Accélérateur
de la transformation
numérique

# Catalogue des modules de formation de SystemX Academy

**Modules co-construits et co-dispensés avec des partenaires de l'IRT SystemX**

Accélérateur de la transformation numérique

# Sciences des données et intelligence artificielle en Industrie 4.0

**Formation dans le cadre du certificat Industrie du Futur en partenariat avec Paris Dauphine-PSL**

| | |
|---|---|
| **Modalité et lieu de la formation** | Hybride (en ligne et dans les locaux de Paris Dauphine-PSL à Paris (75775 PARIS)) |
| **Type de formation SystemX Academy** | Advanced@SystemX |
| **Catégorisation dans les domaines S&T de l'IRT SystemX** | Sciences des données et IA |
| **Public** | Chef de projets industriels, Chef de projets logistiques, Chef de projets transformation numérique, Directeur industriel, Directeur d'usine et Supply Chain Manager |
| **Durée (en jour)** | 1 jour |
| **Descriptif du partenaire académique associé à la formation** | Formation continue de l'Université Paris Dauphine-PSL (Executive Education) |
| **Date de la session** | Nous contacter pour les sessions à venir |
| **Objectifs de la formation** | • Apprendre les concepts clés de data sciences et management des connaissances, Big data, data analytics<br>• Explorer des concepts clés en intelligence artificielle: machine learning, deep learning, natural language processing, vision et pattern recognition<br>• Illustrer les applications en Industrie 4.0 |
| **Contenu et points forts** | • Une sensibilisation à des thématiques innovantes de l'industrie du futur<br>• Illustration des projets de R&D (recherche et développement) de l'IRT SystemX à fort impact dans le domaine de la science des données<br>• Intervenant expert du sujet et la possibilité d'échanger et de discuter avec l'intervenant et les experts de l'IRT SystemX |
| **Prérequis** | Bac+4 et disposer d'une connaissance générale sur le sujet de l'industrie 4.0 |
| **Certificat** | Certificat Industrie du Futur de Paris Dauphine-PSL |

Accélérateur de la transformation numérique

# OpenAltaRica pour les études de sûreté de fonctionnement

**Offre de formation de sensibilisation opérée par l'IRT SystemX**

| | |
|---|---|
| **Modalité et lieu de la formation** | Hybride (en ligne et dans les locaux des apprenants de la formation) |
| **Type de formation SystemX Academy** | Awareness@SystemX |
| **Catégorisation dans les domaines S&T de l'IRT SystemX** | Ingénierie système et sûreté de fonctionnement |
| **Public** | Chef de projets industriels, ingénieurs généralistes |
| **Durée (en jour)** | 1 jour |
| **Date de la session** | Nous contacter pour les sessions à venir |
| **Objectifs de la formation** | • Maitrise du vocabulaire sûreté de fonctionnement et MBSA<br>• Compréhension des concepts clés de l'ingénierie système<br>• Prise en main du langage AltaRica et de la plateforme OpenAltaRica associée<br>• Construction de premières études de sûreté de fonctionnement avec une approche MBSA/AltaRica |
| **Programme** | • Introduction à la sûreté de fonctionnement et à MBSA<br>• Pourquoi le langage AltaRica ?<br>• Installation et manipulation de la plateforme OpenAltaRica<br>• Premiers exemples avec manipulations<br>• Représentation des patterns classiques (redondances, défaillances de cause commune, etc.)<br>• Structuration des modèles (modélisation orientée objet et prototype)<br>• Chaîne de traitement des modèles (par arbres de défaillance, par simulation stochastique) |
| **Prérequis** | Aucun |

Accélérateur de la transformation numérique

# Former à la conception et à l'implémentation d'une application Blockchain

**Formation certifiante en partenariat avec Télécom Paris Executive Education**

| | |
|---|---|
| **Modalité et lieu de la formation** | En présence dans les locaux de Télécom Paris Executive Education (Paris, 15e) |
| **Type de formation SystemX Academy** | Advanced@SystemX |
| **Catégorisation dans les domaines S&T de l'IRT SystemX** | Sécurité numérique et Blockchain |
| **Public** | Développeurs et des architectes souhaitant acquérir les connaissances suffisantes pour pouvoir évaluer l'opportunité de l'utilisation de cette technologie pour développer des applications se basant sur la blockchain |
| **Durée (en jour)** | 3 jours |
| **Descriptif du partenaire académique associé à la formation** | Formation continue de Télécom Paris Executive Education : L'organisme de formation continue de Télécom Paris |
| **Date des sessions** | Nous contacter pour les sessions à venir |
| **Objectifs de la formation** | • Comprendre les enjeux industriels et économiques de la Blockchain<br>• Comprendre les fondements de cette technologie<br>• Mesurer les apports et les limites de la Blockchain par rapport à un cas d'usage |
| **Points forts de la formation** | La formation présente les différents aspects de cette technologie, depuis les bases et leurs applications aux chaînes publiques (Bitcoin par exemple) jusqu'aux fonctionnalités avancées comme les contrats intelligents (Smart Contracts) et les chaînes privées à contrôle d'accès, sans oublier ses limitations intrinsèques. |
| **Programme** | **ENJEUX ECONOMIQUES DES BLOCKCHAINS**<br>• Analyse des éléments disruptifs<br>• Propriétés économiques des blockchains<br>• Blockchain et économie de la sécurité |

| | |
|---|---|
| | • Smart contracts, forks et oracles<br>**ASPECTS JURIDIQUES DE LA BLOCKCHAIN**<br>• Statut législatif des cryptomonnaies et tokens<br>• Réglementation sur les Initial Coin Offering (ICO)<br>• Régime juridique du smart contract<br>• Initiatives de régulation en cours au niveau français<br>• GDPR, droit à l'oubli et blockchain<br>• Blockchain comme register<br>**FONDEMENTS DE LA BLOCKCHAIN**<br>• Les blockchains ouvertes<br>• Le fonctionnement des blockchains, Bitcoin<br>• Notions d'économie, les risques des cryptomonnaies<br>• Blockchains privées, smart contracts, démonstrations<br>• Utilité de la blockchain dans un contexte économique<br>**TOUR D'HORIZON DES TECHNOLOGIES BLOCKCHAIN**<br>• Algorithmes de consensus<br>• Fonctionnement des smart contracts<br>• Propriétés de sécurité et limites…<br>**TRAVAUX PRATIQUES : MISE EN ŒUVRE D'UN RESEAU BLOCKCHAIN**<br>• Gestion d'un nœud blockchain (configuration, monitoring, archivage)<br>• Sensibilisation aux enjeux de sécurité (gestion des permissions, limitations du protocole de consensus)<br>**PANORAMA DES CAS D'USAGES INDUSTRIELS DE LA BLOCKCHAIN**<br>• Energie : Autoconsommation collective d'énergie renouvelable<br>• Véhicule : Passeport du véhicule connecté<br>• Paiement : Application de payement basé sur les cryptomonnaies<br>**TRAVAUX PRATIQUES : REALISATION D'UNE APPLICATION A BASE DE SMART CONTRACT**<br>• Introduction des primitives cryptographiques (hash, signature, commitment)<br>• Illustration des mécanismes au travers d'une étude de cas |
| **Prérequis** | Notions de bases en sécurité informatique sont souhaitables pour tirer un meilleur profit de cette formation La connaissance d'un langage de programmation (Javascript, Python, etc.) est indispensable pour la partie pratique |
| **Certificat** | Certificat délivré par Télécom Paris Executive Education |

Accélérateur de la transformation numérique

# Architecture Blockchain

**Formation certifiante en partenariat avec Télécom Paris Executive Education**

| | |
|---|---|
| **Modalité et lieu de la formation** | En présence dans les locaux de Télécom Paris Executive Education (Paris, 15e) |
| **Type de formation SystemX Academy** | Advanced@SystemX |
| **Catégorisation dans les domaines S&T de l'IRT SystemX** | Sécurité numérique et Blockchain |
| **Public** | Développeurs et des architectes souhaitant acquérir les connaissances suffisantes pour pouvoir évaluer l'opportunité de l'utilisation de cette technologie pour développer des applications se basant sur la blockchain |
| **Durée (en jour)** | 5 jours |
| **Descriptif du partenaire académique associé à la formation** | Formation continue de Télécom Paris Executive Education : L'organisme de formation continue de Télécom Paris |
| **Date des sessions** | Nous contacter pour les sessions à venir |
| **Objectifs de la formation** | • Comprendre les enjeux industriels et économiques de la Blockchain<br>• Comprendre les fondements de cette technologie<br>• Mesurer les apports et les limites de la Blockchain par rapport à un cas d'usage |
| **Points forts de la formation** | La formation présente les différents aspects de cette technologie, depuis les bases et leurs applications aux chaînes publiques (Bitcoin par exemple) jusqu'aux fonctionnalités avancées comme les contrats intelligents (Smart Contracts) et les chaînes privées à contrôle d'accès, sans oublier ses limitations intrinsèques. |
| **Programme** | **ENJEUX ECONOMIQUES DES BLOCKCHAINS**<br>• Analyse des éléments disruptifs<br>• Propriétés économiques des blockchains<br>• Blockchain et économie de la sécurité<br>• Smart contracts, forks et oracles |

| | |
|---|---|
| | **ASPECTS JURIDIQUES DE LA BLOCKCHAIN**<br>• Statut législatif des cryptomonnaies et tokens<br>• Réglementation sur les Initial Coin Offering (ICO)<br>• Régime juridique du smart contract<br>• Initiatives de régulation en cours au niveau français<br>• GDPR, droit à l'oubli et blockchain<br>• Blockchain comme register<br>**FONDEMENTS DE LA BLOCKCHAIN**<br>• Les blockchains ouvertes<br>• Le fonctionnement des blockchains, Bitcoin<br>• Notions d'économie, les risques des cryptomonnaies<br>• Blockchains privées, smart contracts, démonstrations<br>• Utilité de la blockchain dans un contexte économique<br>**TOUR D'HORIZON DES TECHNOLOGIES BLOCKCHAIN**<br>• Algorithmes de consensus<br>• Fonctionnement des smart contracts<br>• Propriétés de sécurité et limites…<br>**TRAVAUX PRATIQUES : MISE EN ŒUVRE D'UN RESEAU BLOCKCHAIN**<br>• Déploiement et configuration d'un réseau Blockchain<br>• Administration d'un nœud Blockchain (monitoring, permissions, …)<br>**PANORAMA DES CAS D'USAGES INDUSTRIELS DE LA BLOCKCHAIN**<br>• Energie : Autoconsommation collective d'énergie renouvelable<br>• Véhicule : Passeport du véhicule connecté<br>• Paiement : Application de payement basé sur les cryptomonnaies<br>**TRAVAUX PRATIQUES : REALISATION D'UNE APPLICATION A BASE DE SMART CONTRACT**<br>• Illustration des mécanismes Blockchain au travers d'une étude de cas (Ethereum)<br>• Développement de Smart Contract (Solidity)<br>**TOUR D'HORIZON DES TECHNOLOGIES BLOCKCHAINS: FOCUS HYPERLEDGER**<br>• Panorama de l'écosystème Hyperledger<br>• Plateforme Hyperledger Fabric<br>• Mise en pratique avec Hyperledger Composer<br>**TRAVAUX PRATIQUES : MISE EN ŒUVRE D'UN CAS D'USAGE**<br>• Développement d'une Dapp sur la base d'un cas d'usage de place de marché<br>• Déploiement et test de l'application décentralisée<br>**TRAVAUX PRATIQUES : APPROFONDISSEMENTS**<br>• Cycle de vie de l'application décentralisée<br>• Architectures orientées évènements<br>• Sensibilisation aux enjeux de sécurité |
| **Prérequis** | Notions de bases en sécurité informatique sont souhaitables pour tirer un meilleur profit de cette formation La connaissance d'un langage de programmation (Javascript, Python, etc.) est indispensable pour la partie pratique. |
| **Certificat** | Certificat délivré par Télécom Paris Executive Education |

Accélérateur de la transformation numérique

# Cybersécurité des systèmes de contrôle industriels

**Formation certifiante en partenariat avec Télécom Paris Executive Education**

| | |
|---|---|
| **Modalité et lieu de la formation** | En présence dans les locaux de Télécom Paris Executive Education (Paris, 15e) |
| **Type de formation SystemX Academy** | Advanced@SystemX |
| **Catégorisation dans les domaines S&T de l'IRT SystemX** | Sécurité numérique et Blockchain |
| **Public** | Responsables de sécurité, automaticiens, architectes et administrateurs réseaux et systèmes ICS/SCADA, auditeurs |
| **Durée (en jour)** | 3 jours |
| **Descriptif du partenaire académique associé à la formation** | Formation continue de Télécom Paris Executive Education : L'organisme de formation continue de Télécom Paris |
| **Date des sessions** | Nous contacter pour les sessions à venir |
| **Objectifs de la formation** | • Sensibilisation des acteurs du monde industriel aux menaces qui pèsent sur les installations industrielles<br>• Illustration des menaces avec des exercices de type « Ethical Hacking » sur des systèmes cyber-physiques<br>• Analyse de la menace et définition de la politique de sécurité<br>• Prise en main des solutions de sécurité (firewall, contrôle d'accès, détection d'intrusion, etc).<br>• Mise en œuvre d'une stratégie de maintien en condition de sécurité et maintien en condition opérationnelle (MàJ, gestion des correctifs, CTI, OSINT, etc) |
| **Points forts de la formation** | La formation permet d'analyser le paysage de la menace qui pèse sur les systèmes industriels et illustre les menaces avec des cas concrets.<br>Par ailleurs, elle passe en revue les standards de sécurité et les solutions de protections associées. |

| | |
|---|---|
| **Programme** | **UN SYSTEME DE CONTROLE INDUSTRIEL (ICS, INDUSTRIAL CONTROL SYSTEM)**<br>• Les technologies (les Automates Programmables Industriels, …)<br>• Composants d'un système industriel (PLC, capteurs, actionneurs, etc.),<br>• Protocoles industriels (Modbus, DNP3, OPC UA, TSN, etc)<br>• Architectures et applications associées (SCADA, EMS, Historian, CIM, etc)<br>**TRAVAUX PRATIQUES**<br>• Déploiement d'une infrastructure industrielle (Swtich, Automate programmable, IHM et application de supervision)<br>**PANORAMA D'ATTAQUES VISANT LES INSTALLATIONS INDUSTRIELLES**<br>• Illustrerons avec des cas concrets et des démonstrations<br>**TRAVAUX PRATIQUES**<br>• Mise en pratique des techniques d'audit et de reconnaissance pour la découverte de vulnérabilités,<br>• Lancement d'attaques de type « rejeu », «Man in the Middle », « DoD » , « Scan », …<br>**LES MESURES DE PROTECTION VISANT A RENFORCER LA SECURITE DES SYSTEMES**<br>• Déploiement et la mise en œuvre de solutions de protection<br>• Normes et standards de sécurité,<br>• Mise en œuvre d'une défense en profondeur,<br>• Déploiement et configuration de firewall industriels,<br>• Installation de sondes de détection, etc.<br>**POLITIQUE DE MAINTIEN DE SECURITE**<br>• Mise en œuvre d'une politique de maintiens en condition de sécurité (MCS) et maintiens en condition opérationnels (MCO).<br>• Gestion des correctifs, CTI, OSINT<br>• Présentation de la Cyber Threat Intelligence et son application à la sécurité des systèmes industriels.<br>• Intérêt du renseignement sur source ouvertes (OSINT) pour le maintien en condition de sécurité<br>**TRAVAUX PRATIQUES**<br>• Déploiement et configuration de solutions de sécurité : firewall, Control d'accès, IDS/IPS,<br>• Mise en place d'infrastructure de cyber threat intelligence pour le maintien en condition de sécurité |
| **Prérequis** | Des connaissances générales permettent de tirer un meilleur profit de la formation |
| **Certificat** | Certificat de présence délivré par Télécom Paris Executive Education |

Accélérateur de la transformation numérique

# Windows et ses mécanismes de protection

**Formation certifiante en partenariat avec Télécom Paris Executive Education**

| | |
|---|---|
| **Modalité et lieu de la formation** | En présence dans les locaux de Télécom Paris Executive Education (Paris, 15e) |
| **Type de formation SystemX Academy** | Advanced@SystemX |
| **Catégorisation dans les domaines S&T de l'IRT SystemX** | Sécurité numérique et Blockchain |
| **Public** | Administrateurs systèmes, ingénieurs, responsables sécurité du SI, chefs de projets informatiques |
| **Durée (en jour)** | 3 jours |
| **Descriptif du partenaire académique associé à la formation** | Formation continue de Télécom Paris Executive Education : L'organisme de formation continue de Télécom Paris |
| **Date des sessions** | Nous contacter pour les sessions à venir |
| **Objectifs de la formation** | • Expliquer le fonctionnement du système d'exploitation Microsoft Windows et ses mécanismes de sécurité internes<br>• Passer en revue les principales vulnérabilités de Windows et les risques liés aux mauvaises configurations du système<br>• Illustrer les menaces et les vulnérabilités au travers d'exercices pratiques de type « Ethical Hacking » sur des infrastructures réalistes et représentatives<br>• Présenter les bonnes pratiques et les corrections à appliquer pour assurer à son système un niveau de protection efficace<br>• Prise en main des solutions de sécurité internes (authentification, contrôle d'accès, politique de sécurité, etc.) et externes (firewall, détection d'intrusion, etc.) |
| **Points forts de la formation** | Dans la formation, nous analyserons la menace qui pèse sur ces systèmes et explorerons ses différentes vulnérabilités. Des travaux pratiques seront proposés pour une meilleure prise en compte du niveau de la menace ainsi que du degré de l'exposition. Nous passerons en revue également les standards de sécurité et les solutions de protections associés. |

| | |
|---|---|
| **Programme** | **DECOUVERTE DE L'ARCHITECTURE WINDOWS**<br>• Introduction générale aux systèmes d'exploitation<br>• Présentation de l'architecture Windows<br>• Description du noyau et des zones mémoire<br>• Explication du processus de démarrage et des appels système<br>• Processus de mise à jour sous Windows et gestion des failles<br>• Gestion des applications tierce et les apps du Store Microsoft<br>**TRAVAUX PRATIQUES**<br>• Déploiement du système d'information d'une petite/moyenne entreprise<br>• Mise en œuvre des concepts d'architecture vus dans la partie théorique<br>• Mise en évidence des vulnérabilités sous Windows (Compromission de l'active directory, mouvement latéral, élévation de privilèges, etc.)<br>• Présentation des techniques, tactiques et procédures et des règles de bonnes pratiques<br>**AUDIT DE SECURITE ET IDENTIFICATION DES DEFAUTS DE CONFIGURATION**<br>• Description et mise en place de stratégie d'audit<br>• Outils de journalisation des évènements natifs sous Windows<br>• Classification des évènements et identification des évènements importants<br>• Principe de transfert d'évènements<br>**TRAVAUX PRATIQUES**<br>• Déploiement et/ou configuration des outils de journalisation Windows<br>• Test d'audit de sécurité et analyse des risques sous Windows<br>• Administration sécurisée et guide des bonnes pratiques<br>**LES MESURES DE PROTECTION VISANT A RENFORCER LA SECURITE DES SYSTEMES**<br>• Présentation des solutions de sécurité : authentification, gestion des mots de passe, gestion des droits, firewall, contrôle d'accès, IDS/IPS<br>• Mise en œuvre d'une politique de maintien en condition de sécurité (MCS)<br>• Présentation de la Cyber Threat Intelligence et son application à la sécurité des systèmes d'exploitation Windows<br>• Intérêt du renseignement sur sources ouvertes (OSINT) pour le maintien en condition de sécurité<br>**TRAVAUX PRATIQUES**<br>• Déploiement et configuration de solutions de sécurité : authentification, gestion des mots de passe, gestion des droits, firewall, Control d'accès, IDS/IPS<br>• Durcissement de services LDAP, DNS, IIS, Bureau à distance, SMB, SQL, etc<br>• Mise en place d'infrastructure de Cyber Threat Intelligence pour le maintien en condition de sécurité |
| **Prérequis** | Être familiarisé avec les systèmes d'exploitation de Windows |
| **Certificat** | Certificat de présence délivré par Télécom Paris Executive Education |

# Sécurité Web : développer et héberger de manière sûre

**Formation en partenariat avec Télécom Paris Executive Education**

| | |
|---|---|
| **Modalité et lieu de la formation** | En présence dans les locaux de Télécom Paris Executive Education (Paris, 15e) |
| **Type de formation SystemX Academy** | Advanced@SystemX |
| **Catégorisation dans les domaines S&T de l'IRT SystemX** | Sécurité numérique et Blockchain |
| **Public** | Architectes de technologies Web, développeurs Web, chef de projet Web, responsable sécurité (RSSI) |
| **Durée (en jour)** | 2 jours |
| **Descriptif du partenaire académique associé à la formation** | Formation continue de Télécom Paris Executive Education : L'organisme de formation continue de Télécom Paris |
| **Date des sessions** | Nous contacter pour les sessions à venir |
| **Objectifs de la formation** | Expliquer les problématiques de sécurité, du développement à l'hébergement d'applications Web |
| **Points forts de la formation** | La formation présente le contexte actuel auquel les entreprises font face et les enjeux afférents. Puis, la « sécurité des infrastructures d'hébergement » montre les enjeux en tant qu'hébergeur, les problématiques et les solutions possibles. Ensuite, la « sécurité du développement des applications Web » passe en revue l'ensemble des classes de vulnérabilité Web, tout en décrivant l'implémentation des mesures de protection corrigeant les vulnérabilités exposées.<br>Cette formation repose en grande partie sur des travaux pratiques qui seront effectués sur la plateforme CyberRange. |
| **Programme** | **INTRODUCTION A LA SECURITE DES APPLICATIONS WEB**<br>• Protocole HTTP, technologies web, architecture d'une application web<br>• Tendances des attaques web |

- Authentification, autorisation, vulnérabilités et moyens de protection

**VULNERABILITES DES APPLICATIONS WEB (OWASP)**

- Vulnérabilités du SSL
- Vol de session
- API et librairies non sécurisées
- Scanning et reconnaissance
- Outils d'analyse Proxy (Burp Suite, ZAProxy)
- Sniffing, spoofing, brute forcing, clickjacking, XSS, CSRF
- Attaque par injection SQL/NoSQL/Shell/LDAP/XML/autres, …
- DNS rebinding

**VULNERABILITES DES SERVICES WEB**

- XML : Attaques et contre-mesures
- AJAX : tendances des attaques, codes malveillants et moyens de protection
- JavaScripts : codes malveillants, rétro-ingénierie, …
- Flash, Java applet : vulnérabilités et moyens de protection

**BONNES PRATIQUES DE SECURITE WEB**

- Sécurisation du code, environnement, navigateur
- Implémentation des aspects sécurité dans un cycle de vie logiciel : description de l'ensemble des mesures à mettre en œuvre dans un cycle de vie logiciel et/ou cycle projet (analyse de risques, formations, règles de développement sécurisé, audits automatisés, audits manuels, bug bounties, ...)
- Protection des services hébergés contre les attaques applicatives
  - Stratégie de protection applicative au niveau de l'infrastructure
  - Mise en œuvre de filtrage applicatif : principes de fonctionnement, règles, déploiement
- Supervision de sécurité des services/infrastructures et gestion d'incident (SIEM)
  - Stratégie de supervision de sécurité
  - Mise en œuvre de la stratégie de supervision de sécurité : remontées en supervision, contre-mesures, traitement des incidents, …

**TRAVAUX PRATIQUES**

- Ethical Hacking sur la plateforme CyberRange : XSS, CSRF, SQL Injection, Shellshock, LFI, RFI et XXE
- Détection et correction des vulnérabilités
- Une mise en situation sera réalisée à la fin de la formation

**SYNTHESE ET CONCLUSION**

| | |
|---|---|
| **Prérequis** | Des connaissances dans le domaine des technologies Web permettent de tirer le meilleur profit de cette formation |