

Catalogue des activités et missions proposées

Thème	Prestations	Description	Durée indicative
Tests d'intrusion 	Pentest White box interne	Test d'intrusion et audit de configuration qui permettent d'être exhaustif dans la recherche de vulnérabilités	5 jours
	Pentest Grey box interne	Test d'intrusion simulant un attaquant disposant d'informations sur l'organisation	3 à 5 jours
	Pentest Black box Interne	Test d'intrusion qui permet de simuler un visiteur souhaitant nuire physiquement à l'organisation	5 à 7 jours
	Pentest Black box Externe	Test d'intrusion qui permet de simuler un attaquant partant de zéro	10 jours
	Test d'intrusion WEB	Test d'intrusion mené sur une application web qui permet d'identifier des failles de développement	5 jours
	Test d'intrusion Azure	Test d'intrusion sur une infrastructure utilisant Azure permettant de mettre en avant les défaut de configuration	3 à 5 jours
	Scan de vulnérabilités	Scan de l'infrastructure qui permet de mettre en lumière des failles potentielles sans les exploiter	2 jours
Audits 	Audit Flash	Audit rapide technique et organisationnel mettant en lumière des axes d'amélioration immédiats	1 à 2 jours
	Audit Guide d'Hygiene	Audit technique et organisationnel basé sur le référentiel de l'ANSSI	3 à 5 jours
	Audit des mots de passe	Audit des bases de mots de passe permettant d'identifier leur robustesse	1,5 jour
	Audit Active Directory	Audit de l'Active Directory permettant d'identifier des défauts de configuration	3 à 5 jours
	Audit Azure / M365	Audit de configuration Azure et M365 permettant d'identifier les défauts de configuration	3 à 5 jours
	Audit 27002	Audit organisationnel permettant d'évaluer le niveau de maturité des équipes sur les sujets Sécurité	3 à 5 jours
	Audit 27001	Audit organisationnel permettant d'évaluer le niveau de maturité du SMSI	3 à 5 jours
Sensibilisation 	Campagne de Phishing	Exercice permettant de tester la réaction des utilisateurs face à un mail frauduleux	2 à 4 jours
	Sensibilisation utilisateurs	Session de sensibilisation des utilisateurs aux risques et enjeux de la cybersécurité pour l'organisation	1 jour par session
	Sensibilisation administrateurs	Session de formation du personnel IT aux risques et bonnes pratiques	3 à 5 jours par session
	Escape Games Cyber	Session de sensibilisation par la mise en situation des utilisateurs de type Escape Game	1H30 par session (Hors installation)
Technique 	Tiering Model AD	Accompagnement organisationnel et technique sur la mise en oeuvre du Tiering Model	20 jours
	Bastion sécurisé	Design et mise en oeuvre d'un bastion d'administration	10 à 15 jours
	Sécurisation Azure / M365	Accompagnement organisationnel et technique sur la sécurisation de tenants Azure et/ou M365	Suivant périmètre
	Sécurisation Infra / Réseau	Accompagnement organisationnel et technique sur la sécurisation de vos infrastructures systèmes et réseaux	Suivant périmètre
	Continuité des opérations IT	Accompagnement organisationnel et technique sur la mise en oeuvre d'une stratégie de résilience IT (PCI / PRI)	Suivant périmètre

Catalogue des activités et missions proposées

Thème	Prestations	Description	Durée indicative
Gouvernance 	Analyse de risque	Analyse de risque orientée cyber, basée sur la méthode EBIOS RM	10 jours
	Accompagnement NIS2	Audit et accompagnement à la mise en conformité à la directive NIS 2	Suivant périmètre
	Accompagnement ISO 27001	Audit et accompagnement à la mise en conformité à la norme ISO 27001	Suivant périmètre
	Accompagnement ISO 27031	Audit et accompagnement à la mise en place d'une continuité informatique de vos systèmes	Suivant périmètre
	Accompagnement ISO 22301	Audit et accompagnement à la mise en place d'une continuité d'activité de vos processus métiers	Suivant périmètre
	Assistance à rédaction PSI / PSSI	Assistance à la rédaction de documents stratégiques dans un SMSI (PSI / PSSI / Politiques)	3 à 5 jours
	RSSI à temps partagé	Mission de RSSI à part entière pour un nombre de jours par semaine / mois afin de vous épauler en continu	Forfait mensuel
Formation 	Formation EBIOS RM	Formation certifiante de vos équipes à la gestion de risque (Formation et certification PECB)	2 Jours
	Formation ISO 27005	Formation certifiante de vos équipes à la norme ISO27005 (Formation et certification PECB)	3 Jours
	Formation 27001 Implementer	Formation certifiante à la mise en place d'un SMSI (Formation et certification PECB)	4 Jours
	Formation 27001 Auditor	Formation certifiante à l'audit d'un SMSI (Formation et certification PECB)	4 Jours
	Initiation au Pentest	Rendez vos équipes autonomes sur la recherche de vulnérabilités sur vos architectures	A partir de 4 Jours
	Formation à la sécurisation Infra	Formation mettant en avant les éléments critiques de configuration (AD / Bastion / Siem)	A partir de 4 Jours
Résilience 	Gestion de crise	Accompagnement à la construction d'un socle de gestion de crise cyber	Suivant périmètre
	Rédaction de fiches réflexes	Réalisation de fiches reflexes sur les sujets cyber à destination du personnel	Suivant périmètre
	Tests en exercices "crash test"	Accompagnement et réalisation d'exercices de simulation de crises IT	Suivant périmètre

Pour tout autre besoin, contactez nous

Notre expertise et notre réseau de partenaires sont à votre disposition pour tous les sujets cyber