Année CSIU 3

Semestre 5

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Cloud & Supervision

Cloud & Supervision

Données Générales			
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**		Responsable(s) Module SANGARE Mamoudou
Type de module : Unité d'Enseignement	**Cloud & Supervision** (LIBCys05UCloudSup)		
Crédits (ECTS)	5		
Effectif maximum	160		
Durée totale : 50h00	Periode Semestre 5	Langue d'enseignement :	

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Cloud & Supervision
- Déploiement de Sondes de Supervision

Déploiement de Sondes de Supervision

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Déploiement de Sondes de Supervision** (LIBCys05EDeplSondSup)			
TP : 20h00 Durée totale: 42h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre les principes de supervision des réseaux industriels.
Déployer des sondes de supervision passives (IDS) ou actives (probes) dans un environnement IT/OT.
Configurer des outils de collecte, de journalisation et d'analyse de trafic réseau
Intégrer les sondes dans une infrastructure SOC ou SIEM.
Analyser les événements collectés pour détecter des anomalies ou menaces

Contenu

Introduction à la supervision en environnement industriel
•
Types de sondes (passives vs actives)
Positionnement stratégique dans les réseaux IT-OT
•Architecture de collecte et d'agrégation des données (Syslog, NetFlow, SPAN, TAPs)
Intégration avec les outils SIEM

Prérequis

UE12_5 et UE12_6

Bibliographie

Zeek Documentation – https://docs.zeek.org
•
Suricata IDS – https://suricata.io
Wireshark User Guide – https://www.wireshark.org/docs/
Elastic Stack – https://www.elastic.co/what-is/elk-stack
SANS ICS resources – https://www.sans.org/industrial-control-systems/

Évaluation(s)			
N°	**Nature**	**Coefficient**	**Objectifs**
1		Rapports de TP, évaluation pratique Projet final (mini-PoC)	TP

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Cloud & Supervision
- Introduction Cloud

Introduction Cloud

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Introduction Cloud** (LIBCys05EIntCloud)			
TP : 10h00 Cours : 10h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre les principes fondamentaux du cloud computing.
-
Identifier les modèles de déploiement (public, privé, hybride) et de services (IaaS, PaaS, SaaS).
Évaluer les enjeux de sécurité dans un environnement cloud.
Appréhender les spécificités du cloud dans les environnements industriels (IT/OT).
Utiliser un

Contenu

Introduction générale au Cloud
•
Historique et évolution du Cloud Computing
•
Concepts clés : virtualisation, mutualisation, élasticité
Avantages et inconvénients du Cloud
Modèles de services Cloud
IaaS, PaaS, SaaS : définitions, cas d’usage
Comparaison entre les modèles
•
Acteurs majeurs : AWS, Azure, GCP, OVH, etc.
Modèles de déploiement
•
Cloud public, privé, hybride, communautaire
•
Cloud industriel (Edge, Fog computing, Cloud OT)
•
Exemples d’intégration dans l’industrie 4.0
Enjeux de sécurité dans le Cloud
•
Risques spécifiques : perte de contrôle, dépendance, confidentialité
•
Normes et standards (ISO/IEC 27017, CSA)
•
Méthodes d’authentification, chiffrement, gestion des accès
Introduction à la conformité et à la résilience
Conformité réglementaire (RGPD, ISO, NIS2)
Continuité d’activité et reprise après incident
Cloud Security Alliance & bonnes pratiques

Prérequis

UE12_5 et UE12_6

Bibliographie

Cloud Security Alliance – Security Guidance for Critical Areas of Focus in Cloud Computing
ENISA – Cloud Computing Risk Assessment
Documentation AWS/Azure/Google Cloud
ISO/IEC 27017:2015

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Évaluation pratique	TP

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Cloud & Supervision
- Projet Recherche: Exposition

Projet Recherche: Exposition

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Projet Recherche: Exposition** (LIBCys05EProjRecExp)			
Cours : 10h00 Durée totale: 10h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Connaissance de base en méthodologie de recherche
Présentation d'un projet de recherche

Contenu

Recherche bibliographique
Exploitation d'articles scientifiques

Prérequis

N/A

Bibliographie

Bibliographie :
-
How to Write and Present a Research Paper - Paul Oliver.
-
Designing Visual Representations - Colin Ware.
-
Turabian, K. L., A Manual for Writers of Research Papers, Theses, and Dissertations.
-
Booth, W. C., Colomb, G. G., Williams, J. M., The Craft of Research.
-
Ec.europa.eu - How to communicate your research effectively.
-
IEEE Author Center : How to prepare your conference paper and poster.
-
OWL Purdue Online Writing Lab: Research Writing Resources.
Webographie :
Tutoriels sur les outils numériques de présentation : Canva, Prezi.
Ressources académiques en ligne : Springer, Elsevier.

Bibliographie
Blogs et articles sur la méthodologie de recherche et la communication visuelle.

Évaluation(s)			
N°	**Nature**	**Coefficient**	**Objectifs**
1		Évaluation sommative	Projet

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Cybersécurité

Cybersécurité

Données Générales			
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**		Responsable(s) Module SANGARE Mamoudou
Type de module : Unité d'Enseignement	**Cybersécurité** (LIBCys05UCyber)		
Crédits (ECTS)	3		
Effectif maximum	160		
Durée totale : 40h00	Periode Semestre 5	Langue d'enseignement :	

Introduction Aux Directives et Réglementations en Cybersécurité

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : SANGARE Mamoudou
Type d'EC : Cours	**Introduction Aux Directives et Réglementations en Cybersécurité** (LIBCys05EIntroDirRegCyb)			
Cours : 20h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement : Français	

Acquis d'apprentissage

Comprendre les grands principes juridiques et réglementaires encadrant la cybersécurité.

Identifier les principales normes, directives et lois applicables à la cybersécurité au niveau national, européen et international.

Appréhender les enjeux de conformité pour les entreprises industrielles.

Savoir intégrer les exigences réglementaires dans une politique de cybersécurité.

Contenu

Introduction au droit du numérique et à la cybersécurité

Les textes fondamentaux (RGPD, NIS 2, Cyber Resilience Act, etc.)

Normes et standards (ISO/IEC 27001, IEC 62443)

Obligations des opérateurs de services essentiels et entités critiques

Impacts réglementaires sur les systèmes industriels (OT/ICS)

Sanctions et responsabilités en cas de non-conformité

Cas pratiques d’analyse de conformité

Prérequis

Aucun prérequis obligatoire, mais des notions de base en cybersécurité ou droit du numérique sont un plus.

Bibliographie

ENISA – Publications on NIS 2 and cybersecurity in critical infrastructure

ANSSI – Guides and white papers on regulatory frameworks

ISO/IEC 27001:2022 – International Standard for Information Security Management

IEC 62443 – Cybersecurity for Industrial Automation

CNIL – Documentation on GDPR compliance

Directive (EU) 2022/2555 – NIS 2 Directive

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Cybersécurité
- Organisation de La Cybersécurité

Organisation de La Cybersécurité

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : SANGARE Mamoudou
Type d'EC : Cours	**Organisation de La Cybersécurité** (LIBCys05EOrgaCyb)			
Cours : 20h00 Durée totale: 68h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Le module couvre les éléments suivants :
-
Les métiers de la cybersécurité et les compétences associées ;
Les modèles d'organisation RSSI et les compétences en cybersécurité nécessaires à une organisation
La maturité des organisations et les modèle d'évaluation de maturité en cybersécurité ;
Les étapes d'un audit organisationnel en cybersécurité
Quelles sont les étapes d'un audit organisationnel en cybersécurité ;
Quels sont les livrables attendus à la suite d'un audit organisationnel en cybersécurité

Contenu

Quelles sont les étapes d'un audit organisationnel en cybersécurité ;
Quels sont les livrables attendus à la suite d'un audit organisationnel en cybersécurité ;

Prérequis

Introduction aux Politiques de Sécurité

Bibliographie

Bibliographie :
-
Cybersecurity Leadership: Powering the Modern CISO - Mansur Hasib.
-
Managing Risk and Information Security: Protect to Enable - Malcolm Harkins.
-
The Cybersecurity Framework - NIST Guidelines.
-
"Managing Information Security Risk" - Donald Pipkin.
-
"Governance of Enterprise IT based on COBIT 5" - ISACA.
Webographie :

Bibliographie

ISO 27001 : www.iso.org.
Ressources du NIST : www.nist.gov.
Articles et cours en ligne : Cybrary, SANS Institute.

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Gestion Des Suivis

Gestion Des Suivis

Données Générales			
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**		Responsable(s) Module SANGARE Mamoudou
Type de module : Unité d'Enseignement	**Gestion Des Suivis** (LIBCys05UGestSui)		
Crédits (ECTS)	5		
Effectif maximum	160		
Durée totale : 50h00	Periode Semestre 5	Langue d'enseignement :	

Gestion de La Production et de La Supply Chain

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Gestion de La Production et de La Supply Chain** (LIBCys05EGestProd)			
TD : 10h00 Cours : 10h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre les principes fondamentaux de la gestion de production et de la supply chain.
-
Savoir planifier, organiser et optimiser les opérations de production et de logistique.
Appréhender les enjeux stratégiques liés à la chaîne d'approvisionnement.
Développer une capacité d'analyse critique face aux défis actuels (digitalisation, durabilité, résilience des chaînes).

Contenu

Introduction à la production industrielle
-
Principes et stratégies de gestion de la production
-
Introduction à la supply chain management (SCM)
-
Planification des ressources de production (MRP, ERP)
-
Gestion des stocks et des approvisionnements
-
Logistique, transport et distribution
Pilotage des flux et lean management
Technologies et digitalisation de la supply chain
Défis contemporains : développement durable et supply chain résiliente

Prérequis

Connaissances de base en management et en économie
Familiarité avec les outils mathématiques et statistiques (ex. : optimisation linéaire, probabilités).
Sensibilisation aux fondamentaux des systèmes d'information (UE24_3-3).

Bibliographie

Bibliographie principale :
-
Ballou, R.H. Business Logistics/Supply Chain Management, Pearson.
-
Chopra, S., Meindl, P. Supply Chain Management: Strategy, Planning, and Operation, Pearson.
-
Slack, N., Brandon-Jones, A. Operations Management, Pearson Education.
-
Webographie :
APICS (Association for Supply Chain Management) : https://www.apics.org/
Supply Chain Management Review : https://www.scmr.com/
Logistique Magazine : https://www.logistiques-magazine.com/

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Évaluation diagnostique, formative et sommative	Devoir écrit

PCA PRA

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**PCA PRA** (LIBCys05EPCAPRA)			
TD : 10h00 Cours : 10h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Le module couvre les éléments suivants :
-
Présentation des concepts clés du Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA) (ISO 22301, méthodologie interne);
-
Méthodes d'élaboration d'un PCA (Identification des processus critiques, sauvegardes, gestion des ressources);
-
Méthodologies de définition des RTO (Recovery Time Objective) et RPO (Recovery Point Objective) (adaptées au Client);
-
Méthodes d'élaboration d'un PRA pour restaurer les opérations après un incident majeur (adaptées au Client);
-
Dépendances entre le PCA, le PRA pour une gestion de crise Cyber efficace;
-
Les objectifs du Recovery Time Objective (RTO), Recovery Point Objective (RPO) et Service Level Agreement (SLA);
L'accompagnement des métiers afin de définir leur RTO et RPO;
L'engagement de SLA pour accompagner les métiers;

Contenu

Les enjeux du Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA) en lien avec les objectifs de l'entreprise et les services concernés.
Mettre en oeuvre et promouvoir un PCA et PRA selon un contexte d'organisation
Rédiger un PCA et PRA pour un scénario d'attaque généralisée sur les systèmes du Client.

Prérequis

Introduction aux Politiques de Sécurité
Principe de gestion de risque

Bibliographie

Bibliographie :

Bibliographie

-
Business Continuity Management - Andrew Hiles.
-
The Disaster Recovery Handbook - Michael Wallace & Lawrence Webber.
-
Resilience Engineering in Practice - Erik Hollnagel.
-
SO 22301: Security and resilience – Business continuity management systems.
-
ITIL Service Continuity Management.
-
NFPA 1600: Standard on Continuity, Emergency, and Crisis Management.
-
Guillaume Desgens-Pasanau, Le Plan de Continuité d'Activité, Dunod, 2016.
-
CERT-FR – Guides de bonnes pratiques de continuité et reprise d'activité.
-
ANSSI – Guide pour l'élaboration d'un PCA dans les infrastructures critiques.
Webographie :
Sites officiels et rapports : ISO 22301 (Gestion de la continuité), NIST.
Plateformes en ligne : Blogs spécialisés en gestion de crise et continuité d'activité.

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Gestion Des Suivis
- Centre D'Opérations de Sécurité (SOC)

Centre D'Opérations de Sécurité (SOC)

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Centre D'Opérations de Sécurité (SOC)** (LIBCys05ESOC)			
Cours : 10h00 Durée totale: 10h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre le rôle et le fonctionnement d'un Security Operation Center (SOC).
Maîtriser l'analyse d'événements de sécurité.
Être capable de détecter, analyser et répondre aux incidents de cybersécurité.
Développer des compétences pour concevoir et améliorer les processus d'un SOC.

Contenu

Introduction aux SOC : missions, organisation, et architecture.
-
Détection des incidents : SIEM, IDS/IPS et outils de monitoring.
-
Analyse des alertes et triage.
-
Gestion des incidents de sécurité : procédures et escalade.
Investigation numérique : logs, forensic léger.
Reporting, communication et amélioration continue en SOC.
Exercices pratiques sur des environnements simulés.

Prérequis

Connaissances de base en cybersécurité (UE23_4-2, UE23_3-3).
Familiarité avec les concepts de gestion des incidents de sécurité (UE23_5).
Sensibilisation aux infrastructures réseau et systèmes d'exploitation (UE12_5).

Bibliographie

Livres :
-
"The Practice of Network Security Monitoring" – Richard Bejtlich.
-
"Incident Response & Computer Forensics" – Jason Luttgens, Matthew Pepe, Kevin Mandia.
-

Bibliographie

"Blue Team Handbook: Incident Response Edition" – Don Murdoch.
-
The SOC Book: Building, Operating and Maintaining Your Security Operations Center - Faisal Yousef.
-
Cybersecurity and Threat Intelligence Handbook - Alan White.
-
Incident Response & Computer Forensics - Kevin Mandia et al.
-
Webographie :
-
Ressources en ligne sur les outils SIEM et EDR (Splunk, Palo Alto, etc.).
-
Rapports et guides du NIST sur la gestion des incidents.
-
Plateformes éducatives : Cybrary, SANS Institute.
-
MITRE ATT&CK Framework : https://attack.mitre.org/
NIST Computer Security Incident Handling Guide : https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
OWASP Incident Response Project : https://owasp.org/www-project-incident-response

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Contrôle continu : étude de cas Travaux pratiques : exercices d'investigation Mini Projet final : simulation d'incident et production d'un rapport d'incident	Contrôle continu

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Investigation

Investigation

Données Générales			
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**		Responsable(s) Module SANGARE Mamoudou
Type de module : Unité d'Enseignement	**Investigation** (LIBCys05UInvest)		
Crédits (ECTS)	5		
Effectif maximum	160		
Durée totale : 50h00	Periode Semestre 5	Langue d'enseignement :	

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Investigation
- Gestion Des Identités

Gestion Des Identités

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Gestion Des Identités** (LIBCys05EGestIden)			
Cours : 20h00 Durée totale: 56h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre les principes fondamentaux de la gestion des identités et des accès (IAM).
-
Apprendre à déployer des solutions de gestion des identités sécurisées et adaptées aux besoins organisationnels.
Identifier et résoudre les problèmes courants liés aux processus d'authentification et de gestion des accès.
Être capable de concevoir des stratégies d'identification et d'accès conformes aux normes de sécurité

Contenu

Introduction à la gestion des identités :
-
Définitions et concepts clés : identité numérique, gestion des accès.
-
Importance stratégique et enjeux organisationnels.
Processus d'authentification et d'autorisation :
-
Méthodes classiques : mots de passe, PIN.
-
Techniques avancées : authentification multifactorielle, biométrie.
-
Gestion des rôles et droits d'accès (RBAC, ABAC).
Technologies et outils IAM :
-
Introduction aux solutions logicielles (Active Directory, Okta, etc.).
-
Sécurisation des API et accès aux données.
Normes et réglementations :
-
Conformité aux standards internationaux (ISO 27001, GDPR).
-
Études des cadres juridiques liés aux identités numériques.
Études de cas pratiques :
Analyse d'architectures IAM existantes.
Résolution de problématiques réelles d'accès et d'identification.

Prérequis

Connaissances de base en cybersécurité (authentification, cryptographie).
Familiarité avec les concepts liés aux systèmes d'information et aux bases de données.
Sensibilisation aux enjeux de gestion des accès et des identités numériques.

Bibliographie

Bibliographie :
-
Identity and Access Management for Dummies - Wiley.
-
Access Control and Identity Management - Mike Chapple.
-
Mastering Identity and Access Management - Jonathan Alexander.
Webographie :
Ressources sur les outils IAM : Microsoft Azure AD, Okta.
Guides ISO pour la gestion des identités : www.

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Évaluation diagnostique, formative et sommative	Devoir écrit

Introduction Forensics

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Introduction Forensics** (LIBCys05EIntFor)			
Cours : 10h00 Durée totale: 10h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre les principes de la criminalistique numérique (Forensics).
Identifier et analyser les preuves numériques tout en respectant les exigences légales et éthiques.
Apprendre les méthodes de collecte, de préservation et de traitement des preuves numériques.
Développer une capacité à utiliser les outils et techniques liés aux enquêtes numériques.

Contenu

Introduction à la criminalistique numérique :
-
Définitions, objectifs et importance dans les enquêtes informatiques.
-
Évolutions historiques et cadre juridique.
Types de preuves numériques :
-
Différenciation entre les données volatiles et non volatiles.
-
Analyse des fichiers, logs, réseaux et périphériques.
Méthodes de collecte et de préservation des preuves :
-
Techniques de capture des données sans altération.
-
Sécurisation des éléments de preuve : chaînage de conservation.
Analyse des preuves numériques :
-
Utilisation d'outils spécialisés (ex. : FTK, EnCase).
-
Investigation sur les malwares, les activités réseau et les systèmes compromis.
Rédaction de rapports d'investigation :
Structuration et contenu.
Préparation à la présentation des résultats devant des juridictions.

Prérequis

Connaissances fondamentales en systèmes informatiques et réseaux.
Notions de base en cybersécurité (ex. : protection des données, gestion des incidents).
Familiarité avec les concepts juridiques liés aux technologies numériques (ex. : droit numérique)

Bibliographie

Bibliographie :
-
Computer Forensics: Investigating Data and Image Files - Chris Davis.
-
Incident Response & Computer Forensics - Kevin Mandia et al.
-
Digital Evidence and Computer Crime - Eoghan Casey.
Webographie :
Ressources du NIST sur la criminalistique numérique : www.nist.gov.
Cours et articles sur Cybrary et SANS Institute.
Forums spécialisés en criminalistique numérique.

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Travaux pratiques : exercices d'acquisition et d'analyse de preuves numériques. Étude de cas : rédaction d'un rapport d'analyse forensic. Examen final : évaluation théorique sur les concepts abordés.	TP

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Investigation
- Introduction Aux Politiques de Sécurité

Introduction Aux Politiques de Sécurité

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Introduction Aux Politiques de Sécurité** (LIBCys05EIntPolSec)			
Cours : 20h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Le module couvre les éléments suivants :
La hiérarchisation des politiques, procédures et standards de sécurité;
Les enjeux du la création et déploiement d'une Politique de Sécurité du Système d'Information (PSSI)
Maîtriser les étapes pour concevoir, améliorer et utiliser une Politique de Sécurité des Systèmes d'Information (PSSI)
Créer une politique de sécurité adaptée à un contexte d'entreprise
Décliner un standard et une procédure d'une politique de sécurité

Contenu

Les concepts, approches, méthodes et techniques permettant l'appréciation et la documentation des contrôles à mettre en place pour assurer la sécurité et la conformité de la Politique de Sécurité des Systèmes d'Information (PSSI)
Le rôle et l'utilité d'une Politique de Sécurité du Système d'Information (PSSI)
Maîtriser les étapes pour concevoir, améliorer et utiliser une Politique de Sécurité des Systèmes d'Information (PSSI)
Créer une politique de sécurité adaptée à un contexte d'entreprise
Décliner un standard et une procédure d'une politique de sécurité

Prérequis

N/A

Bibliographie

Bibliographie :
-
Information Security Policies Made Easy - Charles Cresson Wood.
-
The Security Policies Handbook - E. Eugene Schultz.
-
ISO/IEC 27001: Guide pratique.
-
"Information Security Policies, Procedures, and Standards" – Thomas R. Peltier.
-

Bibliographie

"Managing Information Security" – John R. Vacca.
Webographie :
Site officiel de l'ISO 27001 : www.iso.org.
Guides sur la cybersécurité et les politiques de sécurité du NIST : www.nist.gov.
Articles et ressources en ligne : Cybrary, SANS Institute.

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Outils de Communication 5

Outils de Communication 5

Données Générales			
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**		Responsable(s) Module BUSSELL Frances
Type de module : Unité d'Enseignement	**Outils de Communication 5** (LIBCys05UOutComm)		
Crédits (ECTS)	6		
Effectif maximum	30		
Durée totale : 80h00	Periode Semestre 5	Langue d'enseignement :	

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Outils de Communication 5
- Anglais

Anglais

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Anglais** (LIBCys05EAng)			
TD : 20h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Perfectionner le champ lexical scientifique et technologique.
Développer un esprit critique et une connaissance des réalités sociales et culturelles.
Développer une analyse critique et argumenter
Avoir une approche culturelle des mondes professionnels de pays donnés

Contenu

Plusieurs champs linguistiques : la langue générale, la langue professionnelle, la langue scientifique et technologique et l'interculturalité.
Développement sur les quatre premiers semestres des axes suivants :
- communication orale
- communication écrite
- compréhension orale
- compréhension écrite
- interaction

Méthodes et/ou moyens pédagogiques
Écoute d'extraits

Prérequis

Modules d'anglais précédents

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Évaluation diagnostique, formative et sommative par mise en situation. Auto-	Devoir écrit

Évaluation(s)			
		évaluation de l'évolution des compétences en cours d'acquisition.	

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Outils de Communication 5
- Budget et Calcul Des Coûts

Budget et Calcul Des Coûts

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Budget et Calcul Des Coûts** (LIBCys05EBudCalCou)			
TD : 10h00 Projet : 10h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement : Français	

Acquis d'apprentissage

- Comprendre les principes fondamentaux de la comptabilité de gestion.
- Maîtriser les différentes méthodes de calcul des coûts.
- Élaborer et analyser un budget prévisionnel.
- Utiliser les outils de gestion budgétaire pour la prise de décision.

Contenu

Le but de ce cours est de fournir aux étudiants les compétences nécessaires pour comprendre, analyser et piloter la performance financière d'une organisation à travers deux axes complémentaires : comprendre les coûts pour mieux gérer et maîtriser la logique budgétaire.

Prérequis

Aucun

Bibliographie

Comptabilité de gestion
Horngren, C. T., Datar, S. M., & Rajan, M. V.

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		- Comprendre les principes fondamentaux	Contrôle continu

Évaluation(s)			
		de la comptabilité de gestion. - Maîtriser les différentes méthodes de calcul des coûts. - Élaborer et analyser un budget prévisionnel. - Utiliser les outils de gestion budgétaire pour la prise de décision.	
2		- Comprendre les principes fondamentaux de la comptabilité de gestion. - Maîtriser les différentes méthodes de calcul des coûts. - Élaborer et analyser un budget prévisionnel. - Utiliser les outils de gestion budgétaire pour la prise de décision.	Contrôle continu

Introduction à La Finance D'Entreprise

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Introduction à La Finance D'Entreprise** (LIBCys05EIntFinEnt)			
TD : 10h00 Projet : 10h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

- Comprendre les principes de base (bilan, compte de résultat) dans la comptabilité
- Connaître les principales notions et outils d'analyse financière (fonds de roulement, besoin en fonds de roulement, capacité d'autofinancement, ratios financiers, tableau de financement),
- Intégrer le décalage de règlement ou d'encaissement dans le quotidien de l'entreprise,
- Comprendre les notions essentielles de rentabilité et d'équilibre financier.

Contenu

Le but de ce cours est d'introduire les élèves aux plusieurs concepts clés qui sont essentiels pour la gestion financière efficace d'une entreprise :
Dimension comptable et financière : Finalités ; Usages pour le non-financier
Comptabilité générale : Principes de base ; Bilan ; Compte de résultat
Analyse financière : Soldes intermédiaires de gestion ; Capacité d'autofinancement ;Ratios d'activité ; Structure financière(bilan fonctionnel) ; Rentabilité et risques ;Tableau de financement ;Trésorerie

Prérequis

Approche globale de l'entreprise

Bibliographie

Finance d'entreprise 6e édition

Jonathan Berk (Auteur), Peter DeMarzo (Auteur), Gunther Capelle-Blancard (Auteur), Nicolas Couderc (Auteur)

Évaluation(s)

N°	Nature	Coefficient	Objectifs

Évaluation(s)			
1	Contrôle continu	1	- Connaître les principales notions et outils d'analyse financière (fonds de roulement, besoin en fonds de roulement, capacité d'autofinancement, ratios financiers, tableau de financement), - Intégrer le décalage de règlement ou d'encaissement dans le quotidien de l'entreprise, - Comprendre les notions essentielles de rentabilité et d'équilibre financier.
2	Contrôle continu	1	- Connaître les principales notions et outils d'analyse financière (fonds de roulement, besoin en fonds de roulement, capacité d'autofinancement, ratios financiers, tableau de financement), - Intégrer le décalage de règlement ou d'encaissement dans le quotidien de l'entreprise, - Comprendre les notions essentielles de rentabilité et d'équilibre financier.

Techniques de Communication Pour La Gestion Des Risques IT-OT 3

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Techniques de Communication Pour La Gestion Des Risques IT-OT 3** (LIBCys05ETechComm)			
Cours : 10h00 Projet : 10h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Développer des compétences avancées en communication de crise dans un contexte IT-OT.
Savoir élaborer des stratégies de communication proactive et réactive adaptées aux risques cyber.
Savoir coordonner la communication interne et externe lors d'incidents cyber critiques.

Contenu

Techniques avancées de communication en gestion de crise.
-
Communication proactive : préparation et anticipation.
-
Communication réactive : réponse en situation d'incident.
Élaboration de plans de communication de crise pour l'IT-OT.
Simulation d'incidents : rédaction de communiqués, coordination des parties prenantes.
Analyse post-crise et retour d'expérience en communication.

Prérequis

Connaissances de base en communication d'entreprise et gestion des risques IT-OT.
Avoir suivi les modules « Techniques de communication pour la gestion des risques IT-OT 1 et 2 » est fortement recommandé.

Bibliographie

Bibliographie :
-
Heath, R.L., & O'Hair, H.D. Handbook of Risk and Crisis Communication.
-
Coombs, W.T. Ongoing Crisis Communication: Planning, Managing, and Responding.
-
ENISA. Good Practices for Crisis Communication.
-

Bibliographie

ISO 22361:2022 - Security and resilience — Crisis management — Guidelines for developing a strategic capability.
-
NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery.
Webographie :
ENISA - European Union Agency for Cybersecurity
NIST Cybersecurity Framework

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Évaluation continue à travers des exercices pratiques - Simulation d'une communication de crise - Dossier écrit individuel ou en binôme	Contrôle continu

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Sécurisation It/Ot

Sécurisation It/Ot

Données Générales			
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**		Responsable(s) Module SANGARE Mamoudou
Type de module : Unité d'Enseignement	**Sécurisation It/Ot** (LIBCys05USecurITOT)		
Crédits (ECTS)	6		
Effectif maximum	160		
Durée totale : 80h00	Periode Semestre 5	Langue d'enseignement :	

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Sécurisation It/Ot
- Sécurisation de La Convergence IT-OT

Sécurisation de La Convergence IT-OT

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic,YANGUERE Alfred Walter
Type d'EC : Cours	**Sécurisation de La Convergence IT-OT** (LIBCys05ESecConvITOT)			
TP : 20h00 Durée totale: 20h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre les enjeux et spécificités de la convergence entre les technologies de l'information (IT) et les technologies opérationnelles (OT).
-
Identifier les risques spécifiques liés à l'interconnexion des environnements IT et OT.
-
Appliquer des stratégies de sécurisation adaptées à la convergence IT/OT.
Apprendre à concevoir et mettre en oeuvre des stratégies de sécurisation adaptées à ces infrastructures hybrides.
Être capable d'assurer la résilience des systèmes critiques en cas de menaces ou attaques.

Contenu

Introduction à la convergence IT/OT :
-
Définition et importance de l'intégration IT/OT.
-
Bénéfices et challenges de la convergence dans les infrastructures critiques.
Vulnérabilités et menaces spécifiques :
-
Analyse des vecteurs d'attaques dans les environnements hybrides.
-
Étude des incidents passés dans des environnements industriels.
Techniques et méthodologies de sécurisation :
-
Mise en place de stratégies segmentées pour IT et OT.
-
Utilisation de solutions de détection d'anomalies (IDS/IPS) dans les réseaux industriels.
-
Gestion des mises à jour et des patchs dans les environnements critiques.
Normes et cadres réglementaires :
-
Introduction aux normes telles que NERC CIP, ISO 27019 et ISA/IEC 62443.
-
Obligation de conformité dans les secteurs critiques (énergie, transport, santé).
Études de cas et bonnes pratiques :
Scénarios réalistes de sécurisation de la convergence IT/OT.
Exemples concrets d'optimisation de la résilience dans les systèmes critiques

Prérequis

Connaissances fondamentales en réseaux informatiques et technologies opérationnelles (OT).
Familiarité avec les bases de la cybersécurité (gestion des risques, protection des données).
Notions de base sur les systèmes industriels (SCADA, IoT industriel, capteurs).

Bibliographie

Ouvrages :
-
Industrial Network Security – Eric D. Knapp & Joel Langill, Syngress.
-
Securing Industrial Control Systems – Joseph Weiss, Momentum Press.
-
Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems - Pascal Ackerman.
-
Cybersecurity for Industrial Control Systems - Tyson Macaulay.
-
Securing IT and OT Systems - John Sammons & Michael Cross.
Normes et standards :
-
ISA/IEC 62443 – Security for Industrial Automation and Control Systems.
-
NIST Special Publication 800-82 – Guide to Industrial Control Systems (ICS) Security.
Ressources web :
NIST Cybersecurity Framework : https://www.nist.gov/cyberframework
SANS Institute – ICS Security Resources : https://www.sans.org/ics

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Évaluation continue : exercices pratiques et études de cas Projet final de sécurisation d'une architecture IT/OT	Contrôle continu

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Sécurisation It/Ot
- Sécurité Embarquée

Sécurité Embarquée

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic,SANGARE Mamoudou
Type d'EC : Cours	**Sécurité Embarquée** (LIBCys05ESecEmb)			
TD : 10h00 TP : 10h00 Cours : 10h00 Durée totale: 30h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Comprendre les spécificités de la sécurité des systèmes embarqués, y compris leurs contraintes matérielles et logicielles.
-
Apprendre à identifier et évaluer les vulnérabilités des systèmes embarqués dans différents environnements (automobile, santé, industrie, etc.).
-
Être capable de concevoir et mettre en oeuvre des solutions de sécurité adaptées aux systèmes embarqués.
Développer une expertise dans l'intégration de mécanismes de protection dans des environnements contraints.

Contenu

Introduction à la sécurité embarquée :
-
Définitions et spécificités des systèmes embarqués.
-
Enjeux de la sécurité dans les systèmes critiques.
Analyse des vulnérabilités des systèmes embarqués :
-
Types d’attaques (hardware et software).
-
Études de scénarios réels d’exploitation des failles.
Méthodes de sécurisation des systèmes embarqués :
-
Techniques de chiffrement et d’authentification adaptées.
-
Protection contre les attaques matérielles (ex. : attaques par canal auxiliaire).
Optimisation des performances et sécurité :
-
Gestion des ressources limitées dans les systèmes embarqués.
Compromis entre performance et sécurité.
Applications industrielles et études de cas :
Sécurisation des systèmes embarqués dans des secteurs tels que l’automobile, l’IoT et la santé.

Prérequis

Connaissances fondamentales en systèmes embarqués et électroniques.

Familiarité avec les concepts de sécurité informatique, notamment la cryptographie et les attaques courantes (ex. : injection, buffer overflow).
Notions de base en programmation (langages tels que C/C++, Python).

Bibliographie

Bibliographie :
-
Embedded Systems Security - David Kleidermacher & Mike Kleidermacher.
-
Hardware Security - Debdeep Mukhopadhyay & Rajat Subhra Chakraborty.
-
Principles of Secure Embedded Systems Design - Peter Gutmann.
Webographie :
Articles et ressources sur les systèmes embarqués : IEEE Xplore.
Guides sur les attaques et protections embarquées : NIST.
Plateformes de formation en cybersécurité embarquée : Cybrary, SANS Institute.

Évaluation(s)

N°	Nature	Coefficient	Objectifs
1		Évaluation diagnostique, formative et sommative	Devoir écrit

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 5
- Sécurisation It/Ot
- Sécurisation Des Iot

Sécurisation Des Iot

Données Générales

Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Sécurisation Des Iot** (LIBCys05ESecIoT)			
TD : 10h00 TP : 10h00 Cours : 10h00 Durée totale: 30h00	Statut Obligatoire	Periode Semestre 5	Langue d'enseignement :	

Acquis d'apprentissage

Le module couvre les éléments suivants :
-
Les principales problématiques de sécurité autour de l'IoT;
-
Les faiblesses et les risques associés en matière de Cybersécurité (gestion, installation, MàJ, manque de standardisation);
-
Les spécificités de l'IoT du point de vue de la cybersécurité;
L'approche de Security by Design appliquée aux IoT;
Les techniques de défense en profondeur : approche mixte prévention / détection / mitigation / réaction appliquées aux IoT
Comment mener une analyse de vulnérabilité portant sur un système IoT;
les réponses techniques et organisationnelles mises en place en général pour répondre aux chemins d'attaque d'un IoT;

Contenu

Comment mener une analyse de vulnérabilité portant sur un système IoT;
les réponses techniques et organisationnelles mises en place en général pour répondre aux chemins d'attaque d'un IoT;

Prérequis

Implémentation des IoT

Bibliographie

Bibliographie :
-
"Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development" – David Kleidermacher, Mike Kleidermacher.
-
Internet of Things Security - Shancang Li.
-

Bibliographie

Securing the Internet of Things - Mark Dunkerley & Matt Tumbarello.
-
IoT Security: Advances and Challenges - Fei Hu.
Webographie :
Ressources sur les bonnes pratiques IoT : NIST IoT Security Guideline
Plateformes éducatives : Cybrary, SANS Institute, articles spécialisés IEEE Xplore.
Blogs et forums spécialisés en IoT et cybersécurité.

Semestre 6

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 6
- Expérience Professionnelle 2

Expérience Professionnelle 2

Données Générales			
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**		Responsable(s) Module GASTARD Loic
Type de module : Unité d'Enseignement	**Expérience Professionnelle 2** (LIBCys06UExpPro)		
Crédits (ECTS)	30		
Effectif maximum	160		
Durée totale : 218h00	Periode Semestre 6	Langue d'enseignement :	

- Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon
- Année CSIU 3
- Semestre 6
- Expérience Professionnelle 2
- Stage en Entreprise

Stage en Entreprise

Données Générales				
Programme Académique	**Formation Bachelor Cybersécurité des Systèmes Industriels et Urbains - Campus Lyon**			Responsable(s) Module : GASTARD Loic
Type d'EC : Cours	**Stage en Entreprise** (LIBCys06EStageEnt)			
Durée totale: 0h00	Statut Obligatoire	Periode Semestre 6	Langue d'enseignement :	