



CATALOGUE DES FORMATIONS 2021



www.gotrust.tn

+216 98 802 000 +216 71 856 600

Smart Tunisian Technoparks, Ariana

Nos Atouts :

- Des formateurs expérimentés
- Des études de cas et des mises en situations concrètes issues du milieu professionnel
- Des stages adaptés pour chaque niveau de responsabilité et de savoir-faire
- Un taux d'ouverture élevé et un nombre limité de participants par stage
- La richesse d'une expérience interprofessionnelle

Smart Content Curation & Micro-Learning

- Flexibilité de programmation des actions.
- Formations « catalogue » adaptées à votre environnement :
- Prise en compte de votre contexte et de vos équipements.
- Formations « sur-mesure » : à partir de vos besoins spécifiques, GoTrust développe complètement le contenu de vos formations.





Notre catalogue comporte
42 modules répartis sur 7 axes

1. SSI : Sécurité des Systèmes d'Informations
2. SRA : Sécurité des Réseaux et des Accès
3. SAD : Sécurité Applicative et des Données
4. SEP : Sécurité des Terminaux
5. SNG : Nouvelles Technologies de Sécurité
6. CHP : Hacking & Tests Intrusifs
7. SMG : Gestion de la Sécurité de l'Information

Learning by Practicing...

CATALOGUE DES FORMATIONS 2021

SSI - Sécurité des Systèmes d'Informations			
Ref-T	Thème de la formation	Durée	Contenu
SSI1 1A	Les bases de la Sécurité Numérique	1 Jour	<ol style="list-style-type: none"> 1. Le danger sur Internet et dans les emails 2. Protection de la vie privée et de la e- réputation 3. La sécurisation pour votre environnement numérique
SSI2 1B	Initiation à la Cybersécurité enjeux & attaques	2 Jours	<ol style="list-style-type: none"> 1. Introduction et état des lieux 2. Vocabulaire et Définitions 3. Menaces et risques SI 4. Les attaques et leurs modes opératoires 5. Mettre en évidence de quelques techniques d'attaques classiques
SSI3 1B	Introduction à la Cybersécurité : Sensibilisation & Bonnes pratiques	2 Jours	<ol style="list-style-type: none"> 1. Les enjeux de la sécurité des S.I. 2. Les besoins de sécurité & les notions de base 3. Panorama de quelques menaces 4. Bonnes pratiques de sécurité SI
SSI4 1A	Introduction à la Cybersécurité pour les Admins IT Aspects réseaux et applicatifs	1 Jour	<ol style="list-style-type: none"> 1. La sécurité du protocole IP 2. Sécurisation d'un réseau 3. Les bases de la cryptographie 4. La sécurité des applications web
SSI5 2B	Audit de Sécurité des Systèmes d'Informations	3 Jours	<ol style="list-style-type: none"> 1. La politique de sécurité SI 2. L'Audit Sécurité : Notions et phases 3. Les types d'audit sécurité 4. Illustration d'un déroulement d'une mission d'audit sécurité
SSI6 2D	Gestion du Parc et des incidents IT selon ITIL avec GLPI	2+2 Jours	<ol style="list-style-type: none"> 1. Les enjeux de la gestion de parc 2. Organisation de l'inventaire de votre parc informatique 3. Gestion votre parc administrativement et financièrement 4. Identification des responsabilités du Centre de services 5. Gestion des incidents 6. Gestion des problèmes 7. Gestion des demandes de changement

CATALOGUE DES FORMATIONS 2021

SRA - Sécurité des Réseaux et des Accès

Ref-T	Thème de la formation	Durée	Contenu
SRA1 2E	Sécurité des réseaux et architectures	5 Jours	<ol style="list-style-type: none"> 1. Rappel de la pile protocolaire TCP/IP 2. Les différents mécanismes de la translation d'adresses (NAT&PAT) 3. Le contrôle d'accès via les listes d'accès ACL 4. Les pare-feu, Proxy et Reverse Proxy 5. Architecture de sécurité et scénarios de déploiement 6. Cloisonnement et segmentation logique 7. Les systèmes de détection d'intrusion IDS/IPS 8. Les réseaux virtuels privés (VPN)
SRA2 2A	Haute disponibilité et répartition de charge	1 Jour	<ol style="list-style-type: none"> 1. Les enjeux et les besoins de HA et LB 2. Les techniques de LoadBalancing 3. Les technologies et les protocoles HA : Network, DB, Security
SRA3 3C	Durcissement de la sécurité des équipements réseaux	3 Jours	<ol style="list-style-type: none"> 1. Sécurité de la couche Management 2. Sécurité de la couche Données 3. Sécurité de la couche Contrôle
SRA4 3A	Le contrôle d'accès aux réseaux (NAC)	1 Jour	<ol style="list-style-type: none"> 1. L'authentification réseau 2. Radius et les serveurs AAA 3. Le standard 802.1x et le protocole EAP
SRA5 2A	Sécurité des réseaux sans fils	1 Jour	<ol style="list-style-type: none"> 1. Menaces et attaques liées aux réseaux sans fils 2. Le cryptage sans fils 3. Les contremesures de protection
SRA6 1A	Sécurité du Cloud Computing	1 Jour	<ol style="list-style-type: none"> 1. Concepts et models du Cloud 2. Les menaces et les attaques liées aux Cloud 3. Les lignes directives pour la sécurité du Cloud

SAD - Sécurité Applicative et des Données

Ref.	Thème de la formation	Durée	Contenu
SAD1 2B	Sécurité des échanges et Cryptographie	2 Jours	<ol style="list-style-type: none"> 1. Les besoins en cryptographie 2. Les crypto-systèmes symétriques et asymétriques 3. Les infrastructures à clé publiques PKI 4. Le protocole SSL

CATALOGUE DES FORMATIONS 2021

<p>SAD2 2C</p>	<p>Sécurité et Pentesting des plateformes VOIP</p>	<p>3 Jours</p>	<ol style="list-style-type: none"> 1. Introduction à la VOIP 2. Menaces et attaques liés à la sécurité de la VoIP 3. Hacking Voip 4. Bonnes pratiques et sécurisation des architectures VoIP
<p>SAD3 2A</p>	<p>Sécurité Applicative & OWASP 2017</p>	<p>1 Jour</p>	<ol style="list-style-type: none"> 1. Fondements de la sécurité applicative et prise en charge avec les outils OWASP 2. Présentation des TOP 10 risques OWASP 2017 3. Mise en pratique des attaques sur une plateforme de simulation 4. Exemple de Hardening d'un environnement Web
<p>SAD4 3C</p>	<p>Sécurisation du Code Source avec OWASP</p>	<p>3 Jours</p>	<ol style="list-style-type: none"> 5. Protégez votre code contre l'injection 6. Empêchez le piratage de session 7. Protégez les données en transit 8. Protégez les données stockées sur une application 9. Empêchez l'exploitation des contrôles d'accès 10. Stoppez le cross-site scripting (XSS) 11. Protégez votre code contre les failles XXE et la désérialisation non sécurisée 12. Sécurisez votre environnement de développement
<p>SAD5 3B</p>	<p>Sécurisation du Cycle de Développement</p>	<p>2 Jours</p>	<ol style="list-style-type: none"> 1. Testez la sécurité de votre application 2. Audit applicatif et du code (SAST) 3. Sécurité du cycle de développement (SSDLC)* 4. La sécurité avec l'Agilité 5. Le concept SecDevOps
<p>SAD6 3C</p>	<p>Pentesting Web & Contremesures</p>	<p>3 Jours</p>	<ol style="list-style-type: none"> 1. Menaces des serveurs Web 2. Attaques des serveurs Web 3. Méthodologie du Hacking Web Servers 4. Tests intrusifs et exploits 5. Contremesures de protection des WS 6. Technologies de protection d'une plateforme Web (WAF)
<p>SAD7 3C</p>	<p>Data Protection & Privacy Data Protection Officer</p>	<p>(2+1) Jours</p>	<ol style="list-style-type: none"> 1. DPO Fondation : Les enjeux et les risques liés à la gestion des données personnelles 2. DPO Fondation : Mise en œuvre de la protection de la vie privée 3. DPO Practitioner : Sécurisation des traitements de données sensibles 4. DPO Practitioner : Anonymisation des données

CATALOGUE DES FORMATIONS 2021

SEP – Sécurité des Terminaux			
Ref-T	Thème de la formation	Durée	Contenu
SEP1 3B	Vulnerability Management Vulnerability Handler	2 Jours	<ol style="list-style-type: none"> 1. Introduction à la gestion des vulnérabilités 2. Mise en œuvre d'un Processus de gestion des vulnérabilités 3. Exemple pratique de gestion des vulnérabilités 4. L'évolution du Cycle de Gestion des Vulnérabilités 5. Les nouveaux systèmes de gestion des vulnérabilités – VMS
SEP2 1A	Sécurité des plateformes mobiles	1 Jour	<ol style="list-style-type: none"> 1. Les vecteurs d'attaques des plateformes mobiles 2. Hacking Android, IOS.. 3. Mobile Device Management (MDM) & BYOD 4. Les bonnes pratiques de protection
SEP3 1A	La sécurité des objets IoT	1 Jour	<ol style="list-style-type: none"> 1. Concept IoT 2. Les attaques IoT 3. IoT attack methodology 4. Contremesures
SEP4 2B	Fondements de la Sécurité Windows	2 Jours	<ol style="list-style-type: none"> 1. Sécurité des postes de travail Windows 10 2. Sécurité des serveurs Windows 2016 Server
SEP5 3B	Sécurisation du domaine avec Active Directory	2 Jours	<ol style="list-style-type: none"> 1. Active Directory : Concepts & mise en place 2. Maîtrise du parc grâce aux stratégies de groupe (GPO) 3. Recommandations pour la sécurisation des ressources du domaine
SEP6 3C	Mastering Linux Security & Hardening	3 Jours	<ol style="list-style-type: none"> 1. Sécurisation des comptes utilisateurs 2. Sécurisation du serveur avec un pare-feu 3. Le chiffrement et durcissement SSH 4. Le contrôle d'accès discrétionnaire (DAC) 5. Listes de contrôle d'accès (ACL) et gestion des répertoires partagés 6. Le contrôle d'accès obligatoire (MAC) 7. Audit & Durcissement du Linux

CATALOGUE DES FORMATIONS 2021

SNG- Nouvelles Technologies de Sécurité

Ref-T	Thème de la formation	Durée	Contenu
SNG1 3B	Cybersecurity Intelligence Incident Response Technologies	2 Jours	<ol style="list-style-type: none"> 1. EndPoint Detection & Response - EDR 2. NG Security Information & Event Manager NG-SIEM 3. User Behavior & Entities Analytics -UEBA 4. Security Orchestration Automation & Response - SOAR
SNG2 2B	Cybersecurity Monitoring SOC Foundation	1 - 2 Jour	<ol style="list-style-type: none"> 1. Les enjeux et l'art de la surveillance du SI 2. Security Opérationnel Center –SOC & Modèles 3. La technologie SIEM & Fonctionnement
SNG3 3C	Cybersecurity Monitoring SIEM Lead Implementer	3 Jours	<ol style="list-style-type: none"> 1. Les sources de données et la collecte de logs 2. Centralisation des alertes avec la stack ELK 3. Les scénarios d'attaque et de détections avec la matrice MITRE ATT&CK 4. Les analyses tactiques SIEM

CHP – Hacking & Tests Intrusifs

Ref-T	Thème de la formation	Durée	Contenu
CHP1 2B	Cyber Attacks & Hacking Basics	2 Jours	<ol style="list-style-type: none"> 1. La Cybercriminalité et impacts 2. Nouvelles déclinaisons et vecteurs d'attaques 3. La méthodologie et les phases de Hacking 4. Illustration pratique et prise de contrôle d'une victime 5. Déploiement d'un malware et création d'un Botnet
CHP2 3D	Test Intrusifs Penetration Tester	4 Jours	<ol style="list-style-type: none"> 1. Préparation aux Tests d'intrusion - Notions & Méthodologies 2. Réalisation des tests d'intrusion 3. Rédaction du rapport de test d'intrusion
CHP3 3D	Forensics Investigation Cyber Forensics Analyst	4 Jours	<ol style="list-style-type: none"> 1. Préparez votre investigation numérique 2. Analysez le dump mémoire 3. Analysez la copie du disque dur 4. Analysez les fichiers malveillants 5. Corrélerez vos analyses forensic pour établir un rapport
CHP4 3E	Préparation à la certification CEH	5 Jours	<ol style="list-style-type: none"> 1. Introduction to Ethical Hacking 2. Footprinting and Reconnaissance 3. Scanning Networks 4. Enumeration 5. System Hacking 6. Malware Threats 7. Sniffing 8. Social Engineering

CATALOGUE DES FORMATIONS 2021

SMG – Gestion de la Sécurité de l'Information			
Ref-T	Thème de la formation	Durée	Contenu
SMG1 1A	Introduction à la Cybersécurité pour les Managers La gestion de la cybersécurité	1 Jour	<ol style="list-style-type: none"> 1. Intégrer la sécurité au sein d'une organisation 2. Intégrer la sécurité dans les projets 3. Difficultés liées à la prise en compte de la sécurité 4. Métiers liés à la cybersécurité
SMG2 3C	Cybersecurity Incident Management Cyber Incident Responder	3 Jours	<ol style="list-style-type: none"> 1. Principes de la gestion des incidents cybersécurité 2. Référentiels : ISO27035 & NIST SP800-61 3. Mise en œuvre du processus de gestion des incidents cybersécurité 4. Exemples de réponses à des scénarios d'incidents cybersécurité 5. La gestion des incidents : de la réactivité à la proactivité
SMG3 3C	ISO 22301 Business Continuity Lead Implementer	3 jours	<ol style="list-style-type: none"> 1. Identifiez les enjeux de la continuité d'activité 2. Préparation plan de continuité d'activité 3. Mise en œuvre et maintien du plan de continuité d'activité
SMG4 3B	ISO 27032 LCM Cybersecurity Program	2 jour	<ol style="list-style-type: none"> 1. Notions fondamentales de la cyber sécurité 2. Programme de cyber sécurité 3. Initier un programme de cyber sécurité 4. Analyser l'organisme & Leadership 5. Politique de cyber sécurité 6. Gestion des cyber-risques
SMG5 3A	ISO 27032 LCM Cyberattacks et countermeasures	1 jour	<ol style="list-style-type: none"> 1. Mécanismes d'attaque 2. Mesures de sécurité de cyber sécurité 3. Partage et coordination de l'information 4. Programme de formation et de sensibilisation
SMG6 3A	ISO 27032 LCM Business Continuity & cyber incidents management	1 jour	<ol style="list-style-type: none"> 1. Continuité des activités 2. Management des incidents de cyber sécurité 3. Intervention et récupération en cas d'incident de cyber sécurité 4. Effectuer des tests en cyber sécurité 5. Mesure de la performance 6. Amélioration continue
SMG7 1A	ISO 27001:2013 Essentiels for Information Security Management	1 jour	<ol style="list-style-type: none"> 1. Principes fondamentaux de la sécurité de l'information 2. Processus de certification 3. Système de management de la sécurité de l'information (SMSI)
SMG8 3C	ISO 27001:2013 ISMS Lead Auditor	3 jours	<ol style="list-style-type: none"> 1. Concepts et principes fondamentaux d'audit 2. Approche d'audit fondée sur la preuve et sur le risque 3. Déclenchement de l'audit

CATALOGUE DES FORMATIONS 2021

SMG – Gestion de la Sécurité de l'Information			
Ref-T	Thème de la formation	Durée	Contenu
			<ol style="list-style-type: none"> 4. Audit d'étape 1 5. Préparation de l'audit d'étape 2 6. L'audit d'étape 2 7. La communication durant l'audit 8. Les procédures d'audit 9. Elaboration des plans de tests d'audit 10. Rédaction des constatations d'audit et des rapports de non-conformité 11. Documentation de l'audit et revue de qualité 12. Clôture de l'audit 13. Évaluation de plans d'action par l'auditeur 14. Suites à l'audit initial 15. Gestion d'un programme d'audit interne
SMG9 3A	ISO 27005:2018 Building Risk Management Program	1 jour	<ol style="list-style-type: none"> 1. Cadre normatif et réglementaire 2. Concepts et définition des risques 3. Programme de gestion des risques 4. Etablissement du contexte
SMG10 3B	ISO 27005:2018 Risk Management Process Implementer	2 jours	<ol style="list-style-type: none"> 1. Identification du risque 2. Analyse du risque 3. Evaluation du risque 4. Appréciation des risques avec une méthode quantitative 5. Traitement du risque 6. Acceptation du risque en sécurité de l'information 7. Communication & Suivi du risque



www.gotrust.tn

+216 98 802 000 ☎ +216 71 856 600

Smart Tunisian Technoparks, Ariana