La Région
Auvergne-Rhône-Alpes
ENTREPRISES

Intelligence Économique et Territoriale

LES ACTEURS DE LA FILIÈRE CYBERSÉCURITÉ EN AUVERGNE-RHÔNE-ALPES

Panorama régional - Mars 2026 (2e édition)

PRÉAMBULE

— Ce document a été réalisé par le pôle Intelligence Économique et Territoriale (IET) d'Auvergne-Rhône-Alpes Entreprises en partenariat avec la **Région Auvergne-Rhône-Alpes, la Délégation de la Région à Bruxelles, le Campus Région du numérique**, le pôle de compétitivité **Minalogic**, le cluster **Digital League**, l'**ENE** (les Experts du Numérique en Entreprises), l'**ADIRA**, le **CLUSIR Auvergne-Rhône-Alpes** (Club de la Sécurité des Systèmes d'Information), la **CCI Lyon Saint-Etienne Roanne Métropole, la CCIR Auvergne-Rhône-Alpes, le cluster EDEN, le CEA Grenoble, Cybermalveillance.gouv**, **Grenoble INP ESISAR**, la plateforme technologique **SWARM**, la **French Tech Lyon Saint-Etienne**, l'incubateur **Linksium, Cyber Alps, la Fédération Informatique de Lyon** et le laboratoire de recherche **LIMOS**.

— Ce panorama vise plusieurs objectifs :

- mettre en lumière les enjeux et perspectives de la filière,
- valoriser les acteurs régionaux et leurs compétences,
- montrer le poids économique de la filière cybersécurité en Auvergne-Rhône-Alpes.

SOMMAIRE

MÉTHODOLOGIE

SOURCES

— Les chiffres, les statistiques et l'analyse du tissu économique sont le fruit du travail de recensement et de qualification des acteurs du pôle IET.

— Les données sont issues des sources suivantes :
- la base de données entreprises Diane+ à partir des mots-clés suivants : "*cybersécurité*", "*pare-feu*", "*cyber*", "*protection numérique*", "*cloud*", "*chiffrement*", "*réponse à incident*", "*pentest*", "*audit numérique*", "*gestion des accès*", "*maintien en conditions opérationnelles*", "*SIEM*", "*SOC*"...
- la base CRM et les connaissances des chargés d'affaires de l'agence Auvergne-Rhône-Alpes Entreprises ;
- la veille interne réalisée au sein du pôle IET ;
- la liste des adhérents de **Minalogic, Digital League**, du **CLUSIR**, de l'**ADIRA** et du cluster **EDEN** ;
- les prestataires de services cyber mobilisés par l'ENE dans le cadre d'Industrie du Futur ;
- les exposants aux salons : INCYBER 2025, VivaTech 2025, Les Assises de la Cybersécurité Monaco, Lyon Cyber Expo 2025, Accessecurity, Paris Cyber Summit, European Cyber Week 2025 ;
- Les entreprises recensées dans le Panorama Cybersécurité réalisé en 2024 par le pôle IET d'Auvergne-Rhône-Alpes Entreprises.

PÉRIMÈTRE

— Dans ce panorama, la cybersécurité est considérée au sens large, c'est-à-dire *l'ensemble des entreprises qui relèvent de la protection de l'écosystème de des systèmes d'informations, des ordinateurs, des réseaux, des serveurs, des appareils mobiles, des communications et des données*. Les quatre grands domaines et champs d'intervention de la cybersécurité sont analysés : **Gouvernance, Défense, Protection et Résilience / Remédiation**.

— Sont ciblées par cette étude, les entreprises[1] ayant leur siège ou disposant d'au moins un établissement[1] secondaire en Auvergne-Rhône-Alpes et étant des unités employeuses (sauf pour les cabinets de consultants et d'audit cyber très spécialisés, comme pour les *pure players)*.

— Le cœur de cible de cette étude comprend les fournisseurs de solutions et les prestataires de services possédant au moins une expertise dans le champ de la cybersécurité, les cabinets de consultants, de conseil ou d'audits spécialisés de manière assez explicite sur des missions de cybersécurité, les hébergeurs sécurisés, les centres de formation continue en cybersécurité.

— Sont exclues du panel les entreprises pour lesquelles aucune trace d'activité en cybersécurité n'a clairement été identifiée, les cabinets d'avocats spécialisées en cybersécurité ont également été exclus du recensement.

[1] **Différence entre une entreprise et un établissement** : une entreprise est une combinaison d'unités légales constituant une unité organisationnelle de production jouissant d'une certaine autonomie de décision. Un établissement est une unité de production qui, bien que géographiquement individualisée, se rattache juridiquement à l'entreprise.

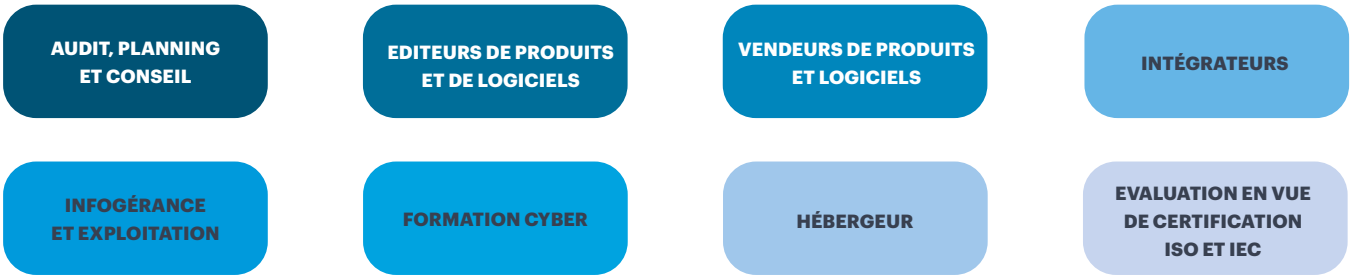
SEGMENTATIONS

— Les entreprises ont été qualifiées selon leur métier cyber principal, leur(s) expertise(s) parmi les quatre grands champs d'intervention de la cybersécurité, et leur domaine d'application dans les produits ou services délivrés

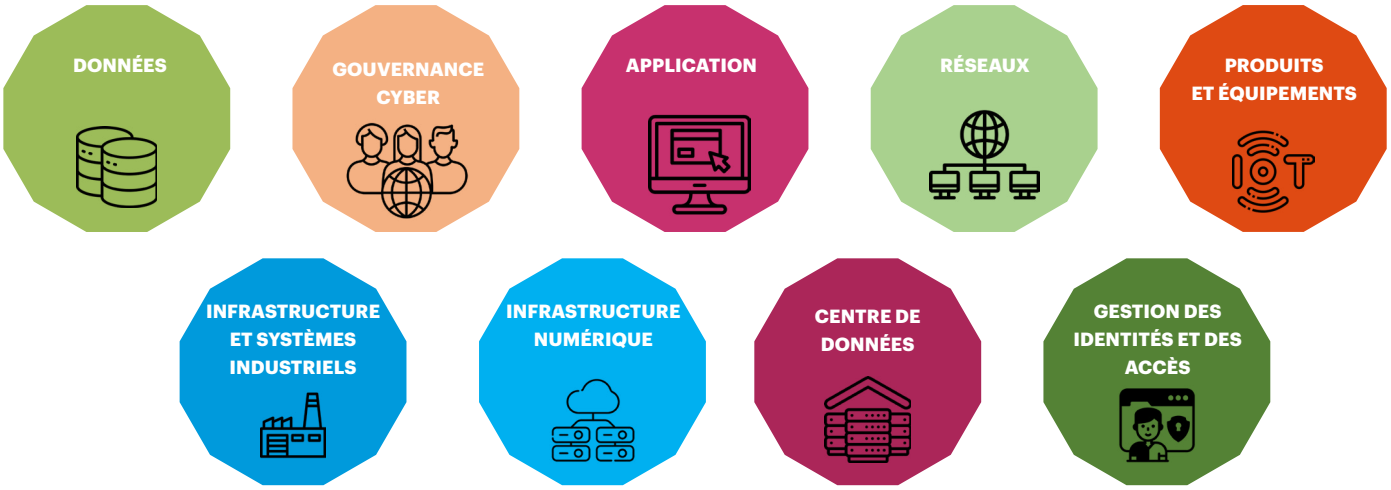
Biais et limites de l'analyse

La qualification des entreprises a été effectuée sur une base déclarative, principalement à partir des contenus des sites Internet des entreprises et l'expertise de nos partenaires lors de la qualification des entreprises.

Métier cyber principal



Domaines d'application



Expertises maitrisées dans les 4 grands champs de compétence cyber

GOUVERNANCE CYBER	PROTECTION CYBER	DÉFENSE CYBER	RÉSILIENCE ET REMÉDIATION CYBER
Assurance	Audit de code source	SOC	Forensique
Audit organisationnel	Exercice de PRI / PCI	SIEM	Conservation de la preuve
Audit technique	Gestion des identités	SecDevops	Pilotage PRA / PCA
Juridique	Communication / sensibilisation	Dashboards sécurité	Gestion de crise
Exercice de crise	Solution de chiffrement	Réponse à incident	Réponse à incident
Cartographie	Protection de la donnée	Analyses forensiques	IAAS sécurisée
Analyse des risques	Protection des produits	Patch Management	Procédure UDRP USR
Politique de sécurité	Protection des postes de travail	MCO	
Ordonnancement / planification	Protection des infrastructures	Service de sécurité infogérés	
Classification de la donnée	Protection des communications	Cloud de confiance	
Veille sur la menace / CTI	Protection des terminaux mobiles	Chiffrement	
Analyse de la surface d'attaque	Veille e-réputation et fuite de données	Blockchain	
	Protection des services	Archivage	
		Pentest	
		Exercice PRI / PCI	
		Exercice de crise	
		Bugbounty	

Note méthodologique

Chaque établissement du panel d'analyse régional (583 établissements) s'est vu attribué une ou plusieurs expertises au sein des 4 grands domaines d'activité cyber : la **gouvernance cyber** (p. 14), la **protection cyber** (p. 15), la **défense cyber** (p. 16) et la **résilience / remédiation cyber** (p. 17).

Par ailleurs, il est possible qu'un établissement ne possède pas d'expertises sur un ou plusieurs de ces 4 grands domaines d'activité cyber.

- Par exemple, une entreprise qui intègre des pare-feu, des antivirus et des antispam au sein des entreprises ne se verra attribuer que des expertises dans le domaine d'activité « Protection cyber » avec les expertises suivantes renseignées : « Protection des infrastructures » et « Protection des communications »

Certifications

PASSI / LPM RGS | PACS / PRIS | SecNumCloud | CSPN | CC

Labellisation

Expert Cyber (AFNOR)

L'ESSENTIEL

LA FILIÈRE CYBERSÉCURITÉ EN AUVERGNE-RHÔNE-ALPES : UN TERRITOIRE MOTEUR À L'ÉCHELLE NATIONALE

469 ENTREPRISES
soit
583 ÉTABLISSEMENTS

135 ENTREPRISES *Pure players*

1 240 EMPLOIS

287 M€ CHIFFRE D'AFFAIRES

65 % TPE/PME

21 % ETI

14 % Grand Groupe

87 % dans

- **309 (53 %)** Rhône
- **91 (16 %)** Isère
- **43 (7 %)** Puy-de-Dôme
- **33 (6 %)** Loire
- **30 (5 %)** Haute-Savoie

Une filière d'excellence

portée par des leaders nationaux et internationaux

(Orange Cyberdéfense, Stormshield, Thales, Capgemini, CGI..) et des PME très innovantes (Algosecure, Tenacy KNS, Chambersign, Aphelio, Excube, Artecys, Vaadata, Recoveo, Root-Me Pro, Serenicity...)

12 % ENTREPRISES À CAPITAUX ÉTRANGERS

- **19** entreprises
- **7** entreprises
- **4** entreprises
- **3** entreprises
- **3** entreprises

Les 5 principaux pays investisseurs cités ci-dessus sont présentés sans prendre en compte le Luxembourg (6 têtes de groupe)

LES PRINCIPAUX MÉTIERS ET DOMAINES D'APPLICATION DES ACTEURS CYBER

TOP 3 – MÉTIERS CYBER

- **182** AUDIT, PLANNING ET CONSEIL
- **139** INTÉGRATION DE PROTECTIONS CYBER
- **107** INFOGÉRANCE ET EXPLOITATION

TOP 5 – DOMAINES D'APPLICATION

- **156** INFRASTRUCTURES NUMÉRIQUES
- **120** GOUVERNANCE CYBER
- **81** DONNÉES
- **75** RÉSEAUX
- **53** INFRASTRUCTURES ET SYSTÈMES INDUSTRIELS

LES PRINCIPALES EXPERTISES PAR GRAND DOMAINE D'ACTIVITÉ EN CYBERSÉCURITÉ

GOUVERNANCE CYBER

- **320** établissements dans L'AUDIT TECHNIQUE
- **312** établissements dans L'AUDIT ORGANISATIONNEL
- **307** établissements dans LA POLITIQUE DE SÉCURITÉ CYBER

PROTECTION CYBER

- **373** établissements dans LA PROTECTION DE LA DONNÉE
- **364** établissements dans LA PROTECTION DES INFRASTRUCTURES
- **308** établissements dans LA PROTECTION DES COMMUNICATIONS

DÉFENSE CYBER

- **216** établissements dans LES SERVICES DE SÉCURITÉ INFOGÉRÉS
- **177** établissements dans LE MAINTIEN EN CONDITIONS OPÉRATIONNELLES
- **161** établissements dans LA RÉPONSE À INCIDENT

RÉSILIENCE ET REMEDIATION

- **127** établissements dans LA GESTION DE CRISE
- **114** établissements dans LE PILOTAGE DE PCA ET DE PRA
- **95** établissements dans L'ANALYSE FORENSIQUE – INVESTIGATIONS POST-MORTEM

CONTEXTE ET ENJEUX DE LA CYBERSÉCURITÉ

UN CONTEXTE MARQUÉ PAR UNE FORTE HAUSSE DES CYBERATTAQUES DEPUIS 5 ANS

— En 2025, près de **4 entreprises sur 10** ont subi au moins une cyberattaque significative. Les modes d'attaques les plus courants restent le phishing, l'exploitation d'une faille de sécurité et l'attaque indirecte due à un tiers.

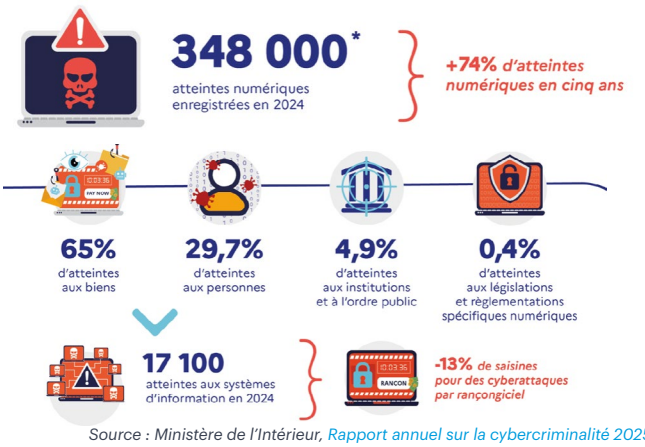
— Le Ministère de l'Intérieur comptabilisait en 2024, près de **348 000 atteintes numériques** avec une progression de **+74 % en cinq ans**. Près de **17 100** atteintes numériques ciblaient ainsi directement les **systèmes d'information**.

— Un manque de vigilance des **collaborateurs internes** au sein des entreprises apparait assez nettement comme le premier moyen d'entrée des cyberattaquants puisque ces acteurs internes représentent près de **57 %** des acteurs ciblés dans le cadre d'un incident de sécurité.

— **Un mauvais usage des outils numériques** (44,8 % des cyberattaques), **un piratage** (30,8 %), **des erreurs humaines** (6,3 %) **ou des logiciels malveillants** (5,2 %) apparaissent comme les principaux **modes opératoires des cyberattaquants**.

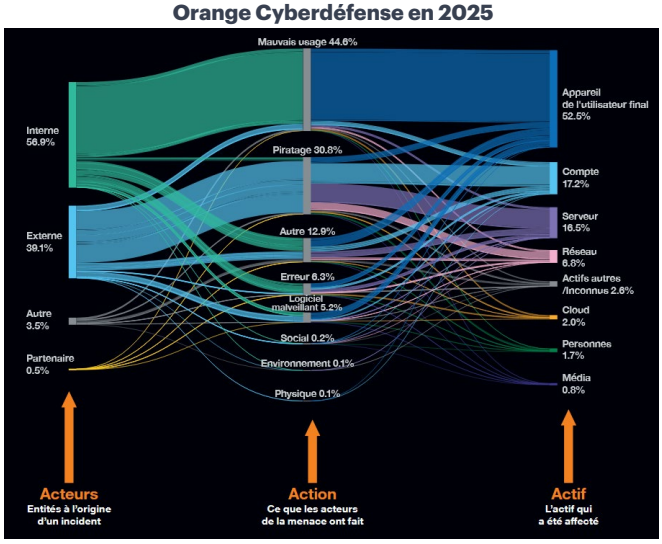
— Les **principaux actifs ciblés** pour rentrer au sein des systèmes d'information sont **l'appareil de l'utilisateur final** (58,5 %), **les comptes utilisateurs** (17,2 %), **les serveurs** (16,5 %), **les réseaux** (6,8 %), **le cloud** (2 %), **les personnes** (1,7 %) et **les médias** (0,8 %).

— **Les principaux impacts** d'une cyberattaque sur le business des entreprises en 2025 concernaient la **perturbation de la production pendant une période significative** (pour 28 % des entreprises touchées), **la perte d'image et l'impact médiatique** (26 % des entreprises), **la compromission d'informations / éléments de processus / savoir-faire de l'entreprise** (18 % des entreprises) et **la perte de chiffre d'affaires** (18 % des entreprises).



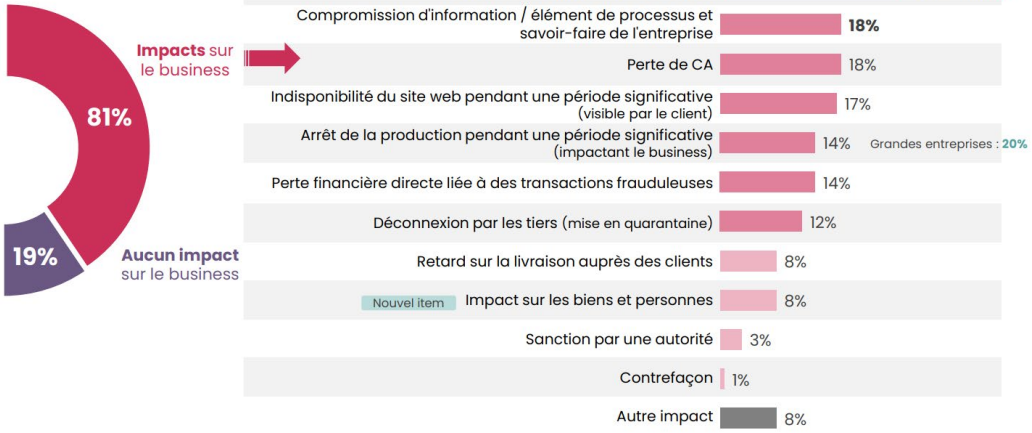
Source : Ministère de l'Intérieur, Rapport annuel sur la cybercriminalité 2025

Flux des principales catégories d'incident recensées par Orange Cyberdéfense en 2025



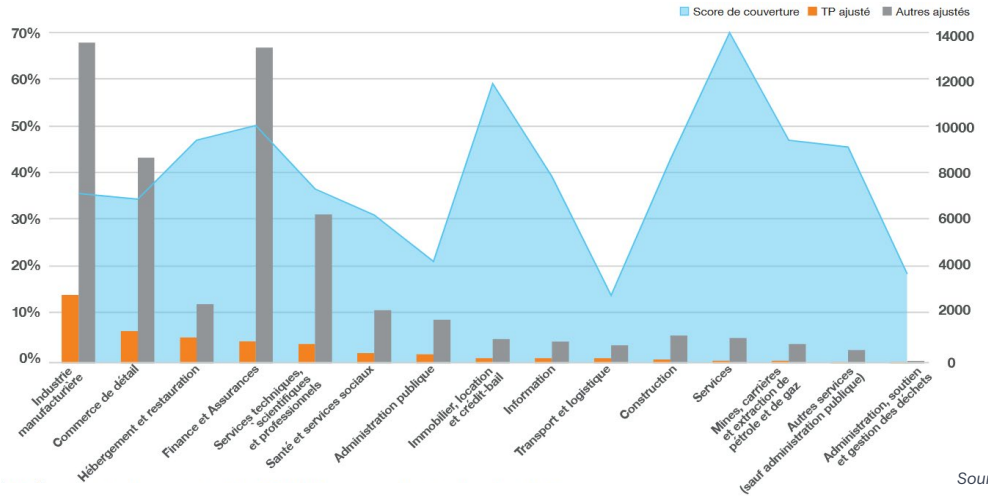
Source : Orange Cyberdéfense, Security Navigator 2026

Impacts des cyberattaques sur le business des entreprises en 2025



Source : CESIN – Opinion Way, Baromètre de la cybersécurité des entreprises – Rapport d'étude Vague 11, Janvier 2026

Incidents de sécurité enregistrés par Orange Cyberdéfense en 2025, normalisés à l'aide du score de couverture



Définition

Le score de couverture correspond à la couverture du secteur d'activité par Orange Cyberdéfense (proportion d'entreprises accompagnées sur volume total d'entreprises dans le secteur). Le nombre d'incidents ajusté (histogramme gris) permet de comparer les entreprises et les secteurs grâce à la prise en compte de leur degré de couverture relatif.

Source : Orange Cyberdéfense, Security Navigator 2026

— **L'industrie manufacturière** apparaît assez nettement comme le **secteur d'activité le plus touché** par les cyberattaques en 2025 avec près de **20 %** de l'ensemble des cyberattaques.

— **Le secteur industriel (1 228 victimes) et les services professionnels, scientifiques et techniques** (1 179 victimes) représentent ensemble près de **40 % de tous les cas observés**, ce qui indique des impacts durables sur l'outil productif et les industries fondées sur le savoir.

LA FILIÈRE DE LA CYBERSÉCURITÉ EN FRANCE

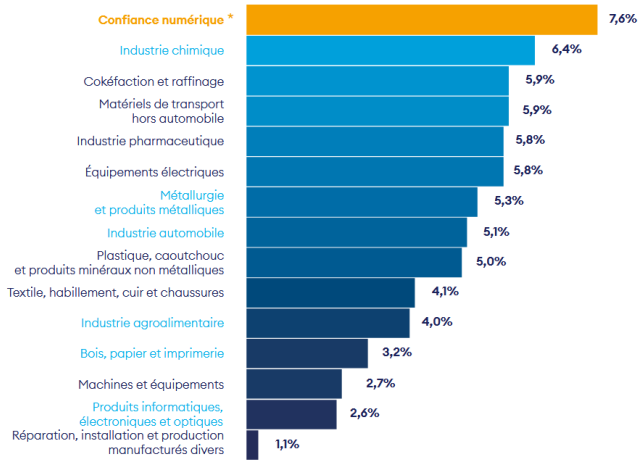
— En 2024, la filière de la confiance numérique (cybersécurité au sens large) générait en France un **chiffre d'affaires** cumulé de **21,3 Md€** et employait près de **107 000 personnes** sur le territoire.

— Dans le détail :

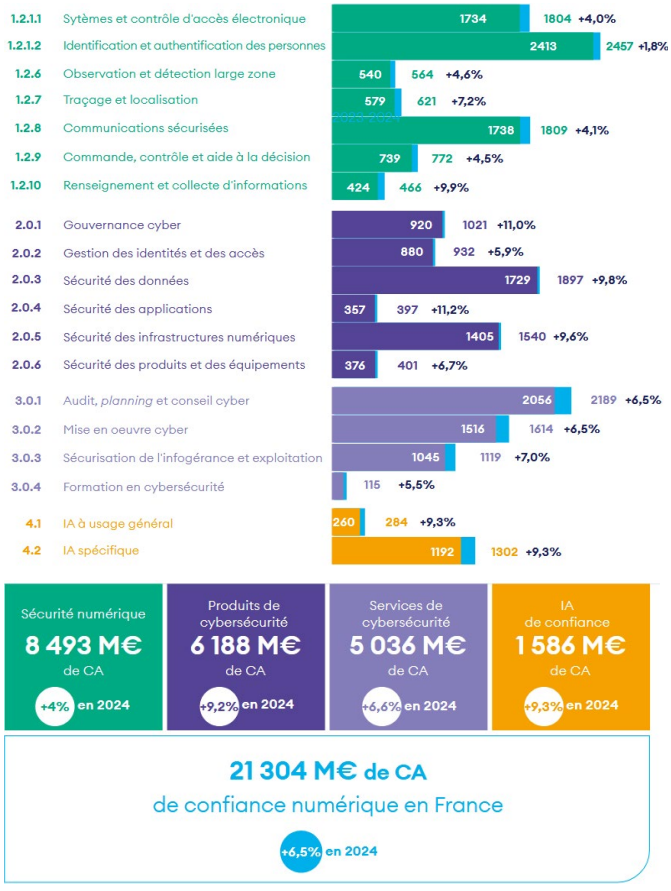
- **La sécurité physique** générait un CA de **8,5 Md€** et employait **36 200 personnes** ;
- **Les produits de cybersécurité** généraient un CA de **6,2 Md€** et employaient près de **29 300 personnes** ;
- **Les services de cybersécurité** généraient près de **5 Md€** de CA et employaient **24 600 personnes** ;
- **Les intelligences artificielles (IA)** de confiance généraient près de **1,6 Md€** et employaient près de **17 200 personnes**.

— La filière de la confiance numérique apparait par ailleurs comme la filière en plus forte croissance sur la période 2016-2023 avec une **croissance annuelle moyenne** de son chiffre d'affaires de **+7,6%**.

Croissance annuelle moyenne des filières françaises sur la période 2016-2023



Chiffre d'affaires du marché de la confiance numérique en France en 2024



21 304 M€ de CA
de confiance numérique en France
+6,5% en 2024

Source : Alliance pour la confiance Numérique, Observatoire de la Confiance Numérique 2025

LA STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ

— Pour l'Union européenne (UE), la cybersécurité recouvre "les activités nécessaires pour protéger les réseaux et les systèmes d'information ainsi que les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces " (règlement ENISA du 17 avril 2019).

— **La stratégie de cybersécurité de l'UE adoptée le 16 décembre 2020** couvre la sécurité des services essentiels (hôpitaux, réseaux énergétiques, chemins de fer, centres de données, ...) ainsi que celle des objets connectés. Elle vise à **renforcer la résilience de l'Europe face aux cybermenaces** et faire en sorte que tous les citoyens et toutes les entreprises bénéficient pleinement de services et d'outils numériques fiables et dignes de confiance.

— Face à l'augmentation massive des attaques cyber (+150 % en 2024), l'UE intensifie fortement ses actions pour renforcer la résilience numérique et de nouvelles législations et révisions règlementaires sont déployées.

— En parallèle, la Commission européenne met en place depuis 2025 **une politique de simplification réglementaire** avec un objectif de **réduire de 25 % les charges administratives pour les entreprises et de 35 % pour les PME** afin de favoriser la compétitivité de l'Europe. Le numérique et la cybersécurité ne font pas figure d'exception.

LE CADRE LÉGISLATIF ET RÉGLEMENTAIRE EUROPÉEN : NIS 2, CSA ET CRA

Commission européenne

La directive NIS 2

— **La directive NIS 2** ou **SRI 2** (acronyme français) s'appuie sur les acquis de la directive NIS 1 et entend remédier à ses lacunes. Elle traite des mesures à mettre en place afin **d'assurer un niveau élevé de sécurisation des systèmes de réseaux et d'information** au sein de UE, en précisant les obligations incombant aux opérateurs en matière de sécurité informatique dans un certain nombre de secteurs. Elle prévoit ainsi un renforcement des obligations des entreprises et l'introduction de mesures de surveillance plus strictes pour les autorités nationales.

— **La directive NIS 2 élargit le champ d'action et la portée de NIS 1** pour apporter davantage de protection :

- **10 secteurs sont considérés comme hautement critiques** : énergie, transport, secteur bancaire, infrastructures des marchés financiers, santé, eau potable et eaux usées, infrastructures numériques, gestion des services TIC, administrations publiques et espace.
- **8 autres secteurs sont considérés comme critiques** : services postaux et d'expédition, gestion des déchets, produits chimiques, denrées alimentaires, fabrication, fournisseurs numériques et recherche.
- **NIS 2 touche par ailleurs un plus grand nombre d'organisations.** D'une part, **les entités essentielles** sont celles qui opèrent dans un secteur hautement critique et répondent à au moins un des critères suivants : 250 salariés ou plus, chiffre d'affaires annuel supérieur à 50 M€, ou bilan annuel dépassant 43 M€. D'autre part, **les entités importantes** sont susceptibles **d'être concernées par NIS 2 si elles remplissent simultanément trois critères** : employer entre 50 et 249 salariés, réaliser un chiffre d'affaires compris entre 10 et 50 M€, ou avoir un bilan annuel compris entre 10 et 43 M€. Elles peuvent relever d'un des 18 secteurs couverts par la directive.

— **La transposition** par le Parlement français de ce texte a subi du retard et est **attendue en 2026**. Néanmoins les entreprises sont invitées à anticiper leur mise en conformité. Au total **15 000 entités françaises sont susceptibles d'être concernées** contre 500 sous NIS 1.

Le règlement européen sur la cybersécurité (Cyber Security Act - CSA)

— **Le règlement CSA** adopté en 2019 vise **à harmoniser le processus de validation des schémas de certification** (EUCC / ECCF en français) pour les produits, services et processus TIC (Technologies de l'information et de la communication) et renforce le rôle moteur de l'ENISA (agence de l'UE pour la cybersécurité) dans la conception de ces schémas. Le CSA définit également différents niveaux d'assurance d'un schéma de certification.

— **Le CSA2** présenté par la Commission le 20 janvier 2026 vise à **renforcer la sécurité des chaînes d'approvisionnement de l'UE en TIC**. Il propose une mise à jour et une extension des cadres de certification de cybersécurité de l'UE afin de pouvoir fournir aux consommateurs des produits sûrs dès leur conception. Les systèmes de certification deviendront **un outil pratique et volontaire pour les entreprises**. Ils leur permettront de démontrer qu'elles respectent la législation de l'UE, ce qui réduira la charge et les coûts. Cela va dans le sens de la simplification qui vient en complément du **guichet unique pour le signalement des incidents de cybersécurité** proposé par la Commission le 19 novembre 2025 dans le cadre du paquet législatif sur la simplification des normes numériques (« Omnibus » numérique).

Le règlement européen sur la cyber-résilience (Cyber Resilience Act - CRA)

— Il établit **des normes communes en matière de cybersécurité pour les produits comportant des éléments numériques**, dans l'intérêt des consommateurs et des entreprises dans l'ensemble de l'UE.

— Ces produits devront satisfaire à des exigences spécifiques en matière de cybersécurité tout au long de leur cycle de vie, y compris pour les mises à jour automatiques de sécurité et les rapports d'incidents. Cela implique donc des obligations contraignantes pour les fabricants de matériels et de logiciels. (Législation sur la cyberrésilience - Mise en œuvre).

Informations recueillies auprès de la Délégation de la Région Auvergne-Rhône-Alpes à Bruxelles

LES APPELS À PROJETS EUROPÉENS

— Le soutien européen à la cybersécurité transite essentiellement par **2 programmes** sur la période 2021-2027 : **Horizon Europe (programme-cadre de recherche et d'innovation) et Digital Europe (Europe numérique)**.

- **Horizon Europe** : **cluster 3 « sécurité civile pour la société »**, destination 4 : « cybersécurité accrue ». Le **programme de travail 2026-2027** prévoit plusieurs appels en 2026 et 2027. Tous les appels en cours peuvent être retrouvés sur **le site Horizon Europe** du Ministère de l'Enseignement Supérieur, de la Recherche et de l'Espace. Exemples de projets financés : consulter ce lien.
- **Digital Europe** : plusieurs appels (en cours et à venir) intègrent une dimension cybersécurité par exemple sur des secteurs spécifiques et/ou par voie de cascad funding (financement en cascade). Retrouver les appels via ce lien (en introduisant dans le moteur de recherche « cybersecurity »), et le Programme de travail 2025-2027. Exemples de projets récents financés par Digital Europe avec des acteurs du territoire :
  - ThreatChase – Plateforme ouverte pour la protection contre le phishing, projet coordonné par la société KOR LABS (Seyssins, Isère) ;
  - SOC4Health – Fourniture de centres d'opérations de sécurité pour les établissements de santé publics projet coordonné par les Hospices Civils de Lyon.

Source : Délégation de la Région Auvergne-Rhône-Alpes à Bruxelles

LA STRATÉGIE NATIONALE DE CYBERSÉCURITÉ 2026-2030

— Commandée par le Président de la République, la **Stratégie nationale de cybersécurité 2026-2030** prolonge les ambitions de la Revue nationale stratégique et fixe la trajectoire de la France pour devenir une Nation cyber de premier rang. Élaborée sous l'égide du Secrétariat général de la défense et de la sécurité nationale (SGDSN), elle a été construite avec l'ensemble des ministères, ainsi qu'un panel d'experts représentatif du monde industriel, scientifique et académique.

- Pilier n°1 : faire de la France le plus grand vivier de talents cyber d'Europe
- Pilier n°2 : renforcer la résilience cyber de la Nation
- Pilier n°3 : entraver l'expansion de la cybermenace
- Pilier n°4 : garder la maîtrise de la sécurité de nos fondements numériques
- Pilier n°5 : soutenir la sécurité et la stabilité du cyberespace en Europe et à l'international

Source : SGDSN, Secrétariat général de la défense et de la sécurité nationale, Stratégie nationale de cybersécurité 2026-2030

LA STRATÉGIE RÉGIONALE DE CYBERSÉCURITÉ

— Consciente des enjeux de cybersécurité, la **Région Auvergne-Rhône-Alpes** a souhaité se doter d'**une stratégie régionale de cybersécurité** afin de contribuer à un environnement économique résilient et à un environnement numérique de confiance. Son élaboration a impliqué, dans une étude préparatoire menée en 2024, les principaux réseaux de l'écosystème. Cette étude a permis de formuler des propositions d'actions qui ont été reprises dans le document stratégique.

— **Le 27 mars 2025**, l'Assemblée Plénière de la Région Auvergne-Rhône-Alpes a adopté une **feuille de route cybersécurité**, dans le cadre de ses compétences de développement économique et de son ambition au service de la sécurité.

— 4 axes structurent cette feuille de route :

- **Protéger les entreprises et renforcer leur appréhension des risques cyber** afin de mieux y faire face. La Région souhaite apporter un soutien à des actions de sensibilisation au risque cyber et à l'accompagnement des entreprises, en s'appuyant notamment sur des dispositifs en place permettant d'adresser le sujet de la cybersécurité.
- **Animer et développer la filière cybersécurité régionale**, en mettant en visibilité les offreurs de solution régionaux et en favorisant la recherche et l'innovation. En s'appuyant notamment sur le cluster, l'ambition régionale est de favoriser le développement d'une offre de solutions cyber régionale.
- **Développer les compétences disponibles sur le territoire en matière de cybersécurité** en valorisant les métiers et en soutenant les structures de formation. Ces deux volets visent ainsi à rendre attractif la filière auprès des jeunes comme des publics en reconversion et à appuyer le développement de la formation de spécialistes de tous niveaux en cybersécurité, au profit des prestataires cyber comme des entreprises.
- **Mettre en place une gouvernance régionale adaptée de la thématique et faire du Campus Région du numérique un lieu totem de la cybersécurité**. Il accueille d'ores et déjà en son sein des entreprises, une fondation, des écoles, ainsi que des réseaux économiques et des consortia industriels impliqués dans la cybersécurité, sur les volets sensibilisation, formation, ou accompagnement des entreprises. Pour incarner ce lieu central, de nouveaux espaces dédiés à la formation et à la sensibilisation ont été mis en place.

— Désormais doté d'un cadre, le travail collaboratif et fructueux entre les acteurs régionaux va pouvoir s'épanouir au service d'une cybersécurité mieux prise en compte côté entreprises et porteuse de valeur côté filière du numérique.

Source : Région Auvergne-Rhône-Alpes

LA FILIÈRE CYBERSÉCURITÉ EN AUVERGNE-RHÔNE-ALPES

50 % DES ÉTABLISSEMENTS CONCENTRÉS DANS LE RHÔNE

— La filière des acteurs de la cybersécurité en Auvergne-Rhône-Alpes rassemble **583 établissements** soit **469 entreprises**. Parmi elles, **135 entreprises** sont véritablement **spécialisées en cybersécurité** ou peuvent même être caractérisées comme des « ***pure players*** » (29 % des acteurs).

— La majorité des entreprises régionales de la filière sont des **TPE** (**33 %**) et **PME** (**32 %**). Cependant, la filière régionale compte une forte proportion d'**ETI** (**21%**) et de **Grands Groupes** (**14 %**).

— Par ailleurs, le tissu économique régional de la cybersécurité se distingue par une présence importante de nouveaux acteurs : **21 % des sociétés ont été créées dans les 5 dernières** années et **48 % dans les 15 dernières années**.

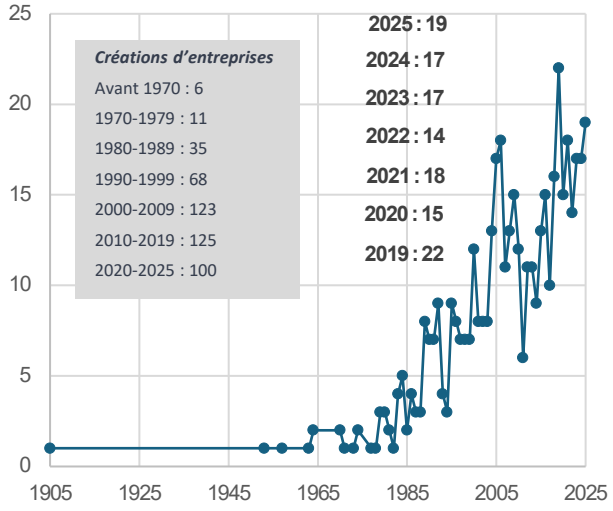
— Plus de **90 %** des établissements se concentrent dans six départements :
- **53 %** sont situés dans le **Rhône**
- **16 %** en **Isère**
- **7 %** dans le **Puy-de-Dôme**
- **6 %** dans la **Loire**
- **5 %** en **Haute-Savoie**
- **5 %** dans la **Drôme**

— Près de **87 %** des entreprises régionales de la cybersécurité relèvent de **capitaux français** (407 entreprises), tandis que **61 entreprises sont à capitaux étrangers**. La majorité des investisseurs étrangers sont **originaires des Etats-Unis** avec **19 groupes américains** de la cybersécurité implantés en Auvergne-Rhône-Alpes (31% des entreprises à capitaux étrangers). On retrouve également de **nombreux groupes européens** (51 %) avec des investisseurs en provenance du **Royaume-Uni** (7 entreprises), du **Luxembourg** (7 entreprises) ou des **Pays-Bas** (4 entreprises).

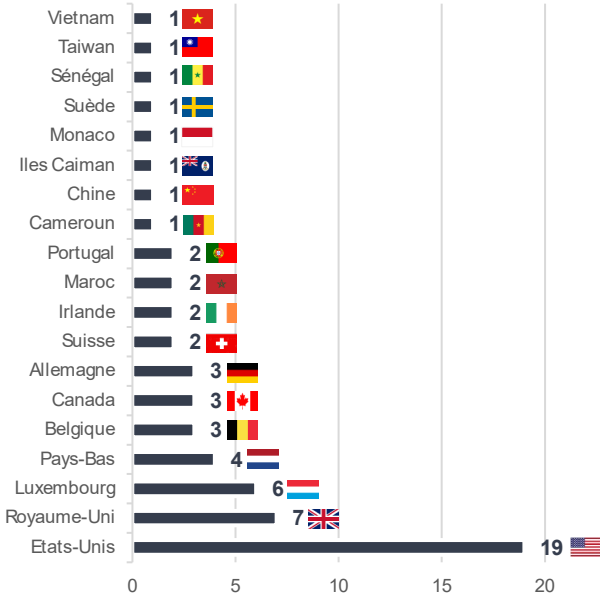
469 ENTREPRISES SOIT **583** ÉTABLISSEMENTS

65 %	21 %	14 %
TPE/PME	ETI	GRANDS GROUPES

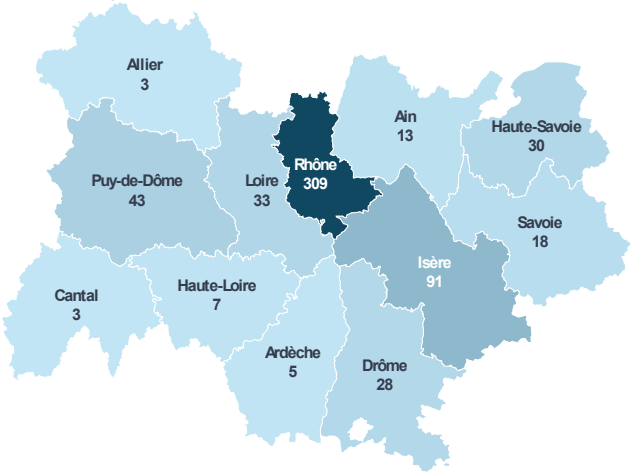
Date de création des entreprises de la filière cybersécurité en Auvergne-Rhône-Alpes



Répartition des entreprises détenues par des capitaux étrangers par pays d'origine de la tête de groupe



Implantation géographique des acteurs de la cybersécurité en Auvergne-Rhône-Alpes (en nombre d'établissements)



Source : Recensement Auvergne-Rhône-Alpes Entreprises
Carte générée avec Bing, ©GeoNames, TomTom

135 *PURE PLAYERS* DE LA CYBERSÉCURITÉ AVEC UNE FORTE CONCENTRATION SUR L'AGGLOMÉRATION LYONNAISE

— Les **135** « ***pure players*** » régionaux de la filière cybersécurité comptabilisaient **1 240 emplois fin 2024** (soit une moyenne de 9 salariés par entreprise) et ont généré un **chiffre d'affaires** de **287 M€** en 2024.

— Ce tissu d'entreprises se distingue de l'ensemble des acteurs de la filière par une proportion plus élevée de **TPE** (**64 %**) avec une part plus faible d'**ETI** (**4 %**) ou de **Grands Groupes** (**3 %**).

— Ces entreprises spécialisées en cybersécurité sont principalement implantées dans le **Rhône** avec **95 acteurs** soit près de **70 %** des pure players.

— Les territoires de l'**Isère** (**13 acteurs** soit 10 %), de la **Loire** (**11 acteurs**, 8 %), du **Puy-de-Dôme** (**7 acteurs**, 5 %) et de la **Drôme** (**6 acteurs**, 4 %) sont aussi bien représentés sur cette typologie d'acteurs.

— Le Rhône (principalement la métropole lyonnaise) concentre près de **85 % des emplois des *pure players*** régionaux notamment en raison de l'activité importante d'Orange Cyberdéfense, de Stormshield, de Squad, de Tenacy ou d'Algosecure.

— Les autres grands territoires de la filière cybersécurité en volume d'emplois sont :
- la **Loire** avec **5 %** des effectifs régionaux (62 emplois au sein de 11 pure players),
- l'**Isère** avec **5 %** des effectifs (57 emplois au sein de 13 pure players),
- le **Puy-de-Dôme** avec **2 %** des effectifs (22 emplois au sein de 7 pure players).

— La filière cybersécurité en Auvergne-Rhône-Alpes est à la fois constituée de **grands acteurs** concentrant une large partie des effectifs régionaux, ainsi que des **PME** très innovantes sur des expertises de pointe telles que **Tenacy** (Rhône), **Algosecure** (Rhône), **KNS** (Rhône), **ID3 Technologies** (Isère), **Chambersign** (Rhône), **Aphelio** (Isère), **Excube** (Rhône), **Artecys** (Loire), **Vaadata** (Rhône), **Recoveo** (Loire), **Root-Me Pro** (Rhône), **Serenicity** (Loire), **SYLink Technologie** (Puy-de-Dôme)...

135
ENTREPRISES
Pure players

Dont

106
AVEC UN SIÈGE SOCIAL EN REGION

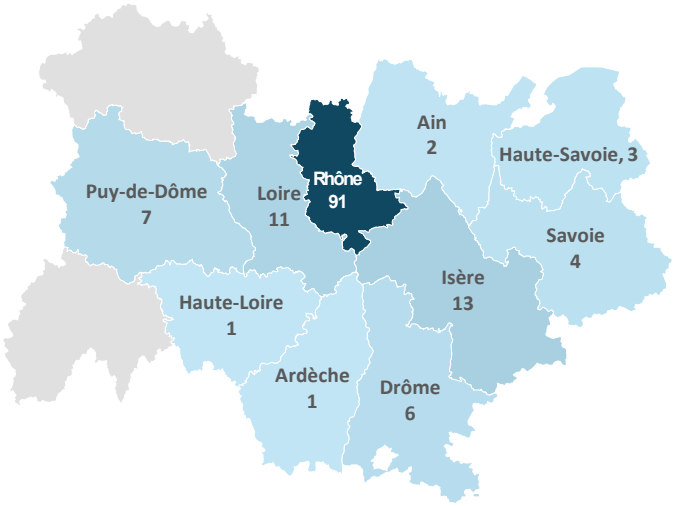
92 %
TPE-PME

1 240
EMPLOIS

287 M€
CHIFFRE D'AFFAIRES *

** 85 entreprises sur 135 pure players recensés en région ont été prises en compte dans le calcul des chiffres d'affaires car 50 entreprises n'ont pas communiqué leurs CA auprès de la DGFIP. Il s'agit pour la plupart d'unités non-employeuses.*

Implantation en Auvergne-Rhône-Alpes des 135 *pure players* régionaux



Effectifs salariés privés des 135 *pure players* de la filière Cybersécurité en Auvergne-Rhône-Alpes

Données DGFIP 2025
Carte générée avec Bing, ©GeoNames, TomTom

Principaux *pure players* de la filière Cybersécurité implantés en Auvergne-Rhône-Alpes

Source : Recensement Auvergne-Rhône-Alpes Entreprises

DE NOMBREUSES ENTREPRISES CERTIFIÉES PASSI (ANSSI) ET LABELLISÉES EXPERTCYBER (CYBERMALVEILLANCE)

— **Les prestataires d'audit de la sécurité des systèmes d'information (PASSI)** évaluent de manière impartiale et objective qu'un système d'information satisfait aux critères d'audit sélectionnés par le commanditaire.

— Les prestataires d'audit de la sécurité des systèmes d'information sont qualifiés pour l'une ou plusieurs des activités suivantes :

- audit organisationnel et physique
- audit d'architecture
- audit de configuration
- audit de code source
- tests d'intrusion

30 entreprises implantées en Auvergne-Rhône-Alpes sont certifiées PASSI
Prestataires d'audit de la sécurité des systèmes d'information par l'ANSSI

Source : ANSSI, Catalogue des produits, services, profils de production et sites certifiés, qualifiés, agréés - Février 2026

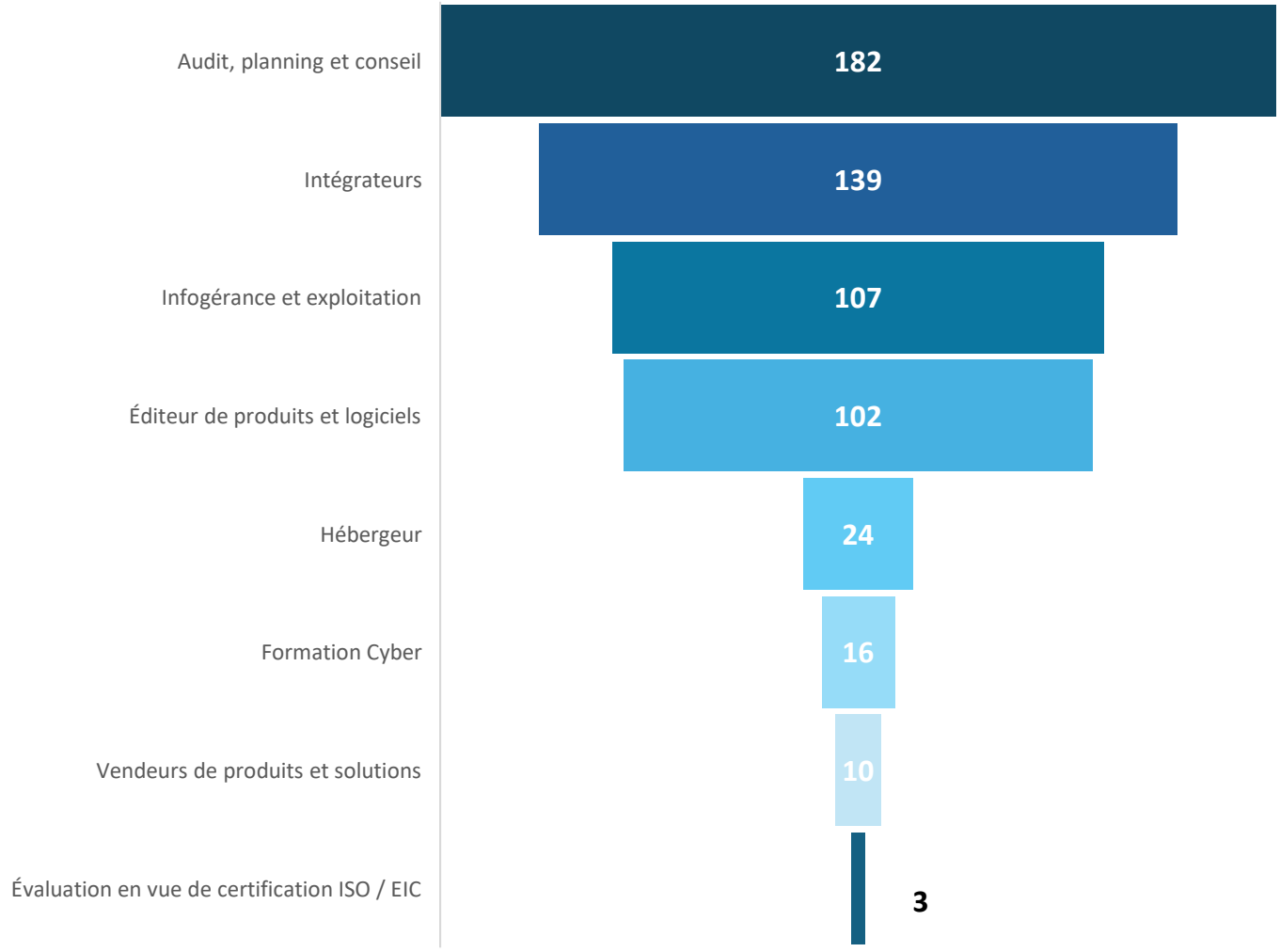
19 entreprises régionales sont labellisées « Expert Cyber » dans 8 départements de la région Auvergne-Rhône-Alpes par Cybermalveillance.gouv.fr au 10/02/2026
(Présentation détaillée du Label Expert Cyber p.33)

Source : Cybermalveillance.gouv.fr

DES COMPÉTENCES EN AUDIT/CONSEIL, EN INTÉGRATION DE SOLUTIONS CYBERSÉCURITÉ ET EN INFOGÉRANCE/ EXPLOITATION

- Les entreprises de la filière cybersécurité les plus représentées en Auvergne-Rhône-Alpes sont les acteurs de **l'audit, planning et conseil** avec **182 établissements** positionnés sur ce métier.
- Les acteurs spécialisés dans l'**intégration** de pare-feu, d'anti-virus, d'antispam, de solution de protection des mails, de gestion des accès et des identités représentent **139 établissements** en région.
- Les spécialistes de l'**infogérance** constituent également un vivier d'acteurs conséquent sur le territoire avec près de **107 établissements** spécialisés dans les services de sécurité infogérés, l'externalisation de RSSI et le maintien en condition opérationnelle.
- **102 éditeurs de produits et logiciels** appliqués à la cybersécurité sont présents en région.
- **Les hébergeurs de données sécurisés** sont au nombre de **24 établissements**, à noter que de nombreuses entreprises régionales sont certifiées HDS (Hébergeurs de données de Santé) et ISO 27001. Par ailleurs, 5 entreprises sont certifiées SecNumCloud par l'ANSSI.
- **16 acteurs de la formation continue et de la sensibilisation** en cybersécurité sont implantés sur le territoire. A savoir que de nombreuses entreprises sur le territoire proposent également des formations et des sensibilisations sans qu'elles aient toutefois été qualifiées en tant que spécialistes de la formation cyber.
- Enfin, **la commercialisation et la distribution de produits et logiciels** en cybersécurité concerne **20 établissements** tandis que l'on compte **3 établissements** spécialisés dans la **certification cyber**.

Principal métier Cyber des 583 établissements régionaux de la cybersécurité
(en nombre d'établissements)



Note méthodologique : chaque établissement du panel d'analyse régional (583 établissements) s'est vu attribué un positionnement métier parmi les 8 principaux métiers Cyber que nous avons établi avec l'ensemble des partenaires régionaux.

Source : Recensement Auvergne-Rhône-Alpes Entreprises

GOUVERNANCE CYBER DES COMPÉTENCES EN AUDIT TECHNIQUE ET ORGANISATIONNEL ET EN POLITIQUE DE SÉCURITÉ

— Les expertises les plus représentées dans le grand domaine d'intervention de la gouvernance cybersécurité sont les expertises d'**audit technique** et d'**audit organisationnel** avec respectivement **320** établissements et **312** établissements spécialisés avec notamment de nombreux cabinets de conseil et d'audit très spécialisés sur des audits complets.

— Les activités de mise en place de **politiques de sécurité cyber** avec en particulier la rédaction de PSSI sont aussi bien représentées avec **307** établissements.

— Avec **232** établissements et **199** établissements spécialisés, les compétences d'**analyse des risques** et d'**analyse de la surface d'attaque** sont aussi largement pris en charge par les acteurs régionaux de la filière.

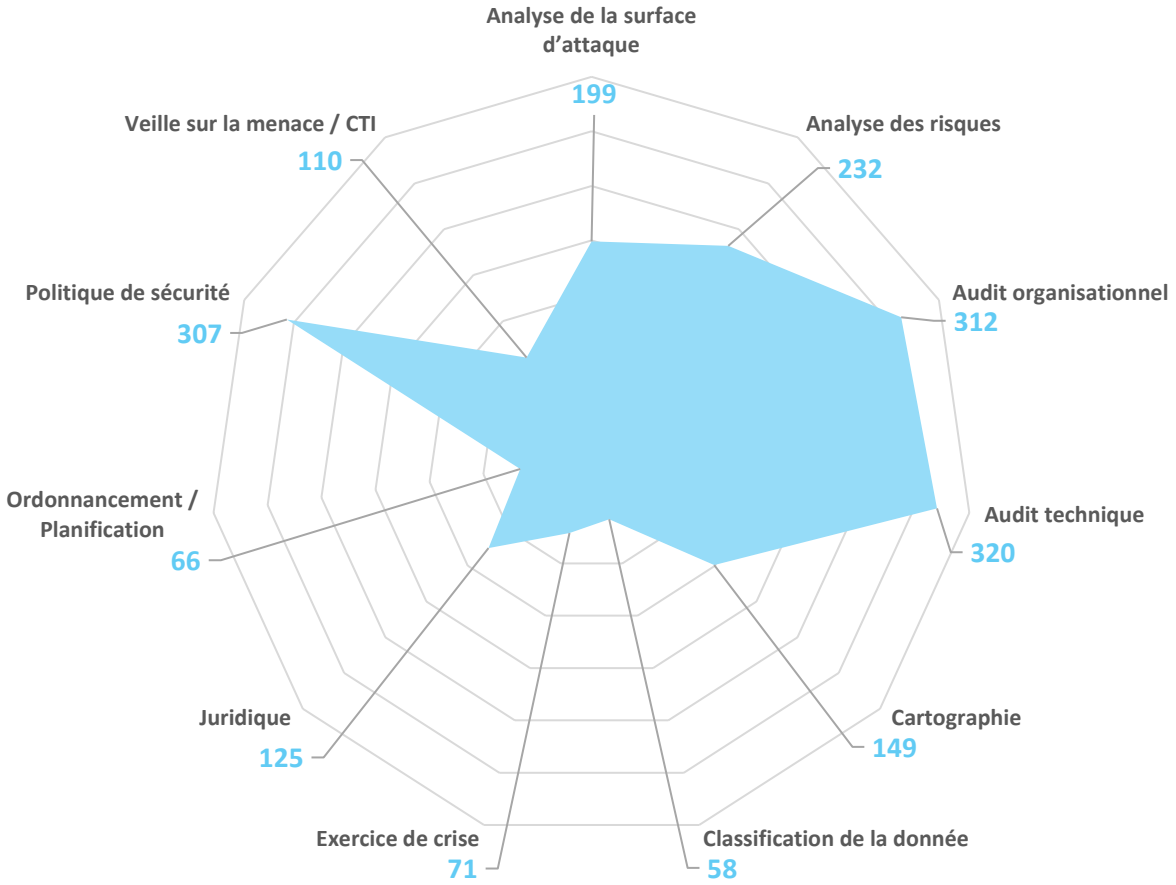
— **La cartographie du système d'informations (SI)** est une expertise de nombreux acteurs en Auvergne-Rhône-Alpes avec près de **149** établissements spécialisés.

— Les compétences **juridiques et de montée en compétences sur la conformité cyber** (NIS2, ISO 27001, HDS...) sont aussi bien représentées sur le territoire avec près de **125** établissements.

— La prise en charge de **la veille sur la menace/CTI** peut être gérée par près de **110** acteurs tandis que la **mise en place d'exercices de crise cyber** relève du domaine de compétences de **71** établissements.

— Enfin, les compétences d'**ordonnancement** et de **planification** sont assurées par **66** acteurs et celles de **classification de la donnée** par **58** acteurs.

Expertises en gouvernance cyber des 583 établissements régionaux de la cybersécurité en Auvergne-Rhône-Alpes
(en nombre d'établissements)



Source : Recensement Auvergne-Rhône-Alpes Entreprises - Cf. note méthodologique p. 4

PROTECTION CYBER DES COMPÉTENCES EN PROTECTION DE LA DONNÉE, DES INFRASTRUCTURES ET DES COMMUNICATIONS

— La **protection de la donnée** apparait comme la principale compétence relevant de la protection cyber maitrisée par les acteurs régionaux de la filière avec **373** établissements spécialisés soit près de **64 %** des acteurs du territoire. Cette forte représentation s'explique par la large diversité des expertises liées aux données : hébergement des données, protection des serveurs, déploiement de solutions cloud sécurisées, PSSI axé sur les thématiques de sécurisation des données...

— La **protection des infrastructures** est également une compétence centrale avec près de **364** établissements spécialisés soit près de **62 %** des acteurs du territoire. Cette compétence regroupe toutes les expertises liées à la protection du système d'information, des serveurs physiques, de l'ensemble des infrastructures numériques, le déploiement d'antispam, ou la mise en oeuvre d'antivirus.

— **308** établissements travaillent dans la **protection des communications** qui regroupe des expertises en protection des réseaux, des messageries professionnelles, le déploiement de solutions de communications sécurisées, d'antispam, d'antivirus, ou encore la mise en œuvre de campagnes de phising.

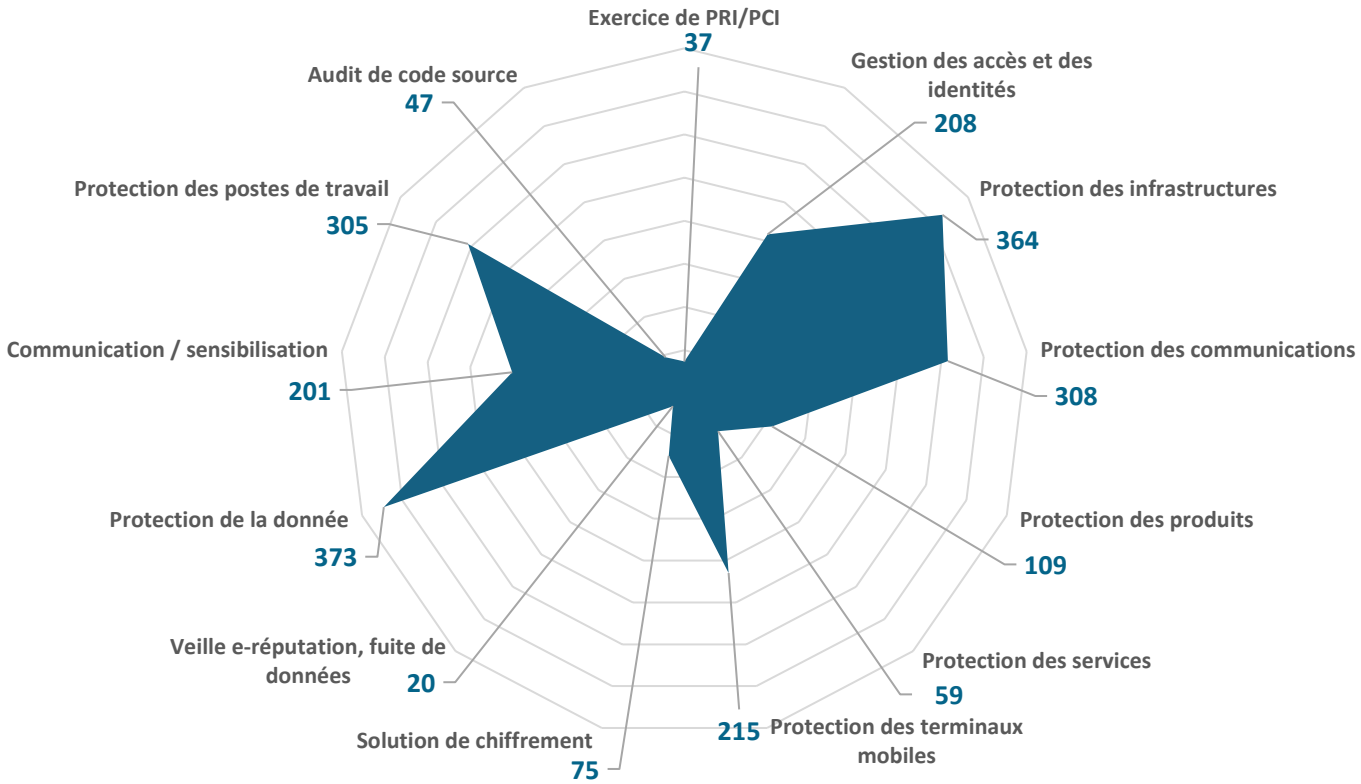
— La **protection des postes de travail** apparait comme la quatrième expertise majeure en protection cyber avec près de **305** établissements spécialisés dans le déploiement de solutions VPN ou de solutions d'authentification à deux facteurs...

— La **protection des terminaux mobiles et la gestion des accès et des identités** (mise en œuvre de solutions de sécurité physique, de contrôle des accès physiques et numériques) avec respectivement **215** établissements et **208** établissements apparaissent comme des expertises de premier plan dans le domaine de la protection cyber.

— Les compétences de **communication**, de **sensibilisation cyber** et de **formation continue** mobilisent **201** acteurs sur le territoire que ce soit via la mise en œuvre de formations classiques, de mises en situation réelles, ou d'initiations aux fondamentaux de la cybersécurité.

— Enfin, les compétences de déploiement de solutions de **protection des produits (IoT), de solutions de chiffrement/cryptographie**, et de **protection des services** sont aussi bien représentées avec respectivement **109**, **75** et **59** établissements spécialisés.

Expertises en protection cyber des 583 établissements régionaux de la cybersécurité en Auvergne-Rhône-Alpes
(en nombre d'établissements)



Source : Recensement Auvergne-Rhône-Alpes Entreprises Cf. note méthodologique p. 4

DÉFENSE CYBER DES COMPÉTENCES EN SERVICES DE SÉCURITÉ INFOGÉRÉS, MAINTIEN EN CONDITIONS OPÉRATIONNELLES, RÉPONSE À INCIDENT ET PENTEST

— L'externalisation des compétences cyber, incluant la gestion de **services de sécurité infogérés**, est la principale compétence en défense cyber maîtrisée par les acteurs régionaux (**216** établissements). Cette forte représentation s'explique par la volonté de nombreuses entreprises d'externaliser les fonctions de RSSI et de DPO.

— Le **maintien en conditions opérationnelles (MCO)** est une compétence centrale pour les acteurs de la défense cyber (**177** établissements). Elle couvre les expertises nécessaires pour garantir la disponibilité constante des applications, infrastructures et matériels.

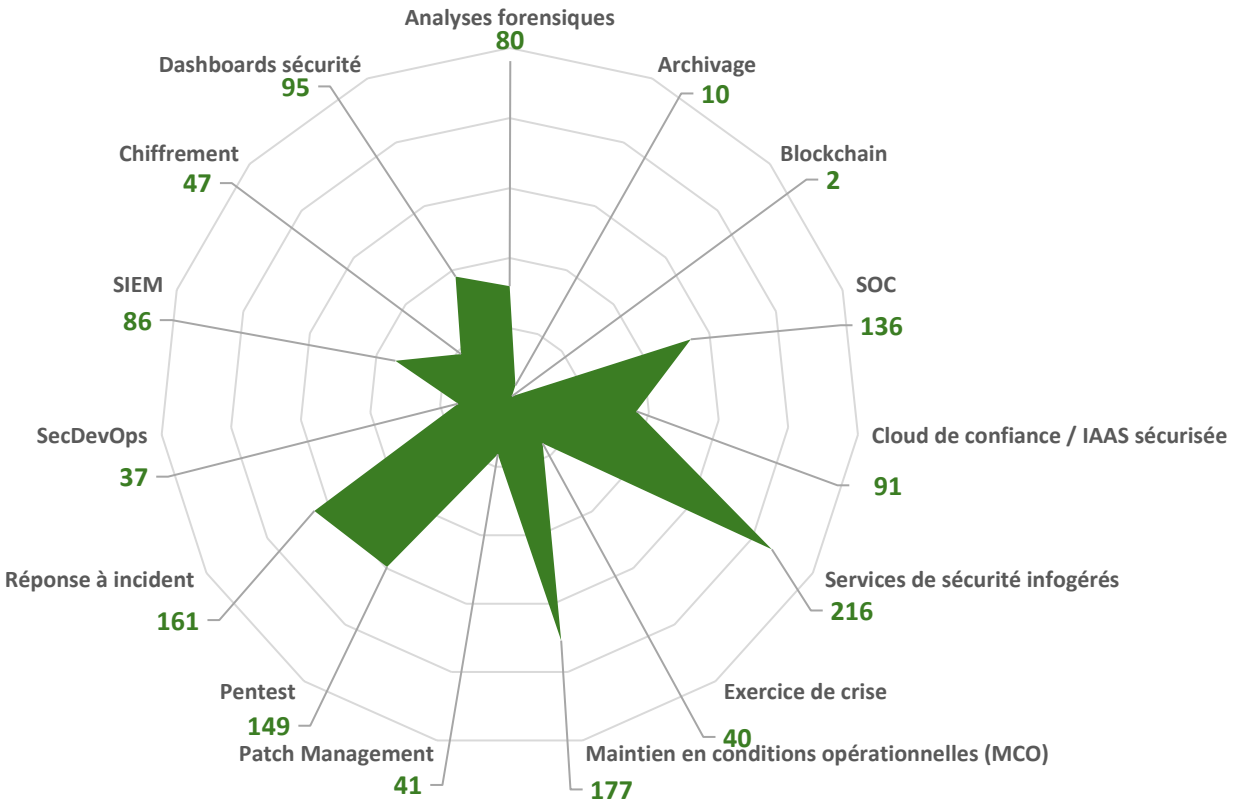
— Avec **161** établissements spécialisés, la **réponse à incident** est une compétence majeure en défense cyber. Elle englobe les actions coordonnées d'identification, d'analyse et de cantonnement d'un incident, puis le rétablissement des systèmes pour limiter les dommages et réparer les vulnérabilités violées.

— La réalisation de campagnes de **pentest** ou de « **tests d'intrusion** » est une expertise clé proposée par les acteurs cyber régionaux (**149** établissements). Ces tests simulent une attaque réelle pour identifier des failles et apporter les correctifs nécessaires.

— Les compétences de **SOC** (« Security Operation Center » ou **Centre des Opérations de sécurité**) permettent la mise en surveillance en temps réel des incidents de sécurité. **136** établissements sont en capacité de proposer ces solutions. Par ailleurs, 86 acteurs sont spécialisés en SIEM (« gestion des informations et des événements de sécurité »).

— Le déploiement et la mise en œuvre de **solutions cloud sécurisées** mobilisent 91 acteurs. Enfin, la génération de **dashboards de sécurité** et les **analyses forensiques post-cyberattaque** sont largement prises en charge (95 et 80 établissements respectivement).

Expertises en défense cyber des 583 établissements régionaux de la cybersécurité en Auvergne-Rhône-Alpes
(en nombre d'établissements)



Source : Recensement Auvergne-Rhône-Alpes Entreprises Cf. note méthodologique p. 4

RÉSILIENCE ET REMÉDIATION CYBER DES COMPÉTENCES EN RÉPONSE À INDICENT (POST-ATTAQUE), EN GESTION DE CRISE ET EN MISE EN ŒUVRE DE PRA/PCA

— La prise en charge de **réponse à incident (post-attaque)** concerne près de **130** établissements sur le territoire.

— **127 établissements** revendiquent des expertises de **gestion de crise**. L'objectif d'une préparation à la gestion de crise est de permettre à toute l'organisation de réagir rapidement et efficacement afin de limiter les impacts négatifs sur l'image de marque, la sécurité des données informatiques et le chiffre d'affaires.

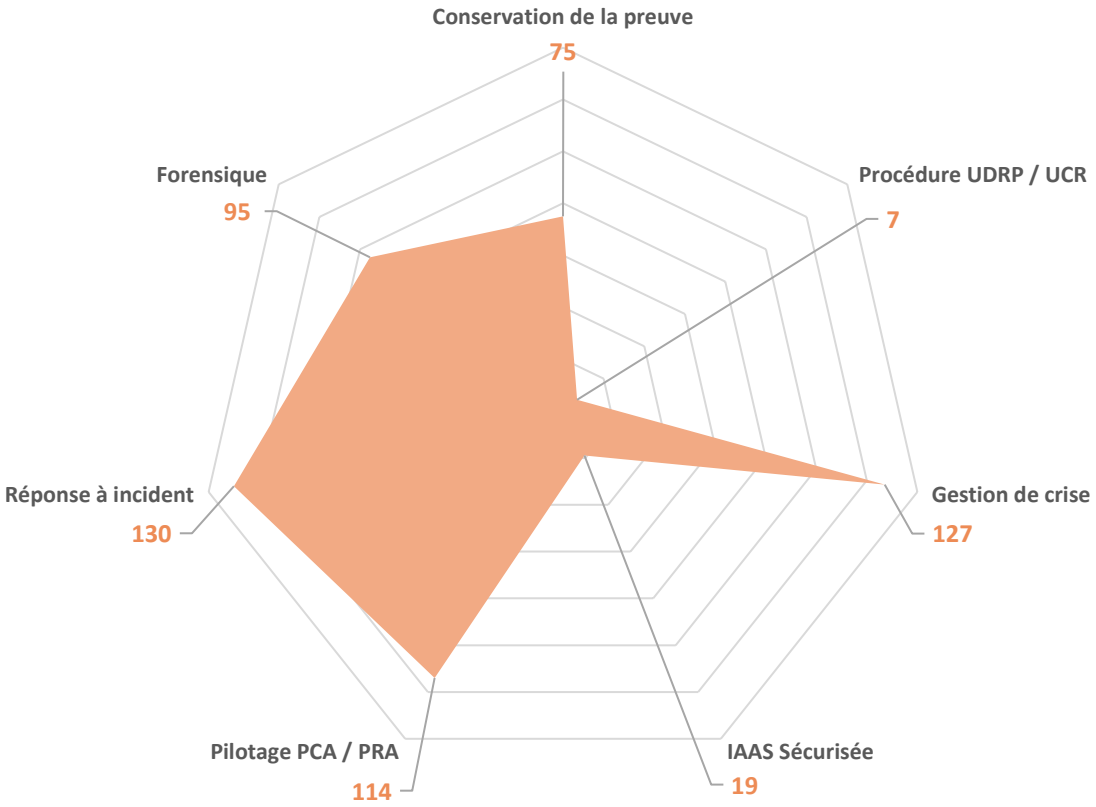
— Le **pilotage** et la **mise en œuvre de PRA (Plan de Reprise d'Activité)** et de **PCA (Plan de Continuité d'Activité)** sont des expertises majeures pour les acteurs de la résilience et de la remédiation cyber régionaux puisqu'elles concernent près de **114** acteurs. Le PRA permet la relance du fonctionnement de l'entreprise après un sinistre. Dans le cadre de la sécurité informatique, ce sinistre consiste en général en une brèche de cybersécurité : perte, vol ou disparition de données sensibles, virus, cyberattaque, cybercrime. Un PCA vise à garantir la survie de l'organisation en cas de panne informatique majeure, de défaillance ou de cyberattaque de son système d'information.

— Avec **95 établissements** spécialisés, les compétences de **forensique** (ou **d'analyses post-mortem**) sont bien couvertes en région. Il s'agit d'une méthode d'investigation numérique qui permet d'enquêter sur les incidents de cybersécurité. À la manière d'une enquête policière sur une scène de crime, l'expert forensique collecte et analyse les preuves numériques pour comprendre le déroulement d'une cyberattaque. Cette approche scientifique et méthodique vise deux objectifs principaux : identifier l'origine et l'étendue d'une intrusion déjà survenue, mais aussi détecter de manière proactive les menaces potentielles avant qu'elles ne causent des dommages.

— Les compétences de **conservation de la preuve** mobilisent près de **75** acteurs en région. Cela consiste à enregistrer certaines des actions effectuées sur les systèmes informatiques afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles ou de déterminer l'origine d'un incident.

— Enfin, les compétences de déploiement d'**IAAS** (Infrastructure as a Service) **sécurisé** et de mise en œuvre de **procédures UDRP et UCR** concernent respectivement **19** établissements et 7 établissements spécialisés.

Expertises en résilience et remédiation cyber des 583 établissements régionaux de la cybersécurité en Auvergne-Rhône-Alpes
(en nombre d'établissements)



Source : Recensement Auvergne-Rhône-Alpes Entreprises Cf. note méthodologique p. 4

DES EXPERTISES CYBER APPLIQUÉES DANS LES INFRASTRUCTURES NUMÉRIQUES, LA GOUVERNANCE CYBER, LES DONNÉES, LES RÉSEAUX ET LES SYSTÈMES INDUSTRIELS

— La troisième clé de lecture et d'analyse des établissements de la filière cybersécurité en Auvergne-Rhône-Alpes renvoie au domaine d'application principal des acteurs de la filière. Cela correspond à la spécialisation principale de l'entreprise sur un domaine d'application cyber spécifique.

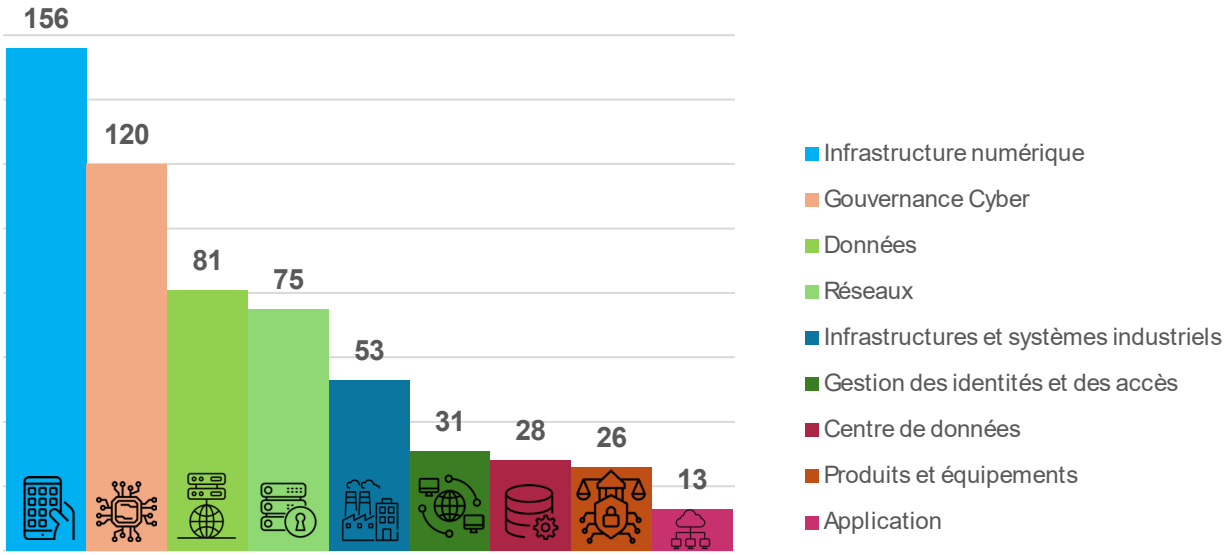
— Le principal domaine d'application est l'**infrastructure numérique** avec **156** établissements, soit près de **27 %** des acteurs régionaux. Cette forte représentation s'explique par une diversité importante des applications avec par exemple les postes de travail, les systèmes d'informations...

— La **gouvernance cyber** apparait comme le second domaine d'application en région avec près de **120** acteurs (**21 %**). Ce domaine d'application renvoie à l'ensemble des compétences de politiques de sécurité cyber, d'accompagnement des dirigeants, des collaborateurs et des RSSI.

— Avec **81** établissements (**14 %**), **les données** apparaissent comme le troisième domaine d'application des acteurs de la cybersécurité en région. Il renvoie à la mise en œuvre de solutions d'hébergement des données sécurisées, de déploiement de solutions cloud, de mise en place de plans de sauvegarde, de politique de conservation et de protection des données.

— La **sécurisation des réseaux** concerne **75** établissements (**13 %**). Ce domaine d'application renvoie au déploiement de pare-feu (firewall), de VPN et des solutions de sécurisation des réseaux.

Principaux domaines d'application maitrisées par les acteurs de la cybersécurité en Auvergne-Rhône-Alpes
(en nombre d'établissements)



— **La sécurisation des infrastructures et systèmes industriel**s concerne près de **53** acteurs soit près de **9 %** des acteurs régionaux. Ce domaine d'application stratégique renvoie à la sécurisation des moyens de production industriels, des machines, des automatismes, des réseaux industriels ou des robots.

— **La gestion des identités et des accès** est représentée par **31** acteurs auvergnats-rhônalpins (**5 %**). Ce domaine renvoie à la sécurisation physique des entreprises, aux solutions d'identification numérique, à la mise en œuvre de politiques de gestion des accès...

— Avec **28** établissements (**5 %**), les **centres de données** ou spécialistes de l'hébergement sécurisé, sont bien représentés sur le territoire régional.

— **La protection cyber des produits et des équipements** avec **26** acteurs (**4 %**) est une vraie spécialisation régionale en lien avec la puissante filière électronique et microélectronique implantée sur le territoire notamment sur le bassin grenoblois.

— Enfin, **la sécurisation des applications mobiles** avec **13** acteurs (**2 %**) est un domaine d'application plus en retrait sur le territoire.

Note méthodologique : Chaque établissement du panel d'analyse régional (583 établissements) s'est vu attribué un domaine d'application parmi les 9 principaux domaines d'application cyber que nous avons établi avec l'ensemble des partenaires régionaux.

Source : Recensement Auvergne-Rhône-Alpes Entreprises

LES ACTEURS DE LA FORMATION

44 FORMATIONS DE NIVEAU BAC PRO ET BTS EN CYBERSÉCURITÉ EN AUVERGNE-RHÔNE-ALPES

Localisation	Diplôme	Spécialités	Etablissements
01 : Ambérieux en Bugey, Belley, Bourg-en-Bresse, Bellignat *03 : Montluçon* *07 : Annonay, Tournon-sur-Rhône* *15 : Aurillac* *26 : Crest, Pierrelatte, Valence* *38 : Nivolas-Vermelle, Échirolles, Grenoble *2, Pont-de-Chéruy, Vizille* *42 : Andrézieux Bouthéon, Roanne *2, Saint-Etienne* *43 : Brives-Charensac* *63 : Clermont-Ferrand* *69 : Lyon 1, Lyon 3, Lyon 5, Lyon 8 (*2), Rillieux la Pape, Décines Charpieu, Villefranche sur Saône, Bron, Oullins, Givors, Vénissieux *2* *73 : La Motte-Servolex, Saint-Jean-de- Maurienne, Ugine, Chambéry* *74 : Chavanod, Collonges sous Salève, Argonay*	**Bac Pro CIEL : Cybersécurité, informatique et réseaux, électronique**	• Etude et conception de produits électroniques, de systèmes électroniques communicants • Production et assemblage d'ensembles électroniques • Intégration matérielle et logicielle • Exploitation et maintien en condition opérationnelle • Mise en œuvre et maintenance des réseaux informatiques • Valorisation de la donnée et la cybersécurité • Développement et validation de solutions logicielles cyber • Gestion d'incidents	01 · 03 · 07 · 15 · 26 · 38 · 42 · 43 · 63 · 73 · 74
01 : Bourg-en-Bresse *03 : Montluçon* *07 : Aubenas* *15 : Aurillac* *26 : Crest, Valence* *38 : Grenoble *2, Vizille, Meylan, Saint Martin d'Hères* *42 : Andrézieux Bouthéon, Saint-Etienne, Rive-de-Gier* *63 : Clermont-Ferrand* *69 : Lyon 5, Lyon 8, Vénissieux* *74 : Argonay, Cluses, Annecy*	**BTS CIEL : Cybersécurité, informatique, et réseaux, électronique (bac+2)**	• Réalise la production, l'intégration et la maintenance de produits électroniques • Mettre en œuvre des réseaux informatiques : installer un système informatique, manager et exploiter un réseau informatique	01 · 03 · 07 · 15 · 26 · 38 · 42 · 63 · 69 · 74

Source : Région Auvergne-Rhône-Alpes, Direction de la formation et de l'orientation (DFOR)

10 SESSIONS DE FORMATIONS EN CYBERSÉCURITÉ À DESTINATION DES DEMANDEURS D'EMPLOI

La Région Auvergne-Rhône-Alpes

— La Direction de la Formation et de l'Orientation de la **Région Auvergne-Rhône-Alpes** lance un projet prévisionnel de **10 sessions de formation en cybersécurité à destination des demandeurs d'emploi**.

Lots	Métier	Titulaire		Co - sous traitant	Localisations proposées
		Organisme	Coordonnées		
Cyber Expert - académie Grenoble	.Chargé de GRC (gouvernance risque et conformité) : normes qualité cyber .Technicien sécurité réseau / Administrateur infrastructure sécurisée (AIS)	le campus numérique in the ALPS	Pauline Lacour : pauline.lacour@le-campus-numerique.fr	CSB.School	Grenoble (38)
Cyber Expert - académie Lyon	.Chargé de GRC (gouvernance risque et conformité) : normes qualité cyber .Technicien sécurité réseau / Administrateur infrastructure sécurisée (AIS) .Analyste SOC	CSB .school	Vianney Wattinne : vianney.wattinne@csb.school	Human booster	Charbonnieres-Les-Bains (69)
Cyber Expert - académie Clermont-Ferrand	.Technicien sécurité réseau / Administrateur infrastructure sécurisée (AIS) .Analyste SOC	Humanbooster	Raphael Coubetergues : rcoubetergues@humanbooster.com	CSB.School	Clermont-Ferrand (63)
Acculturation IA / Cyber - académie Clermont-Ferrand	Acculturation Cyber Industries, Energie, Agriculture	Humanbooster	Raphael Coubetergues : rcoubetergues@humanbooster.com	x	Vichy (03) Aurillac (15) Le Puy-En-Velay (43) Clermont-Ferrand (63)
Acculturation IA / Cyber - académie Lyon	Acculturation Cyber Industries, Energie, Agriculture	Humanbooster	Raphael Coubetergues : rcoubetergues@humanbooster.com	x	Villeurbanne (69) Saint-Etienne (42) Bourg-en-Bresse (01) Saint-Genis-Pouilly (01)
Acculturation IA / Cyber - académie Grenoble	Acculturation Cyber Industries, Energie, Agriculture	SIMPLON.CO	Pauline Gervais : pgervais@simplon.co	Alter'class	Grenoble (38) Châteauneuf-sur-Isère (26) Chambéry (73) Annecy (74) Villefontaine (38)
Cyber Expert académie Lyon et académie Clermont-Ferrand	.Chargé de GRC (gouvernance risque et conformité) : normes qualité cyber .Technicien sécurité réseau / Administrateur infrastructure sécurisée (AIS) .Analyste SOC	isitech CAMPUS DU NUMÉRIQUE	Tayeb Bouraya : t.bouraya@ecole-isitech.fr	n.c.	Lyon (69) Clermont-Ferrand (63)

Source : Région Auvergne-Rhône-Alpes, Direction de la formation et de l'orientation (DFOR)

51 FORMATIONS DE L'ENSEIGNEMENT SUPÉRIEUR EN CYBERSÉCURITÉ EN AUVERGNE-RHÔNE-ALPES

SecNumedu ANSSI **Les formations mentionnant "SecNumEdu" sont des formations spécialisées en cybersécurité labélisées par l'ANSSI (Agence nationale de la sécurité des systèmes d'information)**

Les formations de l'enseignement supérieur en cybersécurité en Auvergne-Rhône-Alpes de niveau bac + 2 (hors BTS)

Etablissement	Diplôme	Spécialités	Métiers visés
mi Formation	**Technicien supérieur systèmes réseaux** Lyon (69)	.Sécurité des accès à Internet .Exploitation d'un environnement virtualisé .Maintenance et exploitation Windows et Linux	.Technicien(ne) Supérieur(e) Systèmes et Réseaux .Administrateur(trice) Réseaux/ Télécom
mi Formation	**Analyste Cybersécurité** Lyon (69)	.Stockage sur cloud .Mise en œuvre solution IoT robuste et sécurisée .Sécurité des systèmes communicants .Mécanismes cryptographiques	.Administrateur sécurité .Spécialiste en gestion de crise .Consultant en sécurité organisationnelle
LA MACHE Supérieur	**Technicien Supérieur Systèmes et Réseaux** Lyon (69)	.Sécurité des applications .Virtualisation et cloud computing .Sécurité des infrastructures .Sécurité des systèmes, services et réseaux	Technicien Supérieur Systèmes et Réseaux
CCI DRÔME	**Technicien supérieur systèmes et réseaux** Alixan (26)	.Exploiter les éléments de l'infrastructure et assurer le support aux utilisateurs .Maintenir l'infrastructure et contribuer à son évolution et sa sécurisation	

Les formations de l'enseignement supérieur en cybersécurité en Auvergne-Rhône-Alpes de niveau bac +3 (1/2)

Etablissement	Diplôme	Spécialités	Métiers visés
IUT Annecy Université Savoie Mont Blanc, IUT de Roanne Université Jean Monnet, IUT1A Université Grenoble Alpes, SecNumedu ANSSI, IUTA Valence Université Grenoble Alpes, UCA IUT Clermont Auvergne	**BUT spécialité réseaux & télécommunications parcours cybersécurité** Annecy (74), Roanne (42), Grenoble (38), Valence (26), Clermont-Ferrand (63)	.Sécurité des systèmes et des réseaux .Audit .Analyse de risques .Normes et cadre juridique	.Responsable de la sécurité informatique au sein d'une petite structure .Analyste sécurité .Responsable de projet de sécurité .Spécialiste sécurité d'un domaine technique .Spécialiste en développement sécurisé
RÉPUBLIQUE FRANÇAISE, greta ARDÈCHE - DRÔME FORMEZ-VOUS À DEMAIN, CAMPUS RÉGION DU NUMÉRIQUE	**BUT 3 Réseaux et Télécommunications parcours Cybersécurité** Valence (26)	.Sécurisation des systèmes informatiques : analyse de l'existant, étude des besoins de sécurité, évolution et mise en conformité .Surveillance et gestion de crise : analyse du système d'information, audit de sécurité, gestion d'un incident	.Administrateur systèmes et réseaux .Technicien en cybersécurité .Superviseur de réseaux mobiles 4G/5G .Pilote d'exploitation de réseaux sans fil Wifi/Lora .Intégrateur Devops/Cloud
MFR CULTIVONS LES RÉUSSITES CAMPUS DU BEAUJOLAIS	**Administrateur d'infrastructures sécurisées** Limas (69)	.Sécurité serveurs, réseaux et hyperviseurs .Sécurité d'une infrastructure distribuée .Création de scripts d'automatisation .Analyse du niveau de sécurité .Mise en œuvre de la politique de sécurité	.Administrateur d'infrastructures sécurisées .Chef de projet sécurité des SI .Expert ingénierie des systèmes
Pôle La Chartreuse, FSA FORMASUP AUVERGNE	**Administrateur d'infrastructures sécurisées** Brives-Charensac (43)	.Sécurité du Système d'Information .Sécurité réseau .SGBD .Cybersécurité des logiciels et applications	.Administrateur sécurité SI .Administrateur réseaux et sécurité .Responsable sécurité informatique
CCI DRÔME	**Administrateur d'infrastructures sécurisées (AIS)** Alixan (26)	.Administrer et sécuriser les infrastructures .Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution, tout en participant à la gestion de la cybersécurité	
epsi l'école d'ingénierie informatique	**Administrateur d'infrastructures sécurisées** Lyon (69), Grenoble (38) ou Saint-Etienne (42)	.Sécurité réseau entreprise .Administration et sécurité environnement .Administration et sécurité infrastructure .Création de scripts d'automatisation .Analyse des risques	.Administrateur systèmes et réseaux .Administrateur réseaux .Administrateur d'infrastructures
WILD CODE SCHOOL	**Administrateur Infrastructures Sécurisées** Lyon (69)	.Administration et sécurité des réseaux .Sécurité des infrastructures .Mise en œuvre de solution adapté à un besoin .Gestion de la cybersécurité	.Administrateur d'infrastructures sécurisées .Technicien systèmes et réseaux

Source : Côté Formations, Tout savoir sur la formation en Auvergne-Rhône-Alpes, Campus Région du numérique, ANSSI

Les formations de l'enseignement supérieur en cybersécurité en Auvergne-Rhône-Alpes de niveau bac +3 (2/2)

Etablissement	Diplôme	Spécialités	Métiers visés
mi Formation – Campus Région du numérique	**Administrateur d'infrastructures sécurisées** En distanciel	.Sécurité du réseau d'entreprise .Sécurité d'environnement système hétérogène .Sécurité d'infrastructure système hétérogène .Gestion de l'infrastructure cloud .Analyse du niveau de sécurité de l'infrastructure .Mise en œuvre de la politique de sécurité	.Administrateur Réseaux Télécom .Administrateur Systèmes .Administrateur Infrastructures .Technicien Support Technique
Afpa – Campus Région du numérique	**Administrateur d'infrastructures sécurisées** Vénissieux (69)	.Sécurité réseaux .Sécurité base de données .Sécurité systèmes .Sécurité infrastructure distribuée .Analyse des risques	.Admin. sécurité informatique, infrastructures sécurisées, systèmes et réseaux .Gestionnaire de réseau .Resp. réseaux et télécoms
LA MACHE - Supérieur -	**Administrateur d'Infrastructures Sécurisées** Lyon (69)	.Administration et sécurité des infrastructures .Analyse des besoins et rédaction de cahier des charges .Sécurité systèmes et réseaux .Infrastructures à haute disponibilité .Politique de sécurité des systèmes d'information	.Administrateur systèmes et réseaux .Responsable infrastructure systèmes et réseaux
Cifep Chambéry & Lyon	**Administrateur d'infrastructures sécurisées** Chambéry (73)	.Sécurité des composants .Administration et sécurité du réseau d'entreprise .Sécurité d'environnement système hétérogène .Sécurité infrastructure de serveurs virtualisé .Analyse des risques et du niveau de sécurité	.Administrateur systèmes et réseaux .Responsable infrastructure systèmes et réseaux
Hesias	**Administrateur d'infrastructures sécurisées** Clermont-Ferrand (73)	.Administration Systèmes et Réseaux .OS hardening et clusterisation .Windows Server & Linux avancés .CCNA Enterprise & O365 Admin .Projets d'archi sécurisée	.Administrateur / responsable systèmes et réseaux .Responsable infrastructure systèmes et réseaux
Aktéap CFA CFC	**Administrateur systèmes, réseaux et cybersécurité** Annecy (74)	.Administrer et optimiser les systèmes d'exploitation et la virtualisation pour la sécurité et la performance .Configurer et administrer l'infrastructure réseau et les solutions cloud .Élaborer et mettre en œuvre des stratégies de cybersécurité et de protection des données .Conduire la gestion de projets d'infrastructure systèmes et réseaux sécurisée	.Administrateur systèmes et réseaux .Analyste en cybersécurité. .Responsable infrastructure informatique .Consultant en systèmes d'information
Saint Michel Annecy Haute-Savoie – Jedha	**Développeur en science des données – Cybersécurité** Lyon (69)	.Stockage sur cloud .Mise en œuvre solution IoT robuste et sécurisée .Sécurité des systèmes communicants .Mécanismes cryptographiques .Attaques physiques	.Consultant Cybersécurité .Ethical hacker .RSSI Junior .Ingénieur en Cybersécurité
CSB school – Campus Région du numérique – SecNumedu	**Spécialiste en cybersécurité** Lyon (69)	.Pentest, tests d'intrusion éthiques .Architecture Sécurité Réseaux .Sécurité des données et des identités .Détection et analyse des événements de cyber	.Analyste de la menace .Architecte sécurité .Auditeur de sécurité orga. .Consultant en cybersécurité
GUARDIA CYBERSECURITY SCHOOL	**Bachelor Cybersécurité** Lyon (69)	.Sécurité des réseaux et des matériels .Sécurité des applications web ou mobile .Virtualisation, Pentesting, Audit .Sécurité des infrastructures du SI	.Pentester / Hacker éthique .Analyste SOC .Administrateur réseau .Superviseur d'infrastructures
ECORIS L'ÉCOLE DE L'ENTREPRISE	**Bachelor Cybersécurité des systèmes industriels** Lyon (69)	.Sécurité des composants .Sécurité de l'infrastructure .Admin. et sécurité d'une infrastructure distribuée .Gestion opérationnelle de la cybersécurité	.Administrateur d'infrastructures sécurisées
ECAM LaSalle	**Bachelor Cybersécurité des systèmes industriels** Lyon (69)	.Sécurité des systèmes industriels et urbains .Analyse de système industriel ou urbain .Exercice de simulations d'attaques .Mise en place de systèmes de défense	.Analyste programmeur informatique industrielle ou Cybersécurité SI industriel .Consultant en cybersécurité IT/ OT/IoT .Automaticien cyber
CCI NORD ISÈRE	**Bachelor AIS Administrateur d'Infrastructures Sécurisées** (bac+3) Villefontaine (38)	.Administrer et protéger les architectures informatiques (fiabilité et cybersécurité) .Concevoir, déployer et maintenir des architectures informatiques en intégrant la sécurité au cœur de chaque composante	.Administrateur Systèmes et Sécurité (ASS) .Technicien Expert en Cyber .Consultant en sécurité des SI .Architecte Réseaux et Sécurité .Gestionnaire de crise cyber
SUPINFO – Campus Région du numérique	**Bachelor of Science Auditeur en Cybersécurité** Lyon (69)	.Maîtrise des surfaces et des techniques d'attaques .Mécanismes de chiffrements .Tests d'intrusion, études des nouvelles menaces, scénarios d'attaques .Audits de sécurité	.Pentester / hacker éthique .Analyste de centre opérationnel de sécurité .Analyste de risques informatiques

Sources : Côté Formations, Tout savoir sur la formation en Auvergne-Rhône-Alpes, Campus Région du numérique, ANSSI

Les formations de l'enseignement supérieur public en cybersécurité en Auvergne-Rhône-Alpes de niveau bac +5

Etablissement	Diplôme	Spécialités	Métiers visés
	Master mention Informatique parcours concepts et application Lyon (69)	.Cryptographie et sécurité .Systèmes informatiques confidentiels .Algorithmes pour la cryptographie à clé publique .Cryptographie de treillis appliquée	.Chercheur et enseignant-chercheur en informatique .Ingénieur en R&D .Cadre dans de grands établissements académiques et laboratoires de pointe
	Master mention informatique : Cybersécurité et informatique légale Grenoble (39)	.Sécurité des systèmes et des réseaux .Audit .Analyse de risques .Informatique légale (forensic) .Sécurité des composants et des logiciels .Aspects juridiques	.Ingénieur en sécurité .Ingénieur d'études et R&D en sécurité .Responsable des SI .Responsable sécurité informatique
	Master mention informatique Cybersecurity Grenoble (en anglais)(38)	.Cryptologie avancée .Robustesse des infrastructures critiques, des composants de sécurité .Protection de la vie privée .Sécurité des infrastructures cloud	.Ingénieur en cybersécurité .Ingénieur en sécurité des SI .Ingénieur spécialisé en audit sécurité des SI
	Master Réseaux Informatiques d'Entreprise Grenoble (38)	.Sécurité des réseaux .Sécurité des infrastructures et des systèmes informatiques .Sécurité des applications .Ingénierie de la sécurité	.Chef de projet cybersécurité .Opérateur d'ingénierie des réseaux .Ingénieur sécurité des IoT .Chef de projet infrastructures cloud
	Ingénieur Réseaux et Cybersécurité Valence (26)	.Cryptographie .Sécurité des réseaux et des systèmes .Sécurité logicielle et sûreté de fonctionnement .Infrastructure Cloud .Architectures de réseaux	.Concepteur et développeur d'applications .Chef de projet en maitrise d'œuvre ou maitrise d'ouvrage .Architecte réseau (Pilotage) .Expert/consultant réseau
	Ingénieur Filière Réseaux et sécurité informatique Clermont-Ferrand (63)	.Sécurité de l'électronique .Sécurité des systèmes d'exploitation .Sécurité des réseaux et protocoles .Cryptologie .Sécurité des bases de données .Tests d'intrusion	.Administrateur sécurité .Analyste SOC .Architecte sécurité .Consultant sécurité .Cryptologue .Développeur sécurité .Expert réponse à incident, RSSI, responsable PCA
	Mastère spécialisé Cybersécurité du numérique Lyon (69)	.Sécurité des systèmes et réseaux .Sécurité des applications Cloud et sécurité Cybersécurité industrielle et SCADA Gestion opérationnelle Gestion des identités Tests de pénétration des infrastructures	.RSSI Chef de projet Cybersécurité Consultant organisationnel Ingénieur et intégrateur de solutions en cybersécurité
	Mastère Spécialisé IoT : Designer of Secure Devices for IoT St-Etienne (42)	.Stockage sur cloud .Mise en œuvre d'une solution IoT robuste et sécurisée .Sécurité des systèmes communicants .Mécanismes cryptographiques .Attaques physiques	.Ingénieur roboticien .Ingénieur en électronique .Développeur .Chef de projet IoT .Responsable système d'information
	Mastère Spécialisé Manager de la Cybersécurité Industrielle Charbonnières-les-Bains (69)	.Protections des systèmes d'information .Convergence IT/OT .Détection, réponses aux attaques, remédiation .Industrie du Futur, Évolutions technologiques	.Responsable de la sécurité des systèmes communicants .Ingénieur en architecture de systèmes d'information (IT/OT) .Analyste en menaces et incidents de cybersécurité .Intégrateur de solutions de sécurité .Chef de projet Sécurité / Consultant en cybersécurité industrielle
	Master Organisation et protection des systèmes d'information en entreprise (OPSIE) Lyon (69)	.Sécurité des infrastructures .Sécurité des données .Cryptographie .Sécurité applicative .Audit informatique .Analyse des risques .Plan de reprise d'activité	.RSSI .Consultant Cybersécurité .Concepteur et Développeur cyber .Evaluateur sécurité .Analyste de la menace .Délégué à la protection des données
	Master Systèmes, réseaux et Sécurité Lyon (69)	.Sécurité réseaux sans fil et avancés .Sécurité systèmes .Cloud, stockage et virtualisation .Sécurité d'une architecture réseau .Administration systèmes et réseaux	.Administrateur systèmes et réseaux .Ingénieur DevOps .Expert Cloud .Ingénieur sécurité .Architecte réseaux .Consultant

Source : Côté Formations, Tout savoir sur la formation en Auvergne-Rhône-Alpes, Campus Région du numérique, ANSSI

Etablissement	Diplôme	Spécialités	Métiers visés
CSB .school / SecNumedu / Campus Région du numérique	**Responsable cybersécurité** Charbonnières-les-Bains (69)	. Cybersécurité industrielle : évaluation de la criticité des sites et infrastructures . Sécurité opérationnelle : événements pouvant conduire à un incident . Gestion des risques et conformité	. Analyste de la menace, réponse aux incidents de sécurité . Architecte sécurité . Auditeur de sécurité organisationnelle
EPITECH LEARN DIFFERENT	**MSC Pro Cybersécurité** Lyon (69)	. Audit de sécurité (pentester) . Sécurité des systèmes informatiques . Cryptographie . Forensic	. RSSI ; Auditeur cybersécurité . Consultant sécurité informatique . Administrateur sécurité . Pentester
GUARDIA CYBERSECURITY SCHOOL	**Master of Science Expert Cybersécurité** Lyon (69)	. Analyse et évaluation d'un SI (pentest, audits, analyse menaces) . Gouvernance, risques et sécurité . Gestion opérationnelle de la sécurité . Mise en place de solutions techniques	. Consultant en cybersécurité . Analyste SOC . Architecte Cybersécurité . Ingénieur Cybersécurité . Hacker éthique
CESI ÉCOLE D'INGÉNIEURS / Campus Région du numérique	**Manager en infrastructures et cybersécurité des SI – option sécurité** Charbonnières-les-Bains (69) / Grenoble (38)	. Design des infrastructures réseaux . Sécurité réseaux . Sécurité du cloud . Sécurité des infrastructures du SI . Audit . LOTJ : Concevoir l'infrastructure du SI	. Architecte du SI . Directeur ou responsable informatique . RSSI . Ingénieur en cybersécurité . Chef de projet informatique . Consultant en SI et sécurité
42 / Campus Région du numérique	**Tronc commun en informatique, spécialisation possible en sécurité** Charbonnières-les-Bains (69)	. Cryptologie avancée . Robustesse des infrastructures critiques . Protection de la vie privée et sécurité des infrastructures cloud . Détection des vulnérabilités dans les protocoles	. Technicien cybersécurité . Administrateur systèmes et réseaux . Administrateur réseaux Cloud . Security Analyst ou Security Engineer . Consultant en Cybersécurité . QA Engineer
CPE LYON / Institut des ressources industrielles / Live and Discover Les Chartreux	**Ingénieur en informatique et cybersécurité (ICS)** Lyon (69)	. Conception, développement des systèmes informatiques ; DevOps . Sécurité informatique . Conception logicielle et gouvernance des données	. Intégrateur de sécurit . Auditeur sécurité informatique . Administrateur de base de données
<it/> akademy / Campus Région du numérique	**Expert en cybersécurité – Responsable de la sécurité du SI** Charbonnières-les-Bains (69)	. Sécurité des réseaux et infrastructures . Sécurité des systèmes et applications . Conduite d'audit et tests de pénétration . Analyse de risques /Forensics . Implémentation d'un SMSI (ISO 27001)	. Coordinateur sécurité ; Risk manager . Pentester ; Analyste SOC . Consultant en sécurité des SI . Auditeur SSI . Intégrateur de solutions de sécurité
AFIP L'école de votre avenir	**Expert en ingénierie informatique** Lyon (69)	. Sécurité réseaux et infrastructures . Sécurité systèmes . Haute Disponibilité sécurité . Théorie de la cybersécurité	. Consultant en SI . Chef de projet sécurité . Analyste SOC ; Forensic . Resp. Systèmes et Réseaux ; RSSI
hexagone École Supérieure d'Informatique	**Mastère Cyberdéfense et sécurité des systèmes d'information** Clermont-Ferrand (63)	. Gestion de crise cyber . Sécurité réseaux, des systèmes industriels . Cryptologie . Audit technique . Sécurité d'une architecture réseau	. Pentester . Cryptologue . Ingénieur Cybersécurité et Cyberdéfense . Consultant
epsi® l'école d'ingénierie informatique	**Expert en cybersécurité** Lyon (69), Grenoble (38), Saint-Etienne (42)	. Sécurité réseaux et systèmes . Data Architectures . Sécurité des données . Gestion de la sécurité et audit sécurité	. RSSI, Architecte SSI . Consultant en cybersécurité . Analyste SOC
Aktéap CFA CFC / Saint Michel Annecy Haute-Savoie	**Mastère Expert en architectures systèmes-réseaux et en sécurité informatique** Annecy (74)	. Sécurité des réseaux . Conception infras. sécurisée Haute Dispo . Sécurisation et intégrité des données . Analyse des risques de sécurité . Test d'intrusion, hacking éthique . Gérer un SI après compromission	. Consultant SI . Architecte SI . Consultant en cybersécurité . Expert SI et réseaux . RSSI
ipi INFORMATIQUE ET NUMÉRIQUE UNE ÉCOLE DU GROUPE IGS / Campus Région du numérique	**Mastère Cyber Xpert : Expert en cybersécurité** Lyon (69)	. Cybersécurité applicative et industrielle . Introduction à la blockchain . Sécurité des architectures et tests d'intrusion	. Chef de projet réseaux, sécurité . Responsable infrastructure et sécurité
mi Formation	**Analyste Cybersécurité** Lyon (69)	. Administration et sécurité des réseaux . Sécurité des objets connectés, IoT . Implémentation de techniques cryptographiques . Analyse de malware, Etudes de failles de sécurité	. Consultant en SI ou en cyber . Chef de projet sécurité . Analyste SOC ; Forensic . Responsable Systèmes et Réseaux ; RSSI
IPAC	**MBA Cybersécurité et architecture réseau** Annecy (74)	. Conception et durcissement des architectures Protection et détection : politiques de sécurité, chiffrement, EDR/XDR, SOC, SIEM, réponse incident . Audit & conformité : investigation numérique	. Architecte de sécurité réseau . Expert systèmes & infrastructures cloud . Chief Technical Officer (CTO) . Responsable SOC / Responsable cyber
ynov CAMPUS / Campus Région du numérique	**Mastère Expert en Cybersécurité** Lyon (69)	. Cybersécurité des systèmes d'exploitation . Cybersécurité des réseaux et des Infrastructures . Cyber Threat Intelligence . Vulnérabilités web et logiciel	. Ingénieur cybersécurité . Consultant en cybersécurité . Auditeur sécurité d'information . Analyste SOC ; Pentester
ynov CAMPUS / Campus Région du numérique	**Mastère Expert en gouvernance de la Cybersécurité** Lyon (69)	. Evaluation des risques . Réponse aux incidents / Gestion de la sécurité . Cryptographie . Analyse de malware, réponse aux incidents, intelligence des menaces	. Ingénieur cybersécurité . Consultant en cybersécurité . Auditeur sécurité d'information . Analyste SOC ; Pentester

Source : Côté Formations, Tout savoir sur la formation en Auvergne-Rhône-Alpes, Campus Région du numérique, ANSSI

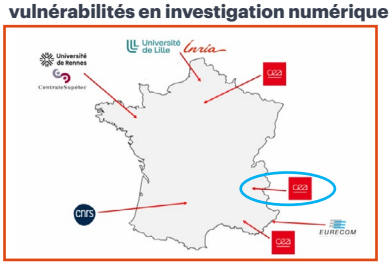
LA RECHERCHE EN CYBERSÉCURITÉ

7 DES 10 PROGRAMMES DE RECHERCHE NATIONAUX IMPLIQUENT DES LABORATOIRES RÉGIONAUX

— **Les laboratoires de recherche de la région Auvergne-Rhône-Alpes sont au cœur de la recherche nationale en cybersécurité** avec une participation dans **7 des 10 PEPR** (Programmes et Equipements Prioritaires de Recherche) pour la cybersécurité, lancés au niveau national en 2021.

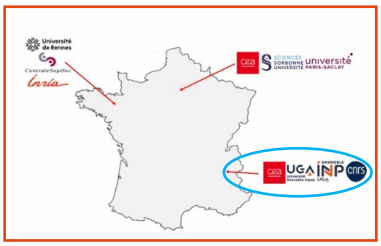
Consortium de recherche IPOP	*Consortiums SecurEval, ARSENE, SuperviZ*	*Consortium ARSENE*	*Consortiums IPOP, SecurEval, ARSENE, Cryptanalyse*	*Consortiums SecurEval, ARSENE, COMPROMIS, SuperviZ, REV*

Implantation du consortium REV : l'exploitation de vulnérabilités en investigation numérique



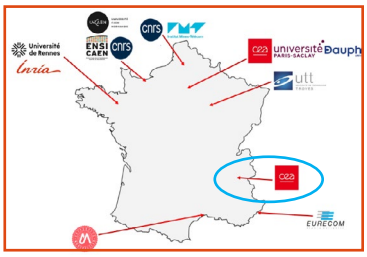
Implantation du consortium de recherche IPOP: la protection des données personnelles

Implantation du consortium de recherche SecurEval : l'évaluation de la sécurité des logiciels

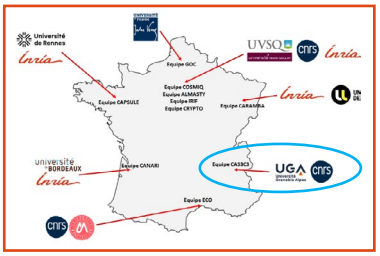


Implantation du consortium ARSENE : la sécurité matérielle et logicielle des systèmes embarqués

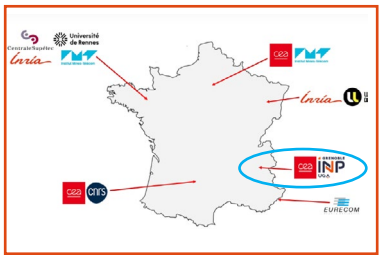
Implantation du consortium COMPROMIS : la sécurité des données multimédia



Implantation du consortium Cryptanalyse : la résistance des systèmes cryptographiques



Implantation du consortium de recherche SuperviZ : la supervision et l'orchestration de la sécurité



Source : France 2030, Programme et équipements prioritaires de recherche pour la cybersécurité

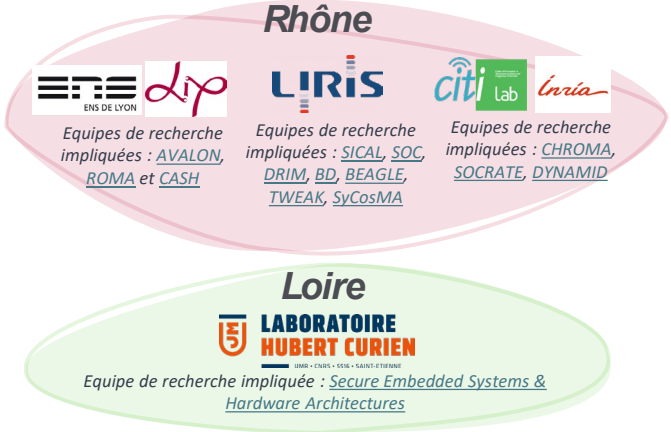
UN ÉCOSYSTÈME DE RECHERCHE LYONNAIS ET STÉPHANOIS SPÉCIALISÉ DANS L'INFORMATIQUE DISTRIBUÉE

Fédération Informatique de Lyon

— Issues des 4 laboratoires **LIRIS, LIP, HUBERT CURIEN et CITI**, les **14 équipes de recherche** de la **Fédération Informatique de Lyon** rassemblées autour du thème de **l'informatique distribuée et calcul haute performance** couvrent un spectre scientifique très large : la modélisation, l'optimisation et l'exploitation des systèmes et applications réparties et parallèles. Parmi les axes de recherche actifs au sein de la fédération, on peut citer :

- **Le calcul haute-performance** (calcul scientifique, simulation, etc.)
- L'algorithmique et la programmation réparties et parallèles
- **La résilience des systèmes et des applications réparties**, la tolérance aux fautes et la gestion de la volatilité et de la dynamicité des systèmes
- **La sécurité et la protection de la vie privée**

Cartographie des principaux centres de recherche lyonnais et stéphanois spécialisés dans les axes de recherche cybersécurité



Source : Fédération Informatique de Lyon

UN ÉCOSYSTÈME DE RECHERCHE GRENOBLOIS TRÈS DYNAMIQUE COORDONNÉ PAR CYBERALPS

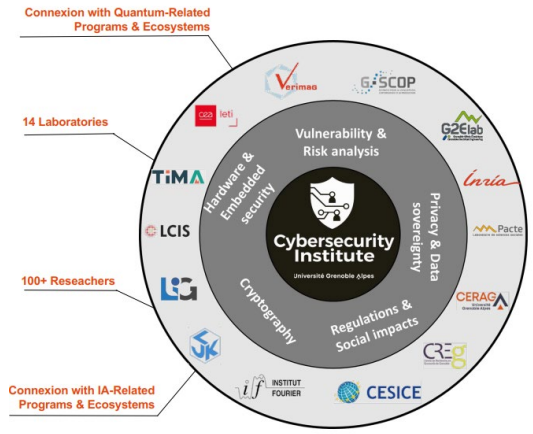
— **La communauté du CyberSecurity Institute (CyberAlps)** est un institut multidisciplinaire unique en matière de cybersécurité qui vise à promouvoir et fédérer les recherches en cybersécurité sur le bassin grenoblois **en associant recherche scientifique, développements technologiques et coopérations scientifiques** internationales.

— Par sa taille, ses nombreuses collaborations et partenariats régionaux, nationaux et internationaux, le caractère multidisciplinaire de ses recherches, le nombre et la qualité de ses publications, **CyberAlps offre au site grenoblois une visibilité de premier ordre dans le domaine de la cybersécurité**.

— CyberAlps s'est notamment positionné sur **cinq domaines d'expertise stratégiques** interdisciplinaires :

- **La sécurité matérielle, de l'embarqué à l'industriel par les systèmes à puce (SoC)**
  - Étudier les conséquences que les choix d'implémentation dans la réalisation matérielle (conception, optimisation, contre-mesures) peuvent avoir sur l'ensemble du cycle de développement sécurisé, en particulier sur le développement de logiciels sécurisés
  - Concevoir et analyser des primitives cryptographiques à la fois économes en énergie, performantes et robustes
  - Répondre aux défis dans les domaines de la sécurité, de la sûreté et de la résilience
- **La souveraineté des données**
  - Favoriser des traitements respectueux de la vie privée dès la conception (privacy by design)
  - Contrôler les services qui ne sont pas respectueux de la vie privée
- **Les outils de cryptanalyse**
  - Développer un « cyber-centaure », terme désignant un expert en sécurité équipé de logiciels afin de multiplier ses capacités
  - Mettre en place une chaîne d'outils de bout en bout permettant d'identifier rapidement les zones critiques et potentiellement vulnérables
  - Étudier de nouveaux outils fondés sur des techniques disruptives afin de mieux anticiper les attaques futures
  - Développer de nouveaux logiciels pour résoudre des problèmes structurés d'algèbre linéaire apparaissant en cryptanalyse
  - Implémenter efficacement les meilleurs algorithmes
- **Les nouveaux risques de la cybersécurité : menace quantique et intelligence artificielle**
  - Étudier et concevoir un coprocesseur hybride optimisé, pré- et post-quantique
  - Étudier et évaluer la faisabilité d'attaques par canaux auxiliaires et par injection de fautes contre ces nouvelles cryptographies, et concevoir des contre-mesures appropriées
- **La réglementation de la cybersécurité aux niveaux national, européen et international**
  - Analyser en profondeur les positions de tous les États et des organisations internationales concernant la régulation de la cybersécurité

Les 14 laboratoires de recherche grenoblois au cœur de la dynamique d'innovation cybersécurité en Auvergne-Rhône-Alpes



14 laboratoires de recherche

- **CEA-LETI** : Architectures de sécurité, cryptographie, communications sécurisées.
- **CERAG** : Problématiques de risques liés aux cryptomonnaies.
- **CESICE** : Enjeux liés au numérique et aux cyberattaques.
- **CREG** : Centre de recherche économique de Grenoble.
- **G2Elab** : Systèmes cyber-physiques, intelligence artificielle et apprentissage automatique.
- **G-SCOP** : Informatique et systèmes d'information, calcul scientifique et systèmes intelligents.
- **INRIA** : Sécurité de l'information et sécurité des systèmes.
- **FOURIER** : Laboratoire de mathématiques
- **LJK** : Laboratoire de mathématiques appliquées et d'informatique
- **LCIS** : Sûreté et sécurité des systèmes embarqués et distribués, modélisation, analyse et supervision des systèmes complexes ouverts et des systèmes radiofréquences sans fil communicants. Travaille sur des domaines d'application variés : internet des objets, systèmes cyber-physiques, environnements connectés naturels ou artificiels, RFID, etc.
- **LIG** : Ingénierie des logiciels et des systèmes d'information, méthodes formelles, modèles et langages
- **PACTE** : Ressorts de la confiance et de la souveraineté dans les processus d'innovations monétaires.
- **TIMA** : Spécification, conception, vérification, tests, outils de CAO et méthodes de conception pour les systèmes intégrés, depuis les composants analogiques et numériques jusqu'aux systèmes sur puce multiprocesseurs avec leur système d'exploitation de base.
- **VERIMAG** : Produit des outils théoriques et techniques permettant de répondre aux attentes des systèmes cyber-physiques avec une rigueur mathématique. Travaille sur des circuits, des processeurs, des systèmes analogiques ou hybrides, des compilateurs, des protocoles de sécurité, des algorithmes distribués, des systèmes intégrant de l'IA, en particulier dans le contexte des systèmes critiques.

Source : Cyber Alps

LE CEA GRENOBLE : UNE RÉFÉRENCE MONDIALE DANS L'ANALYSE DES VULNÉRABILITÉS ET LA PROTECTION DES SYSTÈMES

— Le CEA (Commissariat à l'Energie Atomique et aux Énergies Alternatives) a pour mission de valoriser auprès des industriels les résultats des recherches menées par ses collaborateurs afin de soutenir la compétitivité des entreprises, favoriser la création d'emplois et, plus globalement, contribuer à la souveraineté industrielle de la France. Pour parvenir à ces résultats et développer des technologies au plus près des besoins sociétaux, le CEA met en place les outils et dispositifs permettant de favoriser l'émergence, l'accompagnement et la diffusion des innovations, avec 4 grands objectifs : **accompagner les industriels dans l'innovation, soutenir la création d'entreprise, partager une culture commune de l'innovation, soutenir l'anticipation et la rupture**.

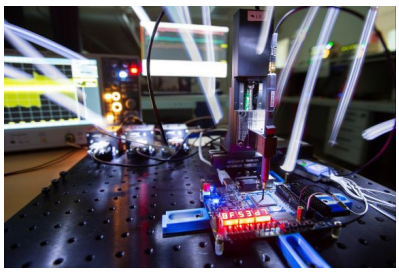
— Le CEA est un acteur majeur de la recherche à l'échelle nationale et mondiale dans le numérique. Depuis 2019, ses activités de **recherche en cybersécurité** sont regroupées dans un grand programme qui mobilise aujourd'hui près de 200 ingénieurs-chercheurs.

— Le **centre de Grenoble est le centre de référence du CEA au niveau national sur les recherches en sécurité du matériel**, notamment sur deux axes forts : l'identification des vulnérabilités et la protection des systèmes.

— Au sein du ***Centre d'Evaluation de la Sécurité des Technologies de l'Information (CESTI) du CEA-Leti***, les équipes de recherche soumettent à rude épreuve les systèmes qui leur sont confiés. Les systèmes ont besoin d'un certificat de sécurité délivré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), cette certification repose sur l'évaluation préalable réalisé par un CESTI de la sécurité et de la conformité des systèmes. Le CESTI reçoit ainsi régulièrement des composants sécurisés et leurs logiciels pour être passés au crible : puces nues, papiers d'identité, cartes de crédit, logiciels embarqués, boîtiers sécurisés de type HSM ou capteurs d'empreintes digitales... peuvent être analysés. Récemment agréé premier CESTI français pour la cryptographie post quantique, le CESTI du CEA-Leti évolue constamment pour rester à la pointe et faire face à la diversification des techniques et moyens d'attaque permis par les technologies du numérique.

— Au-delà de l'expertise pointue sur l'analyse et la mise à nu des vulnérabilités, le CEA est aussi pourvoyeur de solutions pour sécuriser les systèmes en réseaux, embarqués, ainsi que les données associées. En fonction des attaques à contrer, les technologies inventées par le CEA forment un panel très large de réponses, en particulier sur la conception de nouvelles fonctions pour sécuriser les circuits intégrés.

— Expertises mises à disposition des industriels :
- analyses de risques spécifiques aux technologies et aux cas d'usage des partenaires,
- nouvelles stratégies d'attaques matérielles et logicielles,
- étude et conception de mécanismes de sécurité et de contre-mesures, adaptés à la criticité des systèmes et des équipements, technologies et architectures matérielles à haut niveau de sécurité,
- intelligence artificielle pour la sécurité et sécurité de l'intelligence artificielle,
- R&D amont en cybersécurité (au travers du Programme et Equipements Prioritaires de Recherche - PERP et du programme « recherche à risque » - « Audace ! »).



Plateforme cybersécurité du CEA-Leti @C. Morel /CEA

La cybersécurité au CEA à Grenoble

— **100 ingénieurs chercheurs**

— **1 des 3 CESTI matériels nationaux** opéré depuis 25 ans en lien avec l'ANSSI

— **Des plateformes à l'état de l'art** (cybersécurité / conception numérique / microélectronique)

— **Des thématiques de R&D variées** :
- Tests de sécurité
- Implémentation optimisée et sécurisée de cryptographie post quantique
- Conception de briques de sécurité pour circuits intégrés
- Outils de supervision & détection pour la sécurité des systèmes industriels
- Sécurité de l'IA
- TRNGs et PUFs

— **Des collaborations avec les acteurs locaux** (Start-up, PME, grands groupes, et académiques)
- Collaborations avec Schneider Electric, SOITEC, Tiempo Secure...
- Direction scientifique avec CNRS et INRIA du PEPR cybersécurité – présence dans 6 des 10 projets avec CNRS, UGA, G-INP, INRIA, INSA Lyon, Université Lyon, Université Jean Monnet, IMT
- Opérateur du programme cybersécurité de l'IRT Nanoelec

— **Membre et acteur dans diverses initiatives régionales**
- CyberAlps
- Cyber cercle
- Minalogic
- CSAW

Source : CEA Grenoble

LE LIMOS ET L'ÉCOSYSTÈME CLERMONTOIS AU CŒUR DE LA RECHERCHE NATIONALE EN SÉCURISATION DES RÉSEAUX

— Le thème Réseau et Sécurité (RS) du **laboratoire *LIMOS* à Clermont-Ferrand** est dédié d'une part aux questions liées **aux aspects protocolaires de transmission et d'acheminement des données dans les réseaux (principalement, les réseaux sans fil et IoT)**, et d'autre part **à la sécurité de ces protocoles et services**. Les travaux menés au sein de ce thème peuvent se résumer comme suit :

- **La conception de protocoles de communication et d'algorithmes distribués** pour les réseaux de communication.
- **La sécurisation et l'amélioration de la résilience des réseaux et des protocoles de communication**. Les travaux de recherche se concentrent sur la conception et la validation de protocoles sécurisés ou garantissant des propriétés de résilience. L'usage de méthodes formelles permet de concevoir des protocoles sûrs avec ProVerif et Tamarin. Autre domaine de recherche clé : l'évaluation de l'efficacité des systèmes de détection d'intrusion (IDS) basés sur l'apprentissage automatique (Machine Learning) dans des environnements réseau réels.
- **La conception de primitives cryptographiques**

ESYNOV : UNE PLATEFORME TECHNOLOGIQUE D'EXCELLENCE À VALENCE

— ***Esynov* est la plateforme technologique de Grenoble *INP-Esisar* (Valence, Drôme)**, spécialisée depuis 1996 sur les thématiques du système embarqué : CEM, Radio Fréquence, cybersécurité produit, logiciel et informatique, à travers des actions de formation, de recherche et de transfert technologique.

— Dans le cadre d'une collaboration avec un industriel, la vocation d'une plateforme technologique est de mobiliser ses moyens de laboratoires et la compétence de ses experts au profit de l'entreprise pour qu'elle monte en compétences, à travers **des projets de R&D et de pré-industrialisation**.

— *Esynov* est référencée comme expert auprès de programmes comme Industrie du Futur (ENE), les entreprises ont donc des financements de la Région Auvergne-Rhône-Alpes pour mener leurs diagnostics et pentests.

Plateaux techniques cybersécurité proposés par ESYNOV

CYBERSECURITÉ PRODUIT

- Analyse de risques
- Modélisation de menaces
- Normatif - Gap analysis
- Pentest Produit

Réalisations cybersécurité des produits :

- Diagnostic Produit sur des instruments industriels de mesure (états des lieux, préconisation d'actions prioritaires)
- Pentests de Produits pour les dossiers de certification / marquage CE
- Revues de Sécurité et aide aux choix d'architecture, le développement de protocoles radios, etc.
- Formations sur mesure de "Security by Design"

CYBERSECURITÉ IT

- Sécurité des systèmes et infrastructures
- Gestion des identités et des accès
- Évaluation de sécurité IT

Réalisations cybersécurité IT :

- Audits de Sécurité des infrastructures pour PME industriels et collectivités
- Pentests d'applications métiers dans le médical
- Formation niveau avancé dans le nucléaire
- Sensibilisation à grande échelle dans l'industrie agroalimentaire

Les Pentest (Tests d'intrusion) proposés par Esynov :

- Cybersécurité IT : pentests pour des collectivités, PME, ateliers de production...
- Cybersécurité Produit : collectivités, PME, ateliers de production, dossiers de certification de Dispositifs Médicaux certifiés aux USA"

Formations et diagnostics cyber

- **Formation Cybersécurité Produit** et **Diagnostic Cyber Produit** : la formation sur les Dispositifs Médicaux est issue d'une collaboration avec Medicalps et celle sur la mobilité avec CARA.
- **Cybersécurité SI** et **Diagnostic Cyber PME** - plusieurs dizaines de stagiaires par an (collectivités, services, industrie, PME, grands groupes...).

Source : Grenoble INP ESISAR, ESYNOV, LCIS Valence

L'ACCOMPAGNEMENT DES ENTREPRISES

PRÉSENTATION DE L'ÉCOSYSTÈME CYBER RÉGIONAL

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

— **L'ANSSI** est l'autorité nationale en matière de cybersécurité et de cyberdéfense en France en charge de coordonner le champ de la défense et de la protection des systèmes d'information.

— **Représentants officiels de l'ANSSI dans les territoires, les délégués territoriaux** ont pour missions d'irriguer tous les services de l'Agence des réalités locales en matière de sécurité numérique, de démultiplier l'action de l'ANSSI sur le terrain, et de catalyser les initiatives cyber pertinentes dans leur contexte territorial.

— En synergie avec les services déconcentrés de l'État, animateurs d'un collectif composé de multiples acteurs institutionnels et économiques, ils agissent pour permettre aux forces vives de chaque territoire de progresser en matière de prévention, de réaction et de résilience cyber.

MINALOGIC : le pôle de compétitivité de la transformation numérique en Auvergne-Rhône-Alpes

— Créé en 2005, le pôle de compétitivité Minalogic Auvergne-Rhône-Alpes est le moteur de la transformation numérique, au service des enjeux stratégiques de réindustrialisation, de souveraineté nationale et de développement durable.

— Le pôle anime un écosystème de **450 adhérents**, dont **380 entreprises** couvrant l'ensemble de la chaîne de la valeur du numérique, 17 organismes de recherche et de formation réunissant plus de 150 laboratoires, des collectivités territoriales, des investisseurs privés et des prestataires de service.

— Minalogic accélère les mises en relations qualifiées entre ces acteurs et booste leurs projets d'innovation et de business, en France, en Europe et à l'international.

— S'appuyant sur l'expertise reconnue de son équipe d'animation, l'offre de services de Minalogic repose sur trois missions complémentaires :

- L'animation d'un réseau d'innovation régional d'ambition internationale,
- L'accompagnement de projets d'innovation,
- Et la valorisation de l'expertise technologique de l'écosystème.

Le Campus Région du numérique

— Le Campus Région du numérique, situé à Charbonnières-les-Bains dans l'ouest lyonnais, est une initiative stratégique portée par la Région Auvergne-Rhône-Alpes pour accélérer la transformation numérique du territoire.

— Ouvert en 2021, il réunit sur un même site un large écosystème d'écoles, d'entreprises, de laboratoires d'innovation, de clusters et de pôles de compétitivité. Des bureaux, des services, des espaces événementiels sur 14 500 m² et 3 bâtiments constituent un lieu vivant, mixte et collaboratif au service des professionnels, des étudiants et des acteurs publics.

— Le Campus poursuit une mission structurée autour de plusieurs objectifs majeurs :

- **Former aux métiers du numérique** : en tant que site multi-écoles, accueillant 900 étudiants dans des domaines variés du numérique (développement, cybersécurité, industrie 4.0...) et en tant que pilote d'un label régional, il vise ainsi à répondre au manque de main-d'œuvre qualifiée et aux besoins actuels et futurs des entreprises.
- **Stimuler l'innovation numérique et industrielle** : le Campus abrite une usine digitalisée grandeur nature, conçue pour expérimenter l'industrie 4.0, des plateformes d'innovation tournées vers les nouvelles technologies et des espaces permettant aux entreprises de tester outils et méthodes.
- **Accompagner la digitalisation des entreprises** : à travers un portail web de digitalisation, un réseau d'acteurs et des événements, le Campus aide dirigeants et salariés à découvrir et intégrer les technologies numériques, améliorer les performances de leur organisation et à s'adapter aux transitions imposées par le numérique, à commencer par l'IA.

DIGITAL LEAGUE : le cluster des entreprises du numérique en Auvergne-Rhône-Alpes

— **Digital League** est le **cluster des entreprises du numérique en Auvergne-Rhône-Alpes**. Dans un contexte de menaces plus fréquentes et plus complexes, Digital League mobilise son réseau pour aider les organisations à mieux protéger leurs activités, leurs données et leurs infrastructures.

— Digital League produit également des contenus (livres blancs, guide, newsletter cyber) et propose des formations tout au long de l'année.

L'ADIRA : l'association pour le Digital et l'IT en région Auvergne-Rhône-Alpes

— Née en 1969, l'**ADIRA** rassemble plus de **500 organisations**, dont 2 300 collaborateurs membres de 22 groupes de travail. En parallèle des sessions de groupes de travail et évènements hebdomadaires, elle propose une veille innovation & startups, des liens avec les acteurs de l'enseignement et des contenus spécifiques à la région (études, Benchmark DSI...).

— La Cybersécurité demeure un des enjeux principaux traités par l'association via des retours d'expériences, des sessions de groupe croisées, la constitution d'un annuaire dédié et une veille sur les pratiques des Directions SI régionales.

Le Hub des Sécurités - CSIRT Territorial d'Auvergne-Rhône-Alpes

— **Le CSIRT-Territorial Auvergne-Rhône-Alpes**, porté par la ***CCI Lyon Métropole Saint-Étienne Roanne*** et implanté au sein du Hub des Sécurités d'Écully (Rhône), assure la prévention, la qualification et l'endiguement des incidents de cybersécurité, avec un numéro d'appel gratuit. **Ouvert aux entreprises, associations et collectivités d'Auvergne-Rhône-Alpes**, il fournit un accompagnement structuré, adapté aux capacités des structures de toutes tailles. Il renforce l'accompagnement local aux enjeux de cybersécurité.

— L'installation du CSIRT-Territorial s'inscrit dans la dynamique du **Hub des Sécurités**. Ce dernier fédère sur un même site des acteurs de la formation, des entreprises spécialisées en matière de sécurité globale et des services de l'Etat. Il réunit des acteurs complémentaires et favorise la mutualisation des compétences, l'échange de pratiques et la montée en compétence des organisations présentes en son sein. Il permet ainsi une meilleure anticipation et gestion des risques et des crises.

— Le CSIRT-Territorial s'insère dans un réseau structuré composé d'acteurs régionaux et nationaux (ANSSI, CERT-FR, 17Cyber, Campus Région du numérique, etc.), garantissant une coordination opérationnelle fluide.

Les 13 Chambres de Commerce et d'Industrie d'Auvergne-Rhône-Alpes, et la CCI de région

— **Les CCI d'Auvergne-Rhône-Alpes** mènent une action structurée en cybersécurité reposant sur 3 piliers complémentaires :

- **Sensibilisation et formations des entreprises**
- **Diagnostics de premier niveau via le dispositif national "Cyber Départ"** (ANSSI)
- **Diagnostics cybersécurité approfondis** (CCI & EEN)

— Ces actions permettent d'offrir au territoire une réponse complète : prévention, diagnostic, montée en compétence, mise en action et suivi.

L'ENE : Les Experts du Numérique en Entreprise

— L'ENE a pour mission d'**améliorer la compétitivité et favoriser l'innovation des PME et TPE d'Auvergne-Rhône-Alpes en développant l'usage du numérique** en totale neutralité avec les prestataires :

- Informer pour une meilleure compréhension des usages numériques
- Accompagner la mise en œuvre de projets numériques y compris cyber
- Anticiper les usages émergeants à forte valeur ajoutée
- Partager les bonnes pratiques entre pairs

CLUSIR : Le Club de la Sécurité de l'Information en Région Auvergne Rhône-Alpes

— **Le CLUSIR Auvergne Rhône-Alpes** est une association de bénévoles dont l'objet est de contribuer, sur un plan local, à la diffusion d'une culture de la sécurité de l'information et des bonnes pratiques associées.

— Afin de participer à cet objectif, le CLUSIR réunit les acteurs de la cyber (experts, utilisateurs, offreurs, autorités, étudiants, etc.) comme toutes personnes intéressées par celle-ci dans le cadre de trois clubs (Cf. P. 34) ainsi que de différents évènements (CSI, Journées de la Cyber, etc.).

— Avec plus d'une quinzaine de rencontres par an et plus de 300 membres passionnés, le CLUSIR se veut depuis 2004 l'association de référence en matière de cybersécurité sur le territoire de la Région Auvergne-Rhône-Alpes.

CLUSTER EDEN : Le cluster des PME de la défense, de la sécurité et de la sûreté

— Créé à Lyon en 2008 avec le soutien de la DGA et des CCI, **le Cluster EDEN** réunit aujourd'hui plus de 200 PME et ETI stratégiques **dans les secteurs de la défense, sécurité et sûreté**, partout en France, via 5 pôles régionaux.

— Véritable levier de la base industrielle et technologique de défense (BITD), EDEN favorise les synergies entre ses adhérents, renforce leur visibilité internationale et leur développement capacitaire et technologique, offrant une réponse globale aux donneurs d'ordre.

— Il met en relation ses membres avec des acteurs économiques et institutionnels clés afin de créer des opportunités concrètes de croissance et de collaboration.

Linksium et Pulsalys : sociétés d'accélération de transfert de technologies (SATT)

— **Linksium et Pulsalys font partie du réseau des 13 SATT** françaises spécialisées **sur les phases amont des projets d'innovation technologique** (notamment cyber).

— Linksium est membre fondateur du Pôle universitaire d'innovation (PUI) porté par l'Université Grenoble Alpes.

LES DISPOSITIFS D'ACCOMPAGNEMENT CYBER RÉGIONAUX

Le dispositif MinaSmart et le Parcours Cybersécurité

— Minasmart est un dispositif européen porté par 13 partenaires régionaux qui a pour ambition d'accompagner les PME traditionnelles de la région dans leur démarche de transformation numérique.

— **Le Parcours Cybersécurité de MinaSmart** aide les TPE, PME et ETI à **sécuriser leurs actifs numériques et leur propriété intellectuelle** via une démarche simple, pragmatique et progressive en 3 volets : évaluation, planification et accompagnement opérationnel.

- Audit déclaratif en ligne
- Analyse et diagnostic complet multi-niveaux des risques et plan d'action (plan de remédiation)
- Facilité de financement du plan de remédiation par des partenaires bancaires

— Ce parcours est conçu pour être facile à déployer, adapté à la maturité de l'entreprise et peut être cofinancé jusqu'à 50 % (sous certaines conditions) dans le cadre de Minasmart.

Conseil Performance Industrie du Futur - volet Numérique

— La thématique cybersécurité est traitée dans le cadre du dispositif de la Région Auvergne-Rhône-Alpes « **Industrie du Futur** » géré par l'Agence Auvergne-Rhône-Alpes-Entreprises et l'ENE. Parmi les axes du programme, l'axe Piloter / Usine Numérique ou connectée comporte un volet « **Sécurité des données et Cybersécurité** » pour sécuriser l'accès de l'information de l'entreprise.

— Les entreprises régionales peuvent bénéficier de la prise en charge de diagnostics et plan d'action (5 à 20 jours de conseil par des experts, prise en charge à 50 % sous forme de subvention plafonnée à 16 000 € HT).

— **Critères d'éligibilité** : Entreprise industrielle ou avec une activité de production (5 à 5 000 salariées) ayant leur siège social en Auvergne-Rhône-Alpes et un projet informatique / Numérique autour de la production.

Retrouvez la plaquette de présentation d'Industrie du Futur en scannant le QR Code ci-joint

Les dispositifs d'accompagnement des entreprises mis en œuvre par le Campus Région du numérique

— **Le Campus Région du numérique** intègre depuis 2025 une **fonction d'animation de la thématique cybersécurité** au niveau régional, dans la continuité de la stratégie régionale adoptée par la Région Auvergne-Rhône-Alpes. Ces opérations ont comme fil rouge de faire du site de Charbonnières-les-Bains le l**ieu totem de la cybersécurité en région** et d'y **développer un Campus Cyber territorial.**

— L'action du Campus se déploie d'abord dans des actions de sensibilisation : édition de documents, insertions de séquences de sensibilisation cyber dans des évènements économiques et numériques. De même, dans le cadre de son action d'information au service de la digitalisation des entreprises, le portail web regroupe des contenus, liste des dispositifs et recense des évènements dédiés à la cybersécurité des entreprises. Un dossier spécial cybersécurité centralise ces informations : https://campusnumerique.auvergnerhonealpes.fr/dossier-special/cybersecurite/.

— En tant que lieu carrefour du numérique, le Campus abrite plusieurs structures intervenant sur la cybersécurité et met à leur disposition ses espaces de travail, de convivialité et d'évènementiel. Il accueille également les **principaux évènements dédiés** à la thématique en région Auvergne-Rhône-Alpes : **Journées de la Cyber, Challenges Sécurité de l'Information, Rempar25**...

— Pour honorer son activité de « campus », il accueille plusieurs **formations dédiées** à la **sécurité des réseaux et des usages informatiques**. Cette juxtaposition de structures de recherche, d'étudiants et de structures d'accompagnement fait du Campus Région du numérique un carrefour pour la formation et l'innovation.

— Les espaces sont accessibles aux entreprises de cybersécurité qui souhaitent s'installer au cœur de cet écosystème. Résidentes du Campus, elles bénéficient alors des évènements, infrastructures et réseaux.

— Enfin, les espaces cyber du Campus sont dotés de salles spécifiques :

- **une salle de gestion de crise**, équipée de moyens de visio, de captation et de streaming à des fins d'exercice et de formation ;
- **une salle de TP cyber,** installée comme un SOC de 28 places avec un mur d'écrans pour des exercices, des formations et de la sensibilisation via des serious games ;
- **un amphithéâtre de 70 places** pour des réunions et présentations.

— Pour finir, grâce à ses plateformes industrielles et ses consortia, le sujet de la cybersécurité industrielle est au cœur de la dynamique Campus.

Source : Campus Région du numérique

ZOOM SUR LA CYBERSÉCURITÉ INDUSTRIELLE AVEC L'USINE DU CAMPUS RÉGION DU NUMÉRIQUE

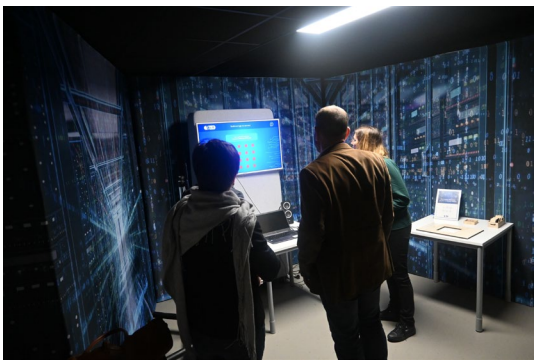
— Située au cœur du **Campus Région du numérique**, à Charbonnière-les-Bains, **l'Usine est un démonstrateur unique dédié à l'industrie 4.0.** Grâce à ses espaces immersifs, ses équipements à l'échelle 1 et ses environnements numériques avancés, l'Usine permet aux entreprises de s'acculturer et de monter en compétences sur les enjeux de transformation industrielle, dont la cybersécurité, devenue essentielle pour la compétitivité et la résilience des organisations.

Au sein de l'Usine, **les plateformes technologiques SWARM et DIWII** jouent un rôle essentiel dans **l'accompagnement des entreprises sur les enjeux de cybersécurité industrielle**, en combinant accompagnement stratégique, mise en pratique et montée en compétences.

SWARM : un tiers-lieu dédié à la maturation cyber des industriels

— SWARM accompagne les entreprises industrielles dans la compréhension et la structuration de leur cybersécurité. Son offre s'articule autour de quatre axes principaux :

- **Sensibilisation et acculturation**
  - Sensibilisation des dirigeants et équipes,
  - Dispositifs pédagogiques immersifs (escape game cybersécurité),
  - Animation de communautés et temps collectifs.
- **Démonstration et expérimentation**
  - Accès à des équipements industriels connectés,
  - des environnements représentatifs des réalités industrielles,
  - des démonstrateurs cybersécurité en conditions quasi réelles.
- **Diagnostic et évaluation de maturité** SWARM propose des diagnostics cybersécurité structurés, permettant :
  - Une évaluation objective du niveau de maturité,
  - L'identification des failles et axes de progrès,
  - Une base de travail partagée avec l'écosystème.
- **Test before invest / aide à la décision** Le dispositif « test before invest » permet de :
  - Tester des cas d'usage avant déploiement,
  - Réduire les risques d'investissement,
  - Orienter les entreprises vers des solutions adaptées et valider le ROI.



DIWII : démonstrateur physique grandeur nature de l'industrie 4.0

— Portée par Mines Saint-Étienne, la plateforme DIWII recrée l'environnement d'une PME de l'Industrie du Futur afin de permettre l'expérimentation et la formation. Elle mobilise des équipements industriels et numériques de haut niveau pour proposer une offre complète dédiée à la cybersécurité industrielle :

- **Sensibilisation aux risques cyber** : ateliers concrets d'expérimentation pour comprendre et initier une démarche cyber (état de la menace, les vulnérabilités industrielles, les bonnes pratiques, les principes de sécurisation...
- **Formations** :
  - Programme de formation continue sur des méthodes de diagnostic, l'analyse des failles, la mise en œuvre de mesures de protection adaptées aux environnements industriels.
  - Programmes diplômants « **managers de la cybersécurité industrielle** » et « experts en convergence IT et OT ».
- **Recherche et transfert technologique** :
  - Accompagnement pour lever les verrous technologiques et accélérer le transfert d'innovation vers les entreprises, y compris PME/TPE.
  - Accueil de travaux de recherche en réseaux, cybersécurité et intelligence artificielle.

Sources : SWARM, DIWII, Campus Région du numérique

LES DISPOSITIFS D'ACCOMPAGNEMENT CYBER NATIONAUX

17 CYBER : service public d'assistance en ligne gratuit pour les victimes de cybermalveillance

— Le **17Cyber.gouv.fr** est un service public d'assistance en ligne gratuit pour les victimes de cybermalveillance (particuliers, entreprises et collectivités), proposé par la Police nationale, la Gendarmerie nationale et Cybermalveillance.gouv.fr. Le module 17Cyber est notamment accessible via le portail web du Campus Région du numérique.

— **À travers un parcours numérique facilité et disponible 24h/24 et 7J/7**, 17Cyber propose aux victimes de cybermalveillances (virus, hameçonnage, arnaque bancaire...) de les assister face à la menace dont ils font l'objet (outil de diagnostic, recommandations personnalisées et assistance technique).

MON EXPERT CYBER : mise en relation avec des prestataires pour la sécurisation des systèmes d'information professionnels

— **Mon ExpertCyber** propose une mise en relation avec des prestataires de confiance labellisés ExpertCyber (par l'AFNOR) et qualifiés pour accompagner les TPE-PME, association, collectivité ou administration dans la **sécurisation de leurs systèmes d'information professionnels**.

— Le label ExpertCyber est ainsi un gage de qualité pour les organisations qui peuvent en attendre :

- un niveau d'**expertise et de compétences** en sécurité informatique
- un **conseil de qualité** pour prévenir la survenue d'actes de cybermalveillance et sécuriser leurs installations informatiques ;
- une **conformité administrative** (respect du cadre législatif et réglementaire, traitement des données personnelles conforme au RGPD...) ;
- un **sens de l'intérêt général** (veille et remontée d'incidents, conservation de la preuve numérique...).

SENS CYBER : programme de e-sensibilisation à la cybersécurité de cybermalveillance.gouv

— **Cybermalveillance.gouv.fr** a lancé **SensCyber**, une **e-sensibilisation à la cybersécurité gratuite et accessible à tous** (particuliers, collaborateurs des TPE/PME et agents de la fonctions publiques).

— Composé de **définitions illustrées, de quiz ou encore de séquences interactives**, le programme est construit autour de 3 modules :

- **Comprendre** les cyberattaques les plus courantes, leur fonctionnement et les risques encourus par les individus dans la sphère privée comme professionnelle ;
- **Agir** pour s'approprier les bonnes pratiques et les bons réflexes dans les usages du quotidien (téléphone portable, réseaux sociaux, usages pro-perso...) ;
- Apprendre à **transmettre** ces connaissances et bonnes pratiques avec son entourage pour une meilleure protection collective et identifier les acteurs publics à contacter en cas d'attaques.

Le diagnostic Cyberdépart de l'ANSSI

— **Le diagnostic Cyberdépart de l'ANSSI est un diagnostic cyber gratuit accompagné par un Aidant cyber** pour améliorer la cybersécurité des TPE/PME, collectivités, ou associations avec au moins deux salariés. En 1h30 seulement **6 recommandations prioritaires** faciles à mettre en œuvre sont formulées pour commencer à se protéger contre les cyberattaques.

— Un **Aidant cyber** accompagne bénévolement, de façon neutre, confidentielle et bienveillante, pour évaluer la cybersécurité de l'organisation et proposer des actions concrètes, accessibles et sans jargon technique. C'est un tiers de confiance, issu d'un organisme public ou adhérent d'une association à but non lucratif en lien avec le numérique, spécialement formé sur le diagnostic cyber par l'ANSSI.

LES CLUBS ET RÉSEAUX DE LA FILIÈRE CYBERSÉCURITÉ EN AUVERGNE-RHÔNE-ALPES

DIGITAL LEAGUE : le Club Experts Cyber

— *MDigital League* fédère et anime la filière au travers d'une série d'événements dédiés et grâce à son **Club Experts Cybersécurité**, un espace d'échanges entre pairs sur l'évolution des menaces, les solutions et les bonnes pratiques.

— L'objectif ? **Structurer la filière régionale et élever le niveau de cybersécurité des acteurs économiques**, TPE, PME-PMI, ETI, associations et collectivités, souvent les plus exposés et les moins armés.

Retrouvez toutes les actions, événements, contenus et formations proposées en lien avec la cybersécurité ainsi que les modalités de participation au Club Experts Cyber de DIGITAL LEAGUE en scannant le QR Code ci-joint

CLUSTER EDEN : Le Groupe de Travail (GT) Sûreté, Infrastructures et Cybersécurité

— Parmi les 7 groupes de travail du Cluster EDEN, l**e GT Sûreté Infra & Cyber** se concentre autour d'entreprises expertes en protection globale : **audit et analyse de risque, cybersécurité, contrôle d'accès, surveillance et gestion de crise**.

— L'objectif est de fournir une offre intégrée, souveraine et conforme qui couvre l'ensemble des besoins liés à la protection des infrastructures critiques et des systèmes d'information.

— Les domaines de compétences au sein de ce groupe de travail :

- **Audit, analyse de risque et investigation** pour établir un diagnostic précis.
- **Veille, surveillance et e-réputation** pour détecter signaux faibles et menaces.
- **Sensibilisation, conseil et formation** pour développer une culture sécurité durable.
- **Ingénierie et accompagnement** pour déployer des solutions adaptées.
- **Détection et protection** contre les intrusions physiques et cyber.
- **Contrôle d'accès** pour sécuriser les sites sensibles.
- **Maintenance opérationnelle** des systèmes de sûreté.
- **Gestion de crises** avec procédures et cellules de réponse dédiées.

CLUSIR Auvergne-Rhône-Alpes : 3 clubs autour de la sécurisation des systèmes d'information

— **Le Club SSI, pour Sécurité des Systèmes d'Information**, est le principal club du CLUSIR. Y sont développées lors de ses réunions différentes thématiques de sécurité de l'information, définies par ses membres en début d'année, qu'il s'agisse par exemple de sécurité des systèmes d'IA, de sécurité des systèmes industriels, d'espionnage en entreprise, de cybersécurité offensive, etc.

— **Le Club EH RM, pour Ethical Hacking Root-Me pro**, a pour objectif de permettre à des personnes bénéficiant d'un premier niveau de compétences techniques en matière de cyber d'entretenir voire de développer celles-ci au cours d'exercices pratiques animés par l'équipe de Root-Me pro et réalisés sur la plateforme éponyme. L'idée de ce club est de donner l'occasion à ses participants de se mettre dans la peau d'un acteur cybermalveillant afin d'être en mesure de mieux en anticiper les actions.

— **Le Club IE/OSINT, pour Intelligence Economique et Open Source INTelligence**, aborde la SSI sous l'angle de la gestion de l'information au sens large. Il s'organise autour de sessions Intelligence Economique ponctuelles et de sessions OSINT trimestrielles. Les premières peuvent aborder toute thématique d'intelligence économique en matière de cyber (souveraineté, financement, actualité juridique, etc.) là où les secondes se concentrent sur des retours d'experts en recherche d'information en sources ouvertes.

L'ADIRA : Les Groupes de Travail (GT) RSSI et CYBER

— **GT Cybersécurité** : Avec une approche pluridisciplinaire, ce groupe veille aux évolutions des menaces et pratiques cyber. Il traite des enjeux liés aux nouvelles technologies de défense, aux pratiques de remédiation, de gestion de crise et de gouvernance de la SSI. Il sensibilise les adhérents de l'association à travers des sessions croisées de groupes, livrables ou encore tables rondes. Les membres du groupe de travail peuvent être des DSI, RSSI, experts Cyber, juristes et tous autres experts de la cybersécurité.

— **GT RSSI** : Le groupe de travail RSSI propose de traiter les problématiques liées à la SSI aussi bien sur les axes technologiques, organisationnels ou de gouvernance. Comme son nom l'indique, le groupe de travail est à destination uniquement des RSSI ou assimilés. C'est un lieu d'échange sur les bonnes pratiques de sécurité et les retours d'expériences des uns des autres : gouvernance, gestion des risques, conformité, veille technologique, sensibilisation à la SSI..

LES GRANDS ÉVÉNEMENTS ANNUELS CYBER EN REGION

— **Les Journées de la Cyber** sont un événement régional majeur dédié à la cybersécurité, co-organisé par l'ADIRA, le CLUSIR Auvergne-Rhône-Alpes, Digital League, l'ENE – les Experts du Numérique en Entreprises – et Minalogic.

— L'objectif de l'événement, qui rassemble plus de **500 participants**, est de permettre aux décideurs publics, aux dirigeants d'entreprises de toutes tailles et de tous secteurs d'activité, aux experts en cybersécurité et aux acteurs de la transformation numérique de mieux **comprendre les enjeux actuels, de maîtriser les risques, de découvrir des solutions, de partager des retours d'expérience**.

— L'événement combine keynotes, conférences, tables rondes, ateliers pratiques, sessions de networking et moments conviviaux autour de thématiques concrètes : menaces émergentes, bonnes pratiques, aspects réglementaires et de gouvernance, résilience, innovations et échanges entre professionnels.

— Lyon Cyber Expo s'affirme comme **le rendez-vous business de référence de la confiance numérique** au cœur de la 2e région économique de France. C'est : 2 jours, 160 exposants, 30 conférences, 90 speakers.

— Cet événement réunit toute la chaîne de valeur de la cybersécurité autour de trois piliers critiques :

- Gouverner les risques
- Protéger les actifs stratégiques
- Répondre avec efficacité en cas de crise pour garantir la continuité de l'activité.

— L'évènement des **Challenges de la Sécurité de l'Information, ou CSI, consiste en une journée de rencontres et de challenges transverses en matière de sécurité de l'information**. Cette journée est ainsi construite autour de trois mises en pratique :

- **Deux compétitions, lots** à la clé, sous forme de CTF (Capture The Flag) organisés en parallèle, l'un en matière d'ethical hacking et l'autre en matière d'OSINT ;
- **Un exercice de gestion de crise cyber**

— Adressée autant aux **étudiants qu'aux professionnels, cette journée vise également à favoriser les rencontres entre ceux-ci**.

— Désormais coorganisés par le CLUSIR et le Campus Région du numérique, les CSI ne cessent de réunir de plus en plus de participants et sont déjà l'un des évènements majeurs de la cyber en région.

— CSAW (Cyber Security Awareness Week) **est la plus grande compétition académique de cybersécurité** dans le monde. **Objectifs** :

- Sensibiliser le grand public aux enjeux de la cybersécurité
- Créer des vocations chez les plus jeunes
- Réunir les plus grands talents européens de la cybersécurité
- Créer des synergies entre la recherche, les entreprises et les étudiants.

— **Grenoble INP – Esisar** (Valence) **organise depuis 9 ans les finales européennes de CSAW** au sein de son école.

— **Intervenants** : 125 finalistes dont 80 en présentiel, 50 partenaires (industriels et institutionnels), 20 juges experts

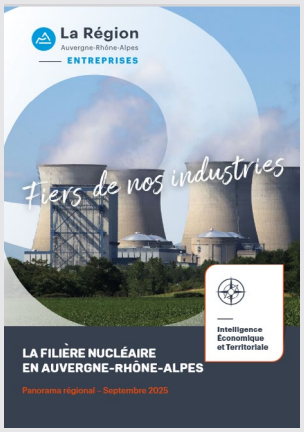
— **Participants** : 50 participants au Cyberday, 80 étudiants participants aux Workshops des partenaires

— **Visiteurs** : 200 scolaires (primaires, collèges, lycées)

— **Staff** : 100 élèves mobilisés et 40 personnels mobilisés

La Région
Auvergne-Rhône-Alpes
ENTREPRISES

Fiers de nos industries



À retrouver sur la plateforme d'informations économiques du pôle :

https://plateforme-iet.auvergnerhonealpes-entreprises.fr/

Nos partenaires

La Région Auvergne-Rhône-Alpes · Campus Région du Numérique · Minalogic · Digital League Auvergne-Rhône-Alpes · ene experts du numérique en entreprises Auvergne-Rhône-Alpes · adira · CLUSIR Auvergne-Rhône-Alpes · CCI Lyon Metropole Saint-Etienne Roanne · CCI Auvergne-Rhône-Alpes · Le Hub des sécurités · EDEN Defense Security Safety Cluster France · Cyber Malveillance .gouv.fr Assistance et prévention en sécurité numérique · SWARM · cea · DIWII · esynov by Grenoble INP - Esisar, UGA · Linksium technology transfer & startup building Grenoble Alpes · LIMOS · Fédération Informatique de Lyon · Cybersecurity Institute Univ. Grenoble Alpes · La French Tech Saint-Etienne Lyon

Sources complémentaires

CLUSIF · CESIN · ACN Alliance pour la confiance numérique · Cyber Cercle Auvergne-Rhône-Alpes · HEXATRUST Cloud Confidence & Cybersecurity · In Cyber Forum Europe

Réalisé par :
Corentin Bonnefois
Analyste sectoriel et territorial

Carine DUWAT
Responsable Intelligence Economique et Territoriale
cduwat@arae.fr

Avec le soutien de :
Hervé Mialon
Référent Sécurité des Systèmes d'Information
hmialon@arae.fr

AUVERGNE-RHÔNE-ALPES ENTREPRISES
30 Quai Perrache, Immeuble Empreinte - 69002 Lyon
auvergnerhonealpes-entreprises.fr

Développement économique · Emploi / Formation · Europe · Innovation · International · Intelligence Économique et Territoriale

INVEST IN Auvergne-Rhône-Alpes