetooth, terminal, système industriel spécifique, portable, tablette, mobile, objet connecté, clé usb, etc. ;
- par virtualisation ou machine virtuelle ou VM, nous entendons toute technologie permettant de simuler ou d'émuler un matériel physique ou une application dans un environnement contrôlé (y compris des technologies plus légères comme docker) ;
- par infrastructure, nous entendons l'ensemble de matériels informatiques et de machines virtuelles interconnectés à travers un réseau, qu'il soit matériel, virtuel ou hybride ;
- par environnement de simulation, nous entendons une instance d'une infrastructure et du scénario qui a été déployée pour et est utilisée par un utilisateur ou un groupe d'utilisateurs ;
- par scénario pédagogique, nous entendons l'ensemble des situations organisées dans le temps avec les infrastructures associées qui permet par l'expérimentation, la collaboration et l'exploration d'amener progressivement l'étudiant/apprenant aux savoir-faire et compétences qu'il convient de développer pour cette formation (sensibilisation, pentesting, défense, durcissement, sécurisation, etc.) ;
- par solution, nous entendons l'ensemble de la solution proposée : infrastructure et environnement de formation et de simulation ;
- par formateur, qu'il soit humain ou virtuel, nous entendons entité dont l'objectif est d'estimer la zone proximale de développement des étudiants/apprenants et d'adapter la difficulté du scénario à la capacité de réponse de l'équipe formée, en jouant, par exemple, sur les paramètres au sein de chaque situation, sur le nombre de situations simultanées ou sur la fréquence de leurs apparitions.

D.4. Dimensionnement de la solution

D.4.1. [Lot 1 – IUT]

La solution doit être en mesure de supporter des simulations de 120 machines virtuelles interconnectées selon tout type d'architecture réseau. Ce qui correspond à 2 groupes de TP de 14 élèves et un total de 28 utilisateurs.

Elle doit exceptionnellement accepter jusqu'à 42 utilisateurs simultanés dans une configuration plus limitée, répartis dans une ou plusieurs salles de l'IUT de Lannion, en utilisant les ordinateurs de ces salles avec un accès réseau au Gigabit. Ainsi, il devra être possible de connecter la solution au cœur de réseau avec une capacité montante de 10 Gbits/s.

Une PSE permettant un passage à 3 groupes TP simultanés soient 42 étudiants et 180 machines virtuelles sera proposée.

D.4.2. [Lot 2 – Enssat]

La solution doit être en mesure de supporter des simulations de 128 machines virtuelles interconnectées selon tout type d'architecture réseau, ce qui correspond à 2 groupes de TP de 16 élèves chacun.

Une PSE permettant un passage à 3 groupes simultanés soient 48 élèves et 192 machines virtuelles sera proposée.

Une seconde PSE permettant un passage à 4 groupes simultanés soient 64 élèves et 256 machines virtuelles sera également proposée.

D.5. Accessibilité de la solution

Le soumissionnaire indiquera les moyens d'accès à la solution (ligne de commande, interface graphique via une application dédiée, navigateur Firefox, Edge et Chrome). En cas d'utilisation d'une application dédiée, le soumissionnaire précisera les systèmes d'exploitation supportés (Windows, Linux, Mac).

L'accès à l'environnement virtuel de formation et simulation doit être possible à la fois depuis notre réseau local (salles de TP) mais également à travers un accès externe : nos partenaires locaux (le lycée Félix Le Dantec, IUT/Enssat), d'autres universités à travers le réseau RENATER, ou depuis n'importe quel poste authentifié à travers tout réseau offrant un débit suffisant pour que l'immersion dans l'environnement virtuel soit possible.

Le soumissionnaire précisera si la solution dispose d'une interface dédiée pour toutes les opérations de type « administration de la solution ».

D.6. Description de l'infrastructure

Les choix technologiques pour la virtualisation devront être clairement explicités. Le type de « Licensing » de la solution sera explicité.

Le soumissionnaire devra notamment préciser quel type de machines virtuelles sont supportées (containerisation, « machines lourdes », etc.) en précisant les types d'OS supportés.

Le soumissionnaire devra indiquer comment sont virtualisés les matériels réseaux et précisera les possibilités de gestion des différentes marques, firmware et versions d'OS.

Le soumissionnaire devra également détailler l'infrastructure physique proposée (serveurs : CPU/mémoire/interfaces réseaux (SFP+ pour les interfaces 10G)/disques, commutateurs, etc.) en précisant bien les éléments de redondance. Il devra également préciser si l'accès aux systèmes « bare-métal » est possible ou pas.

Les infrastructures virtuelles doivent pouvoir s'interconnecter aisément avec différents matériels informatiques, comme, par exemple, des ordinateurs physiques (PC fixe ou portables, tablettes, téléphones, etc.), des équipements réseau (bornes Wifi, commutateurs, routeurs, firewall) ou des objets connectés établissant ainsi des infrastructures hybrides. Le soumissionnaire précisera si ce matériel peut être déporté sur le LAN ou le WAN. Le soumissionnaire précisera également la possibilité de donner ou pas un accès Internet à l'infrastructure.

D.7. Authentification

L'accès à la solution se fera après une authentification simple. Le soumissionnaire précisera si une authentification forte ou à double facteur est disponible, notamment pour les rôles d'administration.

Le soumissionnaire précisera si l'authentification peut s'appuyer sur nos annuaires LDAP. Dans ce cas le soumissionnaire devra indiquer les mécanismes d'import, de filtrage disponible ainsi que la disponibilité de la délégation d'authentification à ce dernier (pas de conservation des empreintes des mots de passe sur la solution). En complément de l'utilisation de cet annuaire, l'utilisation possible de comptes locaux (invités, etc.) sera précisée.

Si la solution ne permet pas d'utiliser nos annuaires, le soumissionnaire devra décrire les mécanismes disponibles pour la création/import des comptes.

La gestion de la suppression des comptes et des données des utilisateurs sera explicitée (dans le cadre de l'utilisation de nos annuaires et dans le cas de comptes locaux).

D.8. Gestion des droits

Le soumissionnaire indiquera les possibilités concernant la gestion des droits et les délégations possibles :

- pour l'accès à la plateforme ;
- pour l'administration de la plateforme ;
- pour la gestion d'un environnement de simulation : droit « enseignant » (création, modification, lancement, supervision, etc.) et « élève » (création, modification, lancement, arrêt, accès, snapshot des VM, etc.). Le soumissionnaire devra également indiquer si ces droits peuvent être limités à un environnement de simulation particulier ou à des groupes d'environnements de simulation ;
- pour l'utilisation d'un environnement de simulation : visualisation que d'une partie de l'environnement, accès limité à la console de certaines machines virtuelles, etc. ;
- notion de groupes ;
- délégation possible.

D.9. Sauvegarde de la plateforme

Les possibilités de sauvegarde et de restauration de la plateforme seront explicitées :

- sauvegarde partielle des données : configuration, données utilisateurs, scénarii, etc. ;
- sauvegarde complète (y compris les VM) : incrémentales, totales, protocole disponible, etc.

Le soumissionnaire indiquera également si des mécanismes de snapshots sont disponibles notamment lors de modification de la configuration.

D.10. Mise à jour de la plateforme

La mise à jour de la plateforme est un enjeu important et potentiellement très consommateur de temps.

Le soumissionnaire devra présenter les mécanismes disponibles pour ces mises à jour (logiciel de gestion, scénarii, machines virtuelles packagées dans la solution, machines virtuelles ajoutées/gérées par nous, etc.). Il devra notamment préciser quel impact a la mise à jour d'une machine virtuelle sur un scénario qui utilise cette machine virtuelle.

D.11. Constructions d'un environnement de formation et de simulation

Les interfaces utilisateurs donnant accès aux fonctionnalités facilitant la construction des environnements de formation et de simulation devront montrer une ergonomie en accord avec nos besoins d'individualisation de la formation afin d'éviter les manipulations répétitives, par exemple, en générant les infrastructures à partir d'un modèle paramétré d'infrastructure pour un ensemble de paramètres, et en accord avec nos besoins d'élaboration d'architectures complexes. Un environnement de formation et de simulation, que ce soit pour le travail individuel ou le travail en groupe, doit permettre d'implanter des infrastructures composées et connectées sans limite logique ou casi sur le nombre de machines virtuelles.

L'environnement doit permettre d'importer et d'exporter des machines virtuelles aux formats standards existants.

Le soumissionnaire précisera les environnements de simulation/architectures/machines virtuelles disponibles par défaut dans la solution.

Le soumissionnaire exposera également les mécanismes mis en œuvre lors de l'utilisation d'un même élément dans plusieurs environnements de formation et de simulation.

D.12. Déploiement d'un environnement de simulation

Le soumissionnaire explicitera les mécanismes de déploiement des environnements de simulation (liste non exhaustive) :

- déploiement d'une instance ;
- délégation possible du déploiement aux élèves ;
- déploiement automatique de plusieurs instances et attribution de droit d'un élève ou d'un groupe à une instance ;
- automatisation du déploiement via un agenda.

D.13. Utilisation d'un environnement de simulation

Les étudiants/apprenants doivent pouvoir travailler seuls (un environnement de simulation par étudiant/apprenant) ou en groupes (un environnement de simulation par groupe d'étudiants/apprenants). Les environnements de simulation doivent pouvoir être paramétrables, composables et connectables et déployables en plusieurs instances.

Le soumissionnaire précisera si la possibilité de former les étudiants/apprenants à la sécurité par le biais des concepts et techniques des jeux sérieux est disponible sur la solution proposée.

Le soumissionnaire indiquera les possibilités d'interaction avec les différents éléments de l'environnement virtuel (y compris les flux réseaux) notamment mais de manière non exclusive :

- accès aux différents éléments (machines, réseaux, etc.) : console, CLI, GUI, applicatif (web), configuration réseau, mémoire, etc. ;
- injection de trafic réseau ;
- analyse de trafic réseau en direct ;
- log ;
- enregistrement des événements, analyse et retour sur ces événements (revoir le contenu des paquets par exemple) avec tous les mécanismes de filtrage et de recherche ;
- gel du temps.

Le soumissionnaire précisera les possibilités offertes en termes de sauvegarde des modifications faites par les élèves sur les différents éléments de l'environnement de simulation notamment dans le cas d'un TP/Projet sur plusieurs séances.

D.14. Scénarii pédagogiques

La gestion des scénarii est un élément indispensable de la solution. Pour chacun des items suivants, le soumissionnaire détaillera les fonctionnalités disponibles.

D.14.1. Simulation de trafic réseau réaliste

L'environnement de simulation étant indépendant du réseau réel, le soumissionnaire précisera les fonctionnalités offertes en termes de simulation de trafic : disponibilité d'un générateur de trafic, capacité de ce générateur à jouer en boucle des enregistrements de trafic réseau et capacité à générer des flux respectant au moins un modèle pseudo-aléatoire simple. Les modèles proposés seront explicités et s'efforceront d'être le plus réalistes possible.

D.14.2. Surveillance des étudiants/apprenants et contrôle des scénarii

Le soumissionnaire précisera les possibilités de surveillance des étudiants/apprenants, des environnements de simulations en cours d'utilisation, le tout avec une interface ergonomique affichant les propriétés des ressources utilisées et permettant la prise en main à distance.

La construction des scénarii s'appuie sur une organisation temporelle de situations associées à une infrastructure mettant les étudiants/apprenants dans un contexte propice à l'acquisition de compétences par l'expérimentation. Le soumissionnaire explicitera les possibilités offertes par sa solution et indiquera les moyens ergonomiques afin de construire ces contextes, puis de les mettre en œuvre lors des expériences.

Les contrôles d'un scénario sont essentiels pour adapter l'expérience pédagogique aux contraintes apportées par les utilisateurs. Il faudrait pouvoir mettre en pause, continuer, interrompre, sauvegarder et reprendre un scénario. Il faudrait aussi pouvoir accélérer, ralentir, réorganiser en cours d'exercice l'enchaînement des situations caractéristiques du scénario, ajouter ou retirer des ressources (matériel, virtualisation, étudiant/apprenant, formateur, etc.). Pour tous ces points, le soumissionnaire indiquera les possibilités de sa solution.

Pour finir, le soumissionnaire indiquera si une API donnant accès aux fonctionnalités proposées dans les interfaces graphiques est disponible.

D.14.3. Scénarii génériques de formation aux risques cyber

Le soumissionnaire indiquera le panel de scénarii prêts à l'emploi disponible par défaut dans sa solution. Le soumissionnaire précisera si cet ensemble de scénarii et d'infrastructures génériques correspondant à des techniques et tactiques de cybersécurité récentes (moins de trois ans) et sensibilisant aux 4 types de risques cyber : la cybercriminalité, l'atteinte à l'image, l'espionnage et le sabotage. La réunion de ces scénarii génériques devrait couvrir au mieux les différents rôles que l'on peut trouver en gestion des risques dans la littérature sur les cyber-range : l'équipe rouge (attaque), l'équipe bleue (défense), l'équipe verte (légitime), l'équipe jaune (infecté), l'équipe pourpre (communicant) et l'équipe blanche (formateur).

D.15. Ouverture et coopération

Afin d'éviter tout désagrément pour la communauté universitaire et les éventuels partenaires, les prestataires concevant une solution logicielle s'engagent à respecter les règles de sécurité et les bonnes pratiques en vigueur en matière de développement, à respecter la Politique de Sécurité des Systèmes d'Information de l'Etat et des clauses SSI applicables à l'infogérance, à permettre l'installation des mises à jour de sécurité régulières et à chiffrer les flux de données entre les différents composants logiciels (cf. document « POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT de l'ANSSI » joint au dossier).

Le soumissionnaire indiquera si l'environnement virtuel de formation et simulation permet le partage et l'interopérabilité avec d'autres plateformes de ce type, notamment :

- import et export de scénarios et infrastructures de cybersécurité, préciser également le format d'import/export ;
- connexion des infrastructures entre plusieurs plateformes de type cyber-range et déroulement de scénarii complexes s'appuyant sur la réunion de ces infrastructures.

Les infrastructures et les scénarii génériques doivent être utilisables sans restriction d'usage par l'IUT de Lannion et par l'Enssat, dans le cadre de leurs différentes formations et travaux de recherche, y compris formation professionnelle, formation continue et formation par apprentissage et dans le cadre des travaux de recherche en cybersécurité des équipes de l'IRISA (par exemple, l'équipe SOTERN).

Les scénarii et infrastructures développées par l'IUT de Lannion et par l'Enssat doivent rester leur entière propriété et doivent être utilisables sans aucune restriction d'usage. Néanmoins, ces scénarii, ainsi que les failles détectées pourront, bien évidemment, être partagés avec d'autres utilisateurs notamment via des plateformes communautaires.

D.16. Extensibilité de la solution

Le soumissionnaire indiquera les possibilités d'extensibilité de sa solution. Il précisera notamment les conditions légales et techniques de ces extensions, l'impact sur les licences, etc.

Les extensions que nous souhaitons voir détaillées sont les suivantes :

- ajout de mémoire ;
- ajout de disque ;
- ajout d'interfaces réseaux ;
- ajout de nœud "esclave".

A titre d'exemple, nous souhaiterions les réponses aux questions suivantes dans le cadre de l'item « ajout de mémoire » :

- Combien de slots mémoire restent disponibles sur la machine physique ?
- Sommes-nous autorisés à rajouter de la mémoire nous-même sans passer par vous ?
 - Si oui, quel impact a cette opération, sur la licence, sur la garantie matérielle ?

E. Garantie, contrat de maintenance, communauté d'utilisateurs

La solution proposée devra inclure une maintenance matérielle et logicielle de 1 an à date de la recette (support téléphonique ou par ticket, mise à jour logicielle, support matériel, télémaintenance, etc.).

Le soumissionnaire devra indiquer les conditions précises de cette maintenance (à minima sur site J+3 5j/7 pour la partie matérielle), notamment et de manière non exhaustive : le contenu, les délais d'intervention, les délais de réparation, les modalités d'accès, la langue utilisée pour le support, sur site, retour atelier, etc.

Le soumissionnaire devra également indiquer le coût annuel de ce même niveau de maintenance matérielle et logicielle pour l'année N+2 ainsi que la règle de calcul pour l'évolution du coût pour les années suivantes.

Concernant les aspects matériels (serveurs), le soumissionnaire précisera le cycle de vie de ce matériel (plus de support au-delà de 5 ans, 7 ans, etc.).

Concernant les aspects logiciels, le soumissionnaire précisera si la licence est une licence à perpétuité ou en location et si la licence est attachée à un matériel dédié ou peut être transférée sur un autre serveur.

Des PSE seront proposées incluant différents types de maintenance et de durée.

Le soumissionnaire pourra indiquer si des groupes d'utilisateurs existent. Dans ce cas, il précisera les modalités d'accès, les avantages spécifiques, etc.

F. Formations

Une offre de formation devra être proposée par le soumissionnaire. Vu que ce marché inclut 2 lots distincts, la formation fait l'objet de PSE puisque la formation sera mutualisée entre l'IUT et l'Enssat si les 2 établissements prennent le même titulaire.

La formation se fera sur site (IUT et/ou Enssat). Elle sera effectuée de préférence sur les nouvelles plateformes installées. La formation sera accompagnée d'une documentation au format numérique. La formation devra couvrir tous les aspects d'utilisation/administration de la plateforme. Le soumissionnaire indiquera ses besoins en termes de logistique nécessaire au bon déroulement de la

formation. La formation devra être réalisée courant 2023 et dans les 15 jours qui suivent la recette de la solution.

La formation sera découpée en deux modules :

- à destination des utilisateurs finaux (enseignants/formateurs) ;
- à destination des opérateurs techniques de la plateforme (techniciens).

Le module « utilisateurs finaux » comprendra au maximum 12 personnes dans le cas d'une formation mutualisée et 6 personnes dans le cas d'une formation individualisée par établissement ; concernant le module « opérateurs techniques », ce sera respectivement 8 et 4.

Pour chacun de ces modules, le soumissionnaire indiquera la durée prévue des formations ainsi que les thèmes abordés.

G. Modalités d'installation et de réception de la solution

G.1. Installation de la solution

G.1.1. [Lot 1 - IUT]

L'environnement virtuel de formation et simulation de type cyber-range pour l'IUT de Lannion sera déployé physiquement dans les locaux de l'IUT de Lannion. Pour cela, une baie informatique standard dans la salle serveur du bâtiment 10 sera mise à disposition. Cette salle dispose des fonctionnalités classiques d'un petit centre de calcul : onduleur, double adduction électrique (non ondulé et ondulé), climatisation. Le(s) kit(s) de rack devra(ont) être compris dans l'offre.

Il sera connecté sur le réseau de l'IUT via une interface cuivre ou optique 10Gb en mode trunk pour permettre le multi vlan. Des interfaces Giga doivent être disponibles en redondance pour la connexion au réseau et l'administration de la plateforme.

L'ensemble des équipements de la plateforme de cybersécurité sera livré à destination franco de port. Le transport s'effectuera sous la responsabilité des titulaires du marché jusqu'au lieu de livraison spécifié ci-après. Une pré-visite sera organisée pour faciliter la logistique et pour juger au mieux du matériel nécessaire pour l'installation. Le conditionnement, le chargement, l'arrimage, le déchargement et l'installation dans la salle des serveurs du bâtiment 10 de l'IUT de Lannion seront effectués sous leur responsabilité.

Les titulaires du marché assureront l'intégralité de l'installation des raccordements électriques et réseaux et de la mise en service des équipements livrés (en coordination avec le service informatique de l'IUT de Lannion), lors de la mise en service.

Le soumissionnaire devra en outre préciser dans son offre tous les attendus en termes de connexions physiques (réseaux, électricité, etc.) et logiques (@IP, routeur, etc.).

Concernant la réception des colis, l'IUT pourra réceptionner les colis en s'assurant juste qu'extérieurement les cartons sont en bon état.

G.1.2. [Lot2 – Enssat]

L'environnement virtuel de formation et simulation de type cyber-range pour l'Enssat sera physiquement déployé dans une baie informatique standard (19", 100 cm de profondeur) dans le centre de calcul principal de l'Enssat. Ce centre de calcul dispose des fonctionnalités classiques d'un petit centre de calcul : onduleur, double adduction électrique (non ondulé et ondulé), climatisation. Au niveau réseau, il sera connecté sur le cœur du réseau de l'Enssat (10Gb) dans un vlan particulier (plus un vlan d'administration supplémentaire si la solution gère cette séparation).

Dans le cas où la solution proposée est une solution complète (matériel et logiciel), le soumissionnaire indiquera si le matériel est rackable ou pas. Dans le cas où le matériel est rackable, le(s) kit(s) de rack devra(ont) être compris dans l'offre. Le soumissionnaire devra en outre préciser dans son offre tous les attendus en termes de connexions physiques (réseaux, électricité, etc.) et logiques (@IP, routeur, etc.). Les actions suivantes seront à la charge du titulaire du marché : transport vers l'Enssat, transport depuis le local de livraison jusqu'au local d'installation (même bâtiment, même étage) déballage, gestion des déchets (le titulaire du marché pourra utiliser les containers présents à l'Enssat), conformité de la livraison, installation, connexion, configuration, intégration au SI de l'Enssat, mise en service. Concernant la réception des colis, l'Enssat pourra réceptionner les colis en s'assurant juste qu'extérieurement les cartons sont en bon état.

Dans le cas où la solution proposée ne comprend que la partie logicielle, Le titulaire du marché devra fournir un manuel d'installation. L'installation est à notre charge, le titulaire du marché devra proposer un support pour l'installation dans le cadre de son offre de support et maintenance classique. Une PSE sera proposée incluant l'installation sur notre infrastructure. Pour mémoire, le soumissionnaire devra préciser les attendus en termes de matériels et logiciels afin de permettre l'installation et le support de sa solution.

G.1.3. Adresses de livraison

IUT de Lannion
Bâtiment 10, Salle 026
Rue Edouard Branly
22300 Lannion
France

ENSSAT
Bâtiment 1, Salle 001D
6 rue de Kerampont
22300 Lannion
France

Une visite pourra être organisée sur demande des soumissionnaires du marché de manière à vérifier les prérequis des baies devant accueillir les solutions.

G.2. Délai de livraison – Date de facturation

La date de livraison sur site sera fixée en accord avec l'acheteur et devra être antérieure au 1^{er} décembre 2023.

La date de facturation devra impérativement être antérieure au 31 décembre 2023.

G.3. Phase de test et de recette

La phase de recette sera faite en présence de l'acheteur et devra à minima valider les fonctionnalités suivantes :

- démarrage de la plateforme ;
- connexion en tant qu'administrateur à la plateforme ;
- ajout d'un compte à la plateforme ;
- connexion en tant qu'utilisateur à la plateforme ;
- lancement d'un scénario simple pré-fournis ;
- utilisation de ce scénario pour 2 « groupes d'élèves » ;
- modification simple de ce scénario ;
- arrêt de la plateforme.

De plus le titulaire du marché devra rendre un livrable, au format électronique, comprenant toutes les opérations qui ont été menées par lui dans le cadre de l'installation/configuration de la solution sur site.

Pour finir, le titulaire du marché devra fournir tous les éléments suivants :

- la documentation technique nécessaire à une utilisation optimale des équipements livrés et à son utilisation courante ;
- le schéma de l'installation (câblage, etc.) ;
- les binaires, code de licence, sauvegarde de l'environnement, etc. permettant une réinstallation en cas de « crash » complet de la solution.

H. Format de la réponse

Le soumissionnaire remettra un mémoire technique répondant point par point à tous les paragraphes en précisant le numéro du paragraphe. Pour chaque paragraphe, la réponse sera scindée en deux parties :

- une première partie qui répondra explicitement à nos questions/demandes d'explications ;
- une seconde partie libre où le soumissionnaire pourra compléter sa réponse (fonctionnalités complémentaires connexes, précisions, etc.) en mettant des liens vers tous types de documents qu'il juge utiles à sa réponse.

En avant-propos de ce mémoire technique, le soumissionnaire donnera les informations suivantes :

- présentation de l'entreprise (nom de l'entreprise, effectifs, localisation, etc.) ;
- liste de références concernant des prestations similaires à la prestation demandée (nom du client, date de la prestation, contact chez le client, brève description de la prestation) afin de pouvoir évaluer l'expérience de l'entreprise concernant les prestations objets de ce marché ;
- présentation de l'organisation du projet (nom du chef de projet, contact administratif et technique, etc.) ;
- calendrier envisagé à compter de la date de notification du marché.

Dans le cas où le soumissionnaire ne peut pas répondre à un attendu, il le précisera clairement en indiquant les limites de sa solution, une éventuelle disponibilité dans une future version (préciser dans ce cas la date de disponibilité de cette version). Sa proposition sera malgré tout acceptée, la note technique sera de facto affectée.

Concernant le prix global forfaitaire pour chaque lot, celui-ci sera détaillé à minima suivant les items suivants :

- matériel et logiciel ;
- maintenance pour la première année ;
- livraison/installation.

I. Développement durable et responsabilité sociétale

Le soumissionnaire nous informera des actions menées par son entreprise dans le cadre du développement durable et de la responsabilité sociétale : BGES, égalité salariale femme/homme, emploi des seniors, emplois des jeunes/apprentis, etc.

J. Listes des prestations supplémentaires éventuelles

Le soumissionnaire est autorisé à ne pas répondre à toutes les PSE.

J.1. [Lot2 – Enssat] PSE 2.1

Dans le lot 2, l'Enssat ne demande que la partie logicielle de la solution. Il s'agit ici de proposer le supplément pour le packaging standard incluant le matériel physique : serveurs, commutateurs, etc.

J.2. Solution de mobilité

Les solutions de type cyber-range sont souvent proposées avec un packaging permettant une mobilité de la solution.

J.2.1. [Lot1 – IUT] PSE 1.1

Supplément afin d'assurer la mobilité de la solution.

J.2.2. [Lot2 – Enssat] PSE 2.2

Supplément afin d'assurer la mobilité de la solution.

J.3. Augmentation du dimensionnement de la solution

J.3.1. [Lot 1 – IUT] PSE 1.2

Complément pour que la solution soit en mesure de supporter 3 groupes de TP simultanés soient 42 étudiants et 180 machines virtuelles.

J.3.2. [Lot 2 – Enssat] PSE 2.3

Complément pour que la solution soit en mesure de supporter 3 groupes simultanés soient 48 élèves et 192 machines virtuelles.

J.3.3. [Lot 2 – Enssat] PSE 2.4

Complément pour que la solution soit en mesure de supporter 4 groupes simultanés soient 64 élèves et 256 machines virtuelles.

J.4. Connexion de matériel physique « délocalisé »

Afin d'avoir une infrastructure hybride, il est nécessaire de connecter le matériel physique sur le commutateur directement piloté par la solution. Certaines solutions ont la possibilité de déporter ce matériel physique en un point quelconque du réseau interne (sous réserve bien sûr d'une connectivité IP).

J.4.1. [Lot 1 – IUT] PSE 1.3

Complément pour que la solution permette la connexion de matériels physiques délocalisés par rapport à la plateforme ; ce matériel participant à une infrastructure hybride.

J.4.2. [Lot 2 – Enssat] PSE 2.5

Complément pour que la solution permette la connexion de matériels physiques délocalisés par rapport à la plateforme ; ce matériel participant à une infrastructure hybride.

J.5. [Lot2 – Enssat] PSE 2.6

Dans le lot 2, l'Enssat ne demande que la partie logicielle de la solution, en prenant à sa charge l'installation de la solution sur son infrastructure physique. Il s'agit ici de proposer le supplément pour que l'installation de la solution logicielle soit à la charge du soumissionnaire. Un transfert de compétence ainsi qu'un document de recette devra être inclus dans la proposition.

J.6. Formation

Merci de vous reporter au paragraphe « F » concernant le détail de la formation. Pour rappel, la formation est scindée en 3 PSE puisque la formation sera mutualisée entre l'IUT et l'Enssat si les 2 établissements prennent le même titulaire. L'option J.6.3 est donc mutuellement exclusive des options J.6.1 et J.6.2.

J.6.1. [Lot 1 – IUT] PSE 1.4

Offre du soumissionnaire concernant la formation individualisée pour l'IUT de Lannion. Le module « utilisateurs finaux » comprendra au maximum 6 personnes et le module « opérateurs techniques » au maximum 4 personnes.

J.6.2. [Lot 2 – Enssat] PSE 2.7

Offre du soumissionnaire concernant la formation individualisée pour l'Enssat. Le module « utilisateurs finaux » comprendra au maximum 6 personnes et le module « opérateurs techniques » au maximum 4 personnes.

J.6.3. PSE X.1

Offre du soumissionnaire concernant la formation mutualisée pour l'IUT de Lannion et pour l'Enssat. Le module « utilisateurs finaux » comprendra au maximum 12 personnes et le module « opérateurs techniques » au maximum 8 personnes.

J.7. Maintenance

Il s'agit ici d'avoir des offres sur différents niveaux de maintenance. De manière globale, le prestataire précisera le niveau exact de la maintenance. Le soumissionnaire est autorisé à proposer d'autres types ou modalités de maintenance.

J.7.1. [Lot 1 – IUT] PSE 1.5

Complément pour une maintenance matérielle sur site en GTI à J+3 5j/7 de 4 ans au-delà de la maintenance initiale de 1 an donnant une maintenance matérielle sur 5 ans au total.

J.7.2. [Lot 1 – IUT] PSE 1.6

Complément pour une maintenance matérielle sur site en GTI à J+3 5j/7 de 6 ans au-delà de la maintenance initiale de 1 an donnant une maintenance matérielle sur 7 ans au total.

J.7.3. [Lot 1 – IUT] PSE 1.7

Complément pour une maintenance logicielle : support téléphonique ou par ticket (délai GTI à J+3 5j/7), mise à jour (mineure/majeure) logicielle, télémaintenance de 2 ans au-delà de la maintenance initiale de 1 an donnant une maintenance logicielle de 3 ans au total.

J.7.4. [Lot 2 – Enssat] PSE 2.8

Complément pour une maintenance matérielle sur site en GTI à J+3 5j/7 de 4 ans au-delà de la maintenance initiale de 1 an donnant une maintenance matérielle sur 5 ans au total.

J.7.5. [Lot 2 – Enssat] PSE 2.9

Complément pour une maintenance matérielle sur site en GTI à J+3 5j/7 de 6 ans au-delà de la maintenance initiale de 1 an donnant une maintenance matérielle sur 7 ans au total.

J.7.6. [Lot 2 – Enssat] PSE 2.10

Complément pour une maintenance logicielle : support téléphonique ou par ticket (délai GTI à J+3 5j/7), mise à jour (mineure/majeure) logicielle, télémaintenance de 2 ans au-delà de la maintenance initiale de 1 an donnant une maintenance logicielle de 3 ans au total.