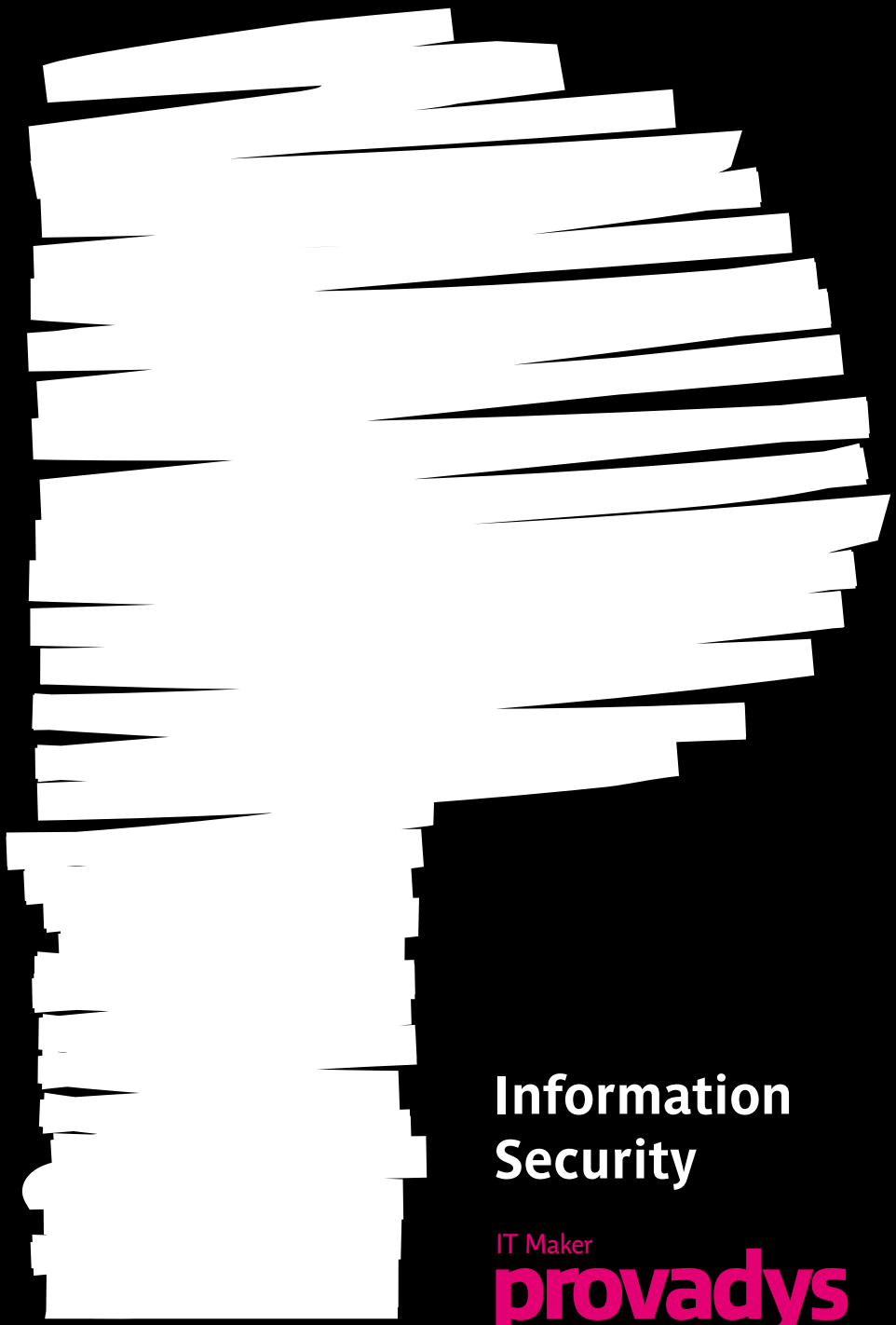


Information Security

IT Maker

provadys

Notre mission

Conseiller autrement.

S'adapter aux besoins des clients
par l'écoute active et des compétences adaptées.
Mettre nos savoir-faire au service des entreprises pour
accompagner leur transformation numérique.

Notre vision

Être un acteur de référence sur tous nos savoir-faire
et délivrer un haut niveau de qualité unanimement reconnu.
Toujours viser l'excellence et transformer
l'expertise en valeur ajoutée.

Nos valeurs

Energie & Structure

VISA DE SÉCURITÉ — ANSSI

Édito

Maîtriser les risques et sécuriser les systèmes d'information semblent aujourd'hui des objectifs évidents pour toutes les organisations.
Pourtant, l'actualité nous montre chaque jour que cette tâche demeure colossale et face à elle beaucoup sont comme désorientés. Au sein de Provadys Information Security, nous sommes persuadés qu'il est possible d'agir efficacement pour aider les entreprises à protéger leurs informations et leur performance face à la cybercriminalité. Nous croyons en effet que pour chaque entreprise il existe une trajectoire faite de stratégie, de processus et de technologies permettant d'atteindre une situation de sécurité optimale. Il n'y a pas de risque zéro pas plus que de budget illimité ou encore de technologie sans faille. Pourtant, nous démontrons tous les jours avec nos clients que, puisque c'est désormais indispensable, ils peuvent opérer et prospérer dans le monde numérique en maîtrisant les risques liés à la sécurité de leurs SI.

“ sécurité optimale ”

LUC DELPHA
Partner & Lead

Provadys
Information Security

@LucDelpha

3 Principes fondamentaux

Les activités de Provadys Information Security sont construites autour de 3 principes fondamentaux :

Sécurité
Conformité
Résilience

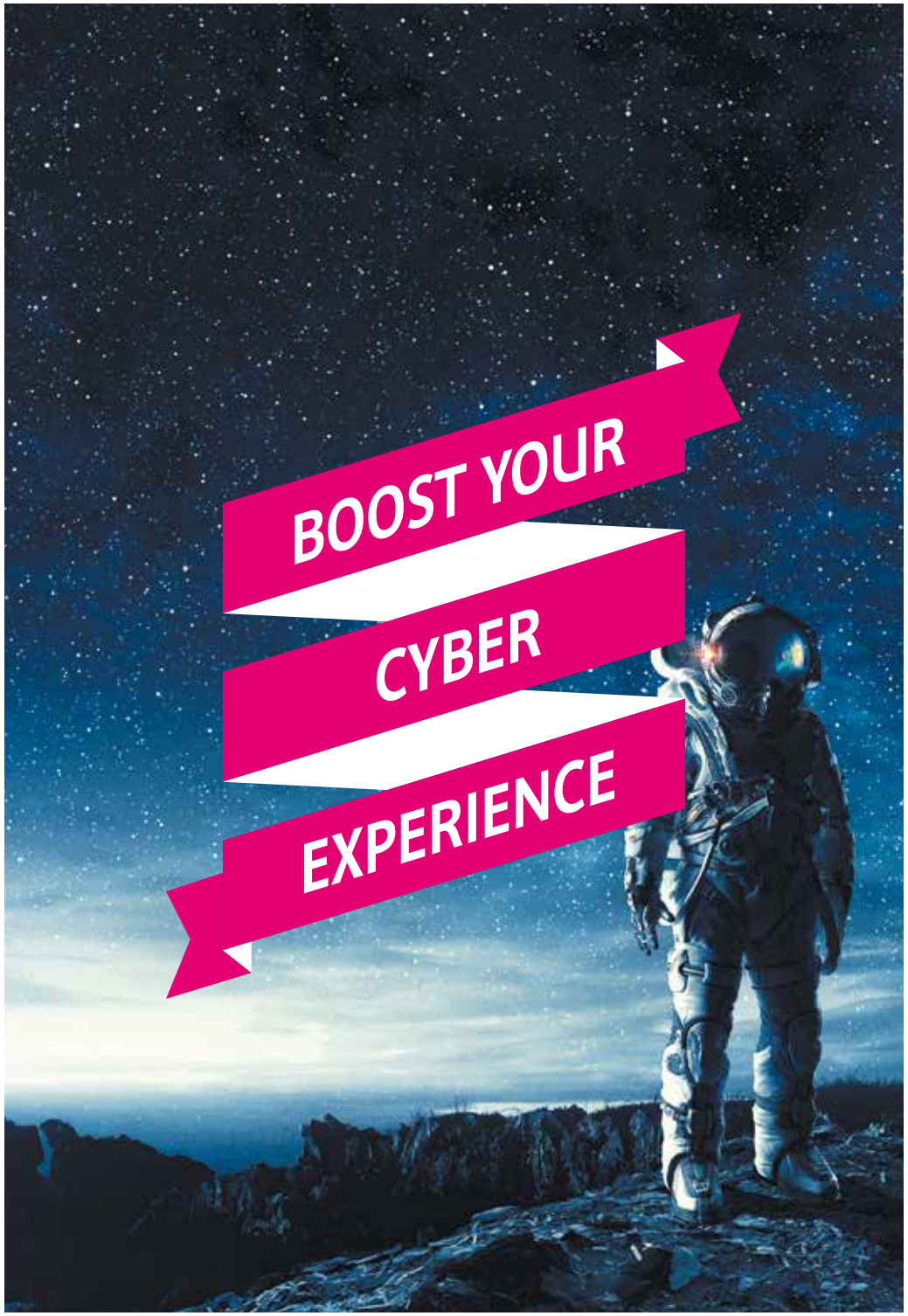
	Offensive Security	Defensive Security	Compliance	SOC
Vos défis	Evaluer objectivement et précisément la sécurité des Systèmes d'Information.	Mettre en œuvre et opérer tous les moyens permettant de défendre le SI et maîtriser les risques.	Atteindre, maintenir et démontrer la conformité aux référentiels choisis ou imposés à l'entreprise .	Protéger au quotidien votre entreprise contre les cybercriminels et gérer les incidents de sécurité pour en limiter les impacts sur votre activité.
Notre vision	L'expertise des techniques d'attaque doit permettre d'alimenter des évaluations qui partent des faits techniques pour démontrer les risques métier.	Le niveau de Cyber-Résilience et la robustesse de la défense d'un SI reposent sur un subtil équilibre entre Stratégie, Technologies et Processus.	La conformité peut être une opportunité si elle est mise au service de l'entreprise et si elle sert de support à des objectifs de sécurité.	La sécurité opérationnelle n'est pas réservée aux grandes entreprises, mais les solutions doivent être adaptées aux enjeux et moyens des PME/ETI.
Notre approche	Détecter des vulnérabilités en utilisant les mêmes techniques que les cybercriminels.C'est aussi en exploitant ces faiblesses que nous déterminerons toutes les possibilités criminelles qui doivent être corrigées.	Placer la sécurité au cœur des projets de transformation et de digitalisation des entreprises. Agir avec expertises et méthodologie aussi bien au niveau des infrastructures, des applications que des processus ; pour la préservation des entreprises.	Mettre en conformité avec les référentiels et certifications Approche pragmatique pour la sécurité et les spécificités de chaque client.	Cibler les menaces pertinentes dans votre contexte. Combiner des solutions simples, prêtes à l'emploi et économiques de protection, de détection et de réponse à incident de sécurité. Optimiser l'usage des moyens disponibles pour adresser en priorité les événements redoutés spécifiquement par votre entreprise.

Nos expertises	• Tests d'Intrusion
	  ◦ Boite noire
	  ◦ Boite grise
	  ◦ Boite blanche
	  ◦ Red Team
	• Audits de code
	• Audits de configurations
	• Audits d'architecture
	• Reverse Engineering
	• Social Engineering
	• Expertises techniques
		• Gouvernance de la SSI
		• PSSI - Charte - TDB
		• Définition et mise en place de processus SSI
		• Analyse de risques
		• Sensibilisation - Phishing factice
		• Accompagnement à la mise en œuvre des solutions de sécurité
		• Audits organisationnels
		• BIA - PCA - PRA - PSI - PRU
		• Gestion, Tests et Exercices de Cyber-Crise
		• Veille, Détection et Gestion d'incidents de sécurité
			• Certification PCI DSS
			• Certification ARJEL
			• Mise en conformité PCI DSS, ARJEL, LPM, ASIP, ISO27001
			• DCP : Cartographie et conformité au RGPD
			• Audit de conformité aux référentiels internes et sectoriels
			• Audit des fournisseurs de services (TMA, Infogérance, SaaS…)
				• Services SOC / C-SIRT
				• Réponse à incident de sécurité : analyse, endiguement, éradication, retour à la normale, gestion de crises cyber, accompagnement communication, notification et dépôt de plainte
				• Services managés de détection d'incidents de sécurité internes et externes
				• Service de protection : scan et gestion de vulnérabilités, gestion solutions EDR
				• Threat intelligence tactique issue de nos activités offensives
				• Conseil et audit organisation SOC / C-SIRT

“

Dans un monde en pleine révolution digitale, les cyber attaques se font de plus en plus présentes. Elles sont à la fois, plus massives et plus ciblées. La technologie ne suffit plus à contrer les attaquants, les utilisateurs par leur capacité d’analyse et de réaction sont bien placés pour détecter une attaque et ainsi contribuer à limiter sa propagation.

”



Boost
your cyber experience

Faites de vos utilisateurs, le maillon fort de votre sécurité informatique !

BYCE, le E-Learning conçu pour vous :

- Une formation intuitive, interactive et ludique.
- Prêts à l'emploi ou sur-mesures plus de 10 modules disponibles en 24h.
- Une solution pour une sensibilisation aux résultats efficaces et pérennes.
- Accessible de 7 à 77 ans !

ACCESSIBLE DE 7 À 77 ANS

- **BYCE**, votre E-learning de sensibilisation, prêt à l'emploi et disponible immédiatement.
- Quel que soit votre nombre d'utilisateurs, leur mode de travail et la configuration de votre système d'information, **BYCE** vous permet de déployer, en un temps record, vos campagnes de sensibilisation.
- **Avec BYCE**, vos utilisateurs auront une vision réelle des dangers et adopteront les bons réflexes pour s'en prémunir.

“ LES + BYCE ”

#1 10 à 15 minutes par module pour être suivi sans contrainte.	#2 Tous les modules sont construits suivant un même schéma pour faciliter l'apprentissage.
#3 Nous proposons une variété de quiz spécialement conçus pour le confort de l'utilisateur.	#4 Nous employons un vocabulaire accessible même pour expliquer des concepts informatiques.

Notre E-Learning vous garantit l'efficacité d'apprentissage.

Nos modules sont entièrement conçus par nos experts qui s'attachent à véhiculer les messages importants permettant à l'utilisateur de comprendre :

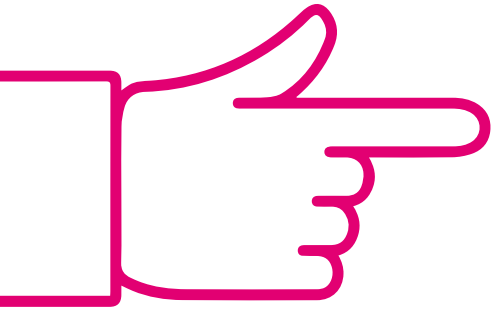
- Les risques de son comportement pour son entreprise et lui-même.
- Les réactions à adopter face aux différentes situations.
- Les personnes à contacter au sein de votre organisation.

L'utilisateur se prend au jeu et a envie de poursuivre. Il ne voit pas le temps passer :

- Les textes sont revus par nos spécialistes en psychologie cognitive.
- L'utilisateur est acteur de sa formation.
- L'utilisateur peut mesurer ses propres progrès.

7

Notes pour composer la sécurité



1. Aligner

Sans stratégie, il n'est pas de victoire possible. Aligner la sécurité sur la stratégie de l'entreprise. Contribuer à la chaîne de valeur de l'entreprise.
SDSSI - PSSI

2. Mobiliser

Impliquer tous les acteurs de l'entreprise. Faire de chaque utilisateur un élément de défense du SI. **Sensibilisation**

3. S'équiper

Mettre en œuvre les technologies de sécurité et les bonnes pratiques adaptées au contexte de l'entreprise. **AMOA - Architecture**

4. S'organiser

Mettre en œuvre l'organisation et les processus de gestion de la sécurité. Se mettre en conformité avec les normes et standards applicables.
RSSI on demand - SMSI

5. Évaluer

Auditer, Corriger, Vérifier et Auditer encore.
Audit - Tests d'intrusion

6. Se préparer

Anticiper et s'entraîner pour minimiser les impacts des crises. **PRA - Cyber-Resilience**

7. Apprendre

Développer l'expertise sécurité. Cultiver la connaissance de la menace pour anticiper.
Veille - Formation

Information Security

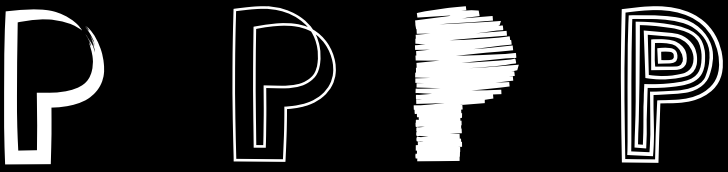
Nos expertises

Offensive Security, Defensive Security

Compliance, SOC, Boost your cyber experience

Pour une sécurité optimale

CESIN arjel PCI DSS CLUSIF



provadys

Paris | Sophia Antipolis | Nantes

provadys.com