La Région
Auvergne-Rhône-Alpes
ENTREPRISES

Fiers de nos industries

Intelligence Économique et Territoriale

LA FILIERE DE LA CYBERSÉCURITÉ EN AUVERGNE-RHÔNE-ALPES

Panorama régional - Mars 2024

PRÉAMBULE

— Ce document a été réalisé par le pôle Intelligence Économique et Territoriale (IET) d'Auvergne-Rhône-Alpes Entreprises en partenariat avec le pôle de compétitivité Minalogic, le Commissariat à l'Energie Atomique (CEA Grenoble), l'Association pour le digital et l'IT en Auvergne-Rhône-Alpes ADIRA, le CLUSIR Auvergne-Rhône-Alpes (Club de la Sécurité des Systèmes d'Information Régional), le cluster des entreprises de l'industrie du numérique Digital League, le Campus Région du numérique et les Experts du Numérique en Entreprises, l'ENE.

— Il a pour vocation de brosser un portrait régional des acteurs de la filière cybersécurité en s'appuyant sur une compilation de données et d'informations issues de sources variées, et de données produites par le pôle IET et ses partenaires.

— L'objectif de ce panorama est de valoriser les acteurs et les compétences régionales, et de montrer le poids économique de la filière 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 d'Auvergne-Rhône-Alpes-Entreprises.

— Les données sont issues de :
- l'extraction d'une liste d'entreprises de la base de données Diane+ sur la base des mots-clés : cybersécurité, pentest, sécurité informatique, SOC, intrusion, incident, audit technique, analyse des risques, chiffrement, cryptologie ;
- la liste des membres du CLUSIR Auvergne-Rhône-Alpes ;
- le panorama Intelligence Artificielle du pôle IET d'Auvergne-Rhône-Alpes Entreprises ;
- l'annuaire Cybersécurité de l'ADIRA ;
- l'annuaire Cybersécurité de Solutions Numériques.com ;
- l'annuaire des prestataires du numérique régionaux d'Auvergne-Rhône-Alpes Digital : https://www.auvergnerhonealpes.digital/
- les entreprises régionales accompagnées par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- la veille informationnelle réalisée par le pôle IET (presse quotidienne régionale, nationale et spécialisée) ;
- la liste des exposants régionaux aux salons FIC 2023, INCYBER 2024, Assises de la Cybersécurité.

PÉRIMÈTRE

— Dans ce panorama, nous considérons la cybersécurité au sens large, c'est-à-dire l'ensemble des entreprises qui relèvent de la protection 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 couverts dans ce panorama : Gouvernance, Défense, Protection et Résilience/Remédiation.

— Sont ciblées par cette étude, les entreprises ayant leur siège ou disposant d'au moins un établissement secondaire en Auvergne-Rhône-Alpes et étant des unités employeuses.

— 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 assureurs et les cabinets d'avocats spécialisées en cybersécurité ont également été exclus du recensement.

SEGMENTATIONS RETENUES

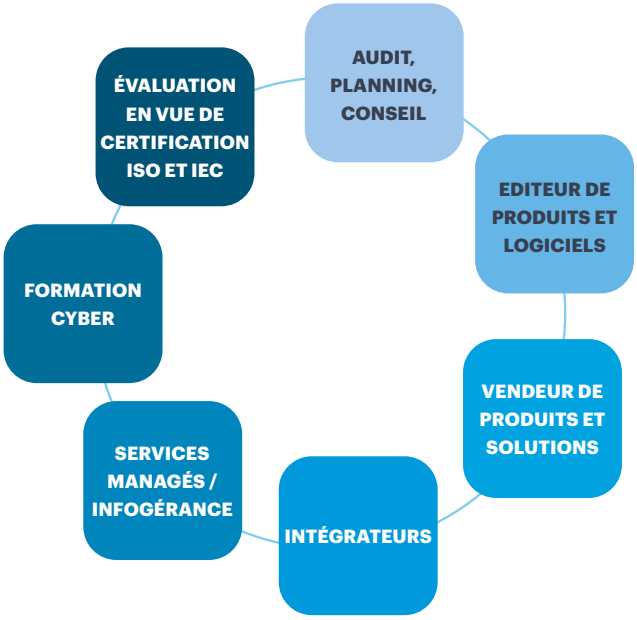
— Les entreprises ont été qualifiées selon leur(s) expertises parmi les quatre grands champs d'intervention de la cybersécurité, leurs expertises, les domaines d'applications de leurs produits ou services délivrés.

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 les déclarations de plusieurs responsables d'entreprises captées dans la presse ainsi que les informations de qualification issues de l'annuaire Cybersécurité.

CHAÎNE DE VALEUR ET MARCHÉS D'APPLICATION

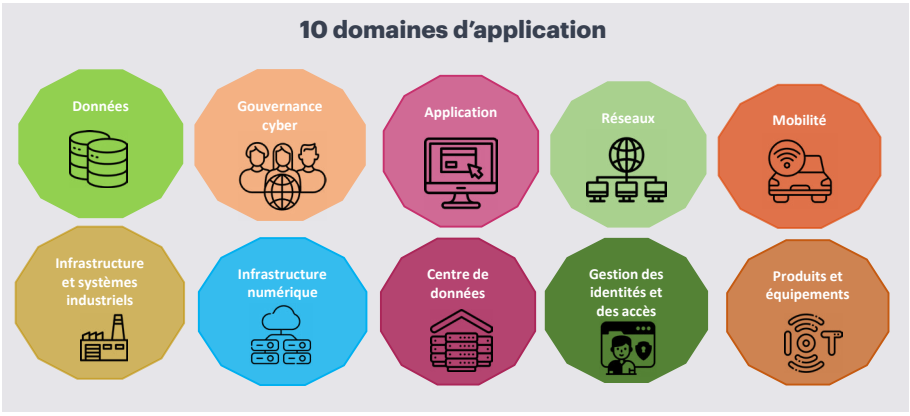
Activité principale des établissements cybersécurité en Auvergne-Rhône-Alpes



Expertise (s) maitrisée(s) par les établissements cybersécurité en Auvergne-Rhône-Alpes

GOUVERNANCE	PROTECTION	DÉFENSE	RÉSILIENCE
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	

10 domaines d'application



Certifications et qualifications

- PASSI / LPM RGS
- PACS / PRIS / PDIS / PVID / PAMS / CESTI
- SecNumCloud
- PSCo (ClubPSCo)
- CSPN
- CC (European Cybersecurity Scheme on Common Criteria (EUCC) – enisa)
- AICPA-SOC
- ISO 9001
- ISO 27001
- ISO 22301
- IEC 62443 (Industrial Cyber)
- EIDAS

Labellisations

- Label France Cyber Security
- Expert Cyber (AFNOR)
- Cybersecurity Made in Europe

Adhésion

- Fédération française de la cybersécurité

L'ESSENTIEL

— La filière de la cybersécurité en Auvergne-Rhône-Alpes est concentrée sur la métropole de Lyon avec près de **56 %** des établissements implantés au sein de la zone d'emploi lyonnaise.

— Près de **29 établissements** sont spécialisés dans les infrastructures et systèmes industriels, une véritable spécialisation régionale.

— Les cabinets d'audits, de conseil et de conformité représentent le plus grand contingent d'acteurs en région (**118 établissements**) devant les intégrateurs de solutions technologiques (**79**) et les éditeurs de produits et logiciels (**65**).

— Les principaux domaines d'application pour les acteurs de la cybersécurité sont l**a sécurité des infrastructures numériques, la gouvernance cyber et la sécurité des données**.

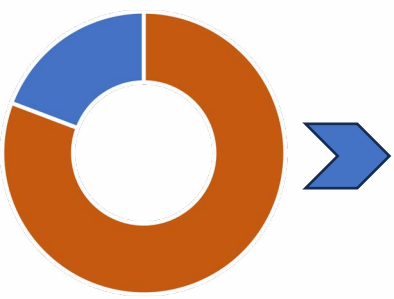
— Les principaux acteurs internationaux que sont Thalès, Atos, Cisco, Palo Alto, Orange Cyberdéfense, Docaposte, IBM, Koesio, Axians, Capgemini, Accenture, Sopra Steria sont tous présents en région.

314
ENTREPRISES
(387 ÉTABLISSEMENTS)

dont

45
GRANDS GROUPES

102
TPE ET STARTUP



71
ÉDITEURS DE PRODUITS ET DE LOGICIELS

82
« PURES PLAYERS » EN CYBERSECURITÉ

Lyon
195 établissements

Grenoble
51 établissements

Clermont-Ferrand
21 établissements

Top 3 des domaines d'application

INFRASTRUCTURE NUMÉRIQUE
96
établissements

GOUVERNANCE CYBER
75
établissements

DONNÉES
58
établissements

19 %
des entreprises à capitaux étrangers*
40
Établissements

*206 entreprises sur un total de 293 entreprises recensées ont renseigné la nationalité de leur tête de groupe

Principaux investisseurs étrangers

ETATS-UNIS, ROYAUME-UNI, BELGIQUE

LA CYBERSECURITÉ DANS LE MONDE ET EN FRANCE

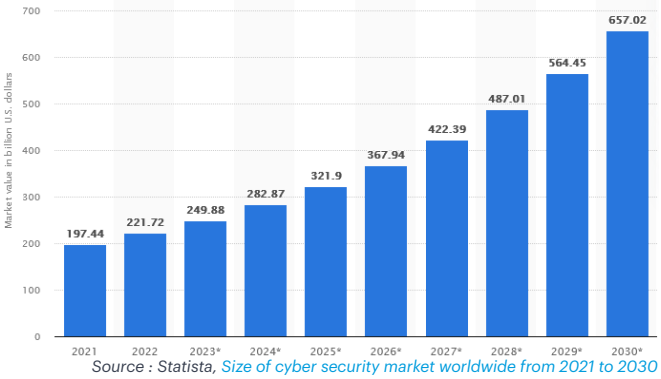
UNE CROISSANCE DU MARCHÉ MONDIAL ACCÉLÉRÉE PAR DES ATTAQUES MASSIVES

— La hausse continue du volume de cyberattaques subies par de nombreuses entreprises à travers le monde depuis trois ans, participe pleinement au dynamisme de la filière Cybersécurité qui bénéficie d'investissements massifs.

— Les acteurs mondiaux de la cybersécurité sont aussi portés par une plus grande exposition au risque cyber lié à l'évolution des infrastructures (cloud, IOT), des nouveaux usages (télétravail par exemple..) et par l'émergence très rapide de l'I.A.

— Les experts de la filière tablent sur une croissance du marché mondial de la cybersécurité de + 267 % entre 2023 et 2030 pour atteindre un chiffre d'affaires consolidé de 657 Md$ contre près de 250 Md$ actuellement.

Chiffre d'affaires du marché mondial de la Cybersécurité sur la période 2021-2030 (en Md$)



Source : Statista, Size of cyber security market worldwide from 2021 to 2030

UNE FILIÈRE FRANÇAISE DE LA CYBERSÉCURITÉ PARTICULIÈREMENT DYNAMIQUE

— La filière cybersécurité compte en France **2 129 entreprises** dont 75 grandes entreprises, 67 ETI, 644 PME et 1 343 micro-entreprises.

— Elle regroupe près de **86 700 emplois** et affiche un chiffre d'affaires consolidé de près de **17,7 Md€** dont 5,4 Md€ de chiffre d'affaires à l'export.

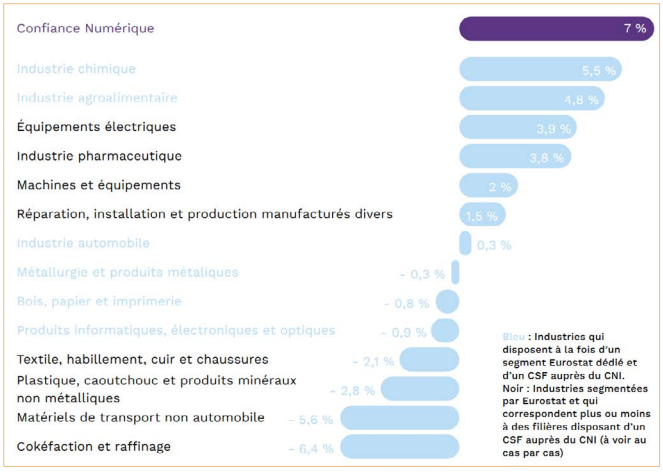
— La croissance exponentielle de la filière cybersécurité au niveau mondial concerne également la France puisque la filière de la confiance numérique (= cybersécurité au sens large) apparait sur la période 2016-2020 comme la filière la plus dynamique tous secteurs d'activité confondus avec une croissance annuelle moyenne de près de **7%**.

— Une filière française qui est notamment portée par **la croissance rapide de la demande en produits cyber**.

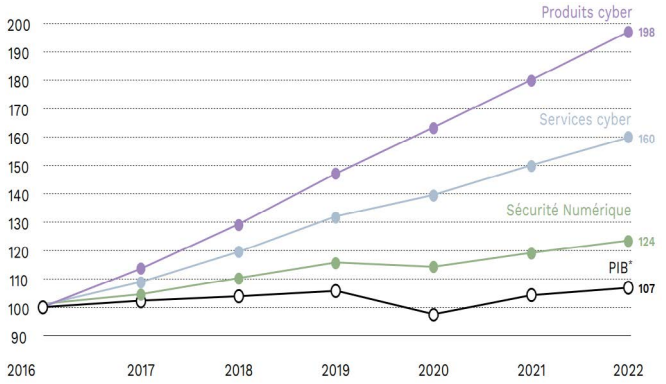
— Ainsi sur l'année 2022, la filière a affiché une **croissance de 10,1%**, un chiffre bien supérieur à celui du PIB français (+ 2,6 % sur la période). Cette dernière est notamment portée par les produits cyber qui ont connu une croissance de leur chiffre d'affaires global de **+ 98%** entre 2017 et 2022 pour atteindre 5,2 Md€.

— Les principaux acteurs en France que sont Thalès, Airbus, Atos, Orange Cyberdéfense, Idemia, Docaposte, IBM, In Groupe, Accenture, SopraSteria portent le marché avec un chiffre d'affaires cumulé de près de 6,2 Md€.

Croissance annuelle moyenne des filières françaises sur la période 2016-2020



Croissance comparée des trois grands segments de la cybersécurité sur la période 2017-2022



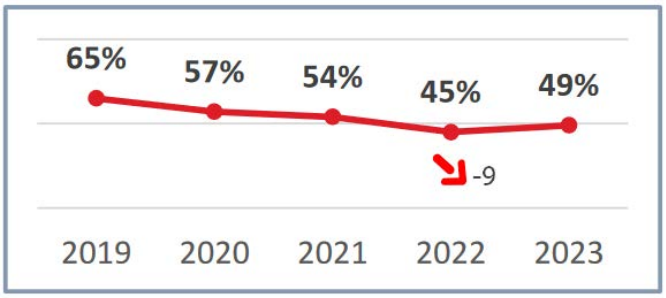
Source : Alliance pour la Confiance Numérique, Observatoire de la Filière de la Confiance Numérique 2023

Sécurité Numérique	Poduits & logiciels Cyber	Services cyber
+ 9,4%	+ 10,5%	+ 10,7%
7 762 Mds €	5 197 Mds €	4 750 Mds €

UNE HAUSSE CONTINUE DES CYBERATTAQUES EN 2023

— Près de **49 %** des entreprises françaises interrogées par le CESIN ont constaté au moins une cyberattaque en 2023, un chiffre en hausse de 4 points par rapport à 2022.

Entreprises ayant constaté au moins une cyberattaque sur 12 mois



Sources : CESIN et OpinionWay, Baromètre de la cybersécurité des entreprises - 2024

— Le niveau de la menace informatique continue d'augmenter sur cette année 2023 dans un contexte géopolitique mondial marqué par des tensions exacerbées et la tenue d'événements internationaux sur le sol français. Les cyberattaquants réputés liés à la Russie, la Chine et les groupes structurés de cybercriminels constituent par ailleurs selon l'ANSSI les trois grandes menaces pour l'année 2024.

— Les cyberattaques à but lucratif se sont maintenues à un niveau élevé en 2023 tandis que le **nombre total d'attaques par rançongiciel** portées à la connaissance de l'ANSSI ont augmenté de près de **+30 %** par rapport à 2022.

— Ces attaques par rançongiciel se concentrent de plus en plus sur **les entreprises stratégiques** (+ 4 points en un an) et les établissements d'enseignement supérieur. Les TPE/PME/ETI sont un peu moins ciblées en proportion (-6 points en un an) même si le volume de cyberattaques en valeur absolue reste en hausse.

— Selon le Security Navigator 2024 d'Orange Cyberdéfense, les hackeurs ciblent principalement les **acteurs externes** aux organisations en tant que principal point d'entrée dans le système d'informations. Ces derniers représentent ainsi **44%** du point d'entrée des cyberattaques.

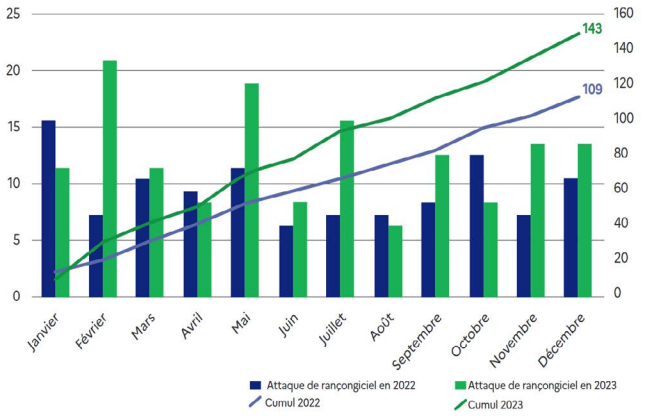
— Les acteurs internes sont également privilégiés par les cyberattaquants, ils constituent la seconde entité causant l'intrusion à hauteur de **37%** des cyberattaques, notamment lorsque les hackeurs profitent de l'utilisation abusive*.

— Le hacking est d'assez loin la principale technique d'intrusion des cybercriminels notamment au sein des réseaux d'entreprises à hauteur de **30%**.

— Les actifs les plus touchés par les cyberattaques sont les terminaux utilisateurs (28 %), le réseau de l'organisation (27%) ou un autre actif (22%).

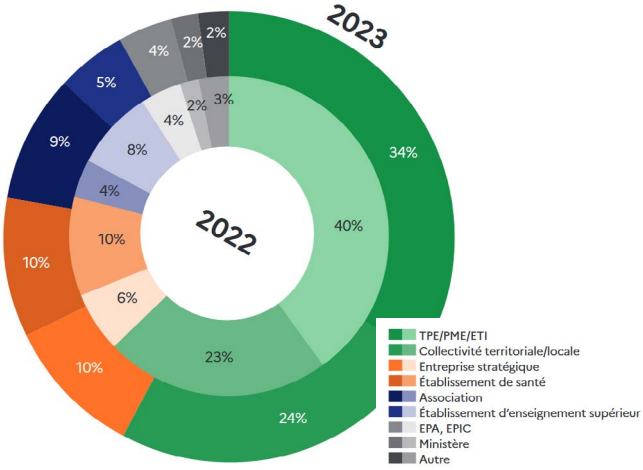
**L'utilisation abusive est définie comme l'utilisation de ressources organisationnelles de confiance ou de privilèges à des fins ou de manière contraires à celles prévus.*

Comparaison des signalements d'attaques par rançongiciel en 2022 et 2023



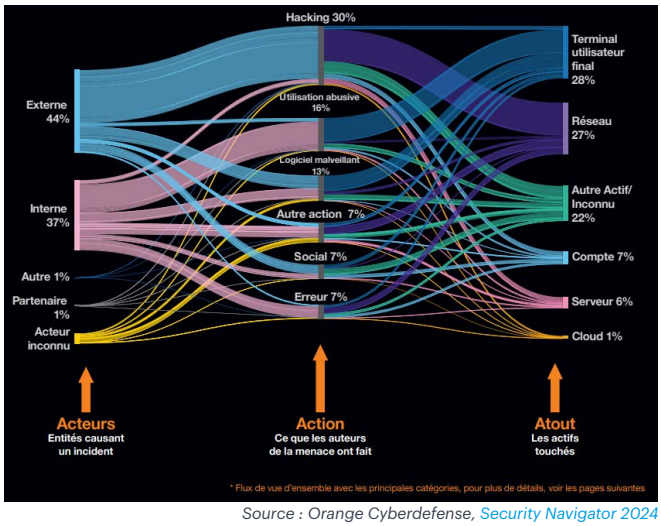
Source : ANSSI, Panorama de la cybermenace 2023

Répartition des victimes d'attaque par rançongiciel en 2023



Source : ANSSI, Panorama de la cybermenace 2023

Flux des principales catégories d'incident recensées par Orange Cyberdéfense en 2023



Source : Orange Cyberdefense, Security Navigator 2024

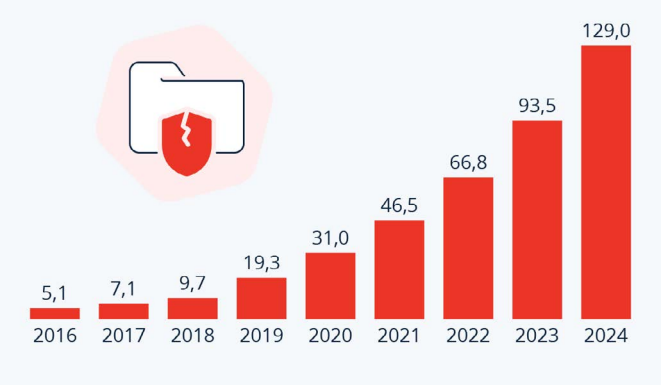
DES CYBERATTAQUES QUI PERTURBENT L'ACTIVITÉ DES ENTREPRISES FRANCAISES

— Le volume de cyber-extorsions en France n'a cessé d'augmenter depuis 2020 en raison de la structuration progressive des groupes de cyberattaquants et de la généralisation de l'intelligence artificielle qui facilite désormais l'accès aux outils de hacking pour des cyberattaquants novices.

— Le nombre de victimes de cyber-extorsion est ainsi passé de 519 au 3e trimestre 2020 à 1 086 au 3e trimestre 2023, soit une augmentation de **+109 %** sur la période.

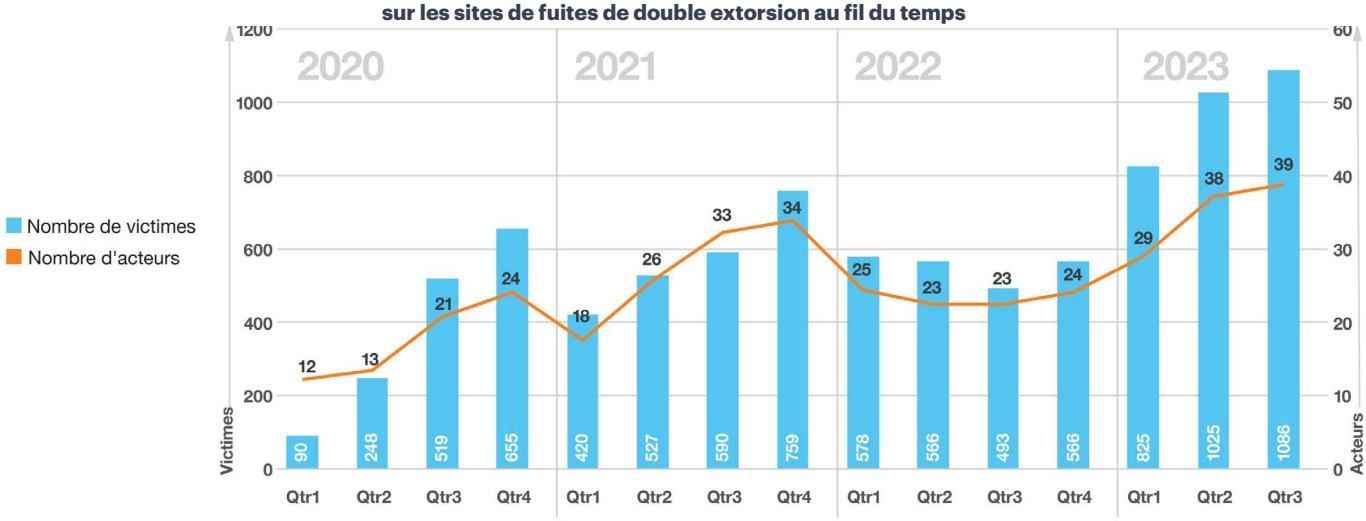
— Cette montée en puissance linéaire de la cybercriminalité fait peser un coût financier de plus en plus important sur les entreprises. Le coût annuel de la cybercriminalité pour les entreprises françaises devrait ainsi atteindre **129 M€** au cours de l'année 2024 contre **31 M€** en 2020.

Estimation du coût annuel de la cybercriminalité en France
(en milliards de dollars américains)



Source : Statista Technology Market Insights

Cyber-extorsion dans le temps : nombre de victimes et d'acteurs observés sur les sites de fuites de double extorsion au fil du temps

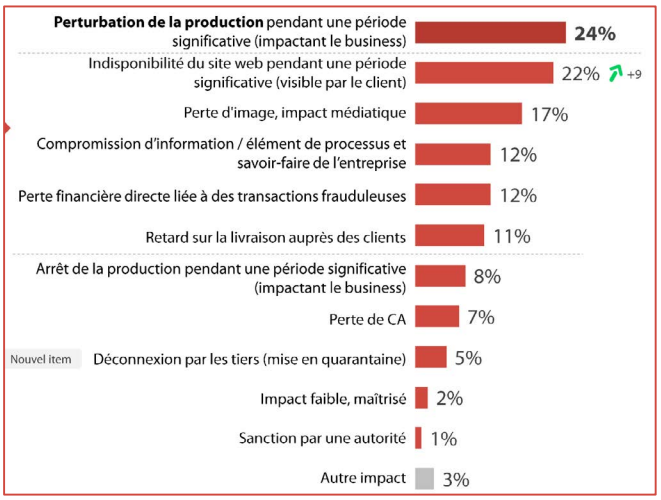


Source : Orange Cyberdefense, Security Navigator 2024

— Le principal impact d'une cyberattaque sur l'activité d'une entreprise prend souvent la forme d'une perturbation de la production pendant une période significative (pour 24 % des entreprises attaquées), suivi de près par l'indisponibilité du site web pendant une période significative (+ 9 points en un an).

— La perte d'image, la compromission d'informations, ou de savoir-faire de l'entreprise, la perte financière directe liée à des transactions frauduleuses représentent les autres grands dommages observables à la suite d'une cyberattaque réussie.

Principaux impacts observés sur l'activité d'une entreprise suite à une cyberattaque



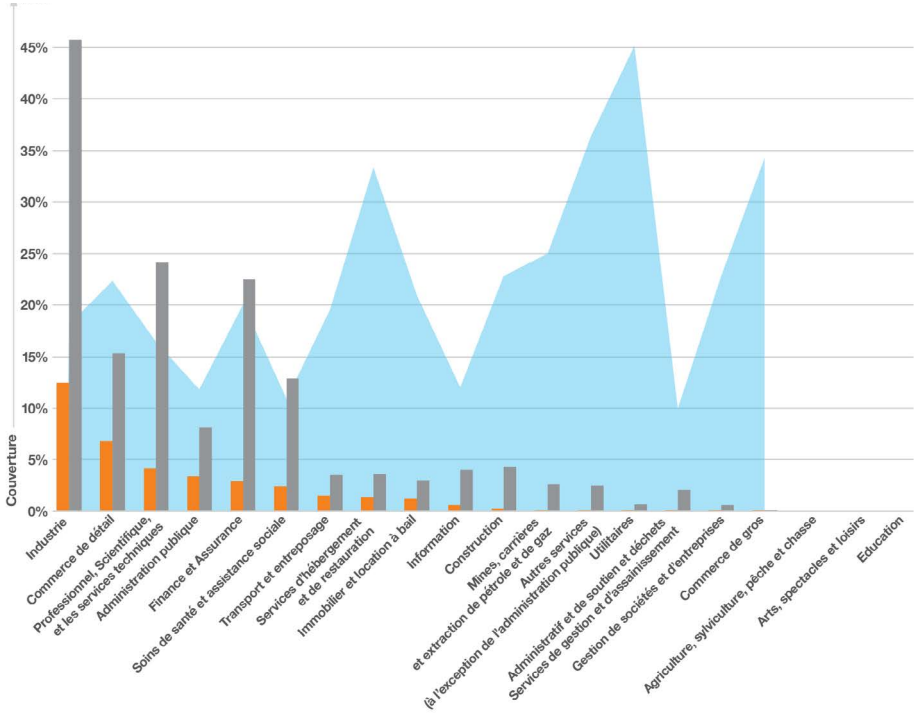
Sources : CESIN et OpinionWay, Baromètre de la cybersécurité des entreprises - 2024

UN SECTEUR INDUSTRIEL PARTICULIÈREMENT CIBLÉ PAR LES CYBERATTAQUANTS

— **L'industrie** apparaît assez nettement comme le **secteur d'activité le plus touché** par les cyberattaques en 2023 avec près de **20 %** de l'ensemble des cyberattaques.

— La numérisation des outils de production explique en partie cette stratégie offensive sur les actifs industriels en raison d'une proportion de plus en plus forte de machines, automates et autres robots industriels programmés via commande numérique.

Incidents de sécurité, normalisés à l'aide du score de couverture



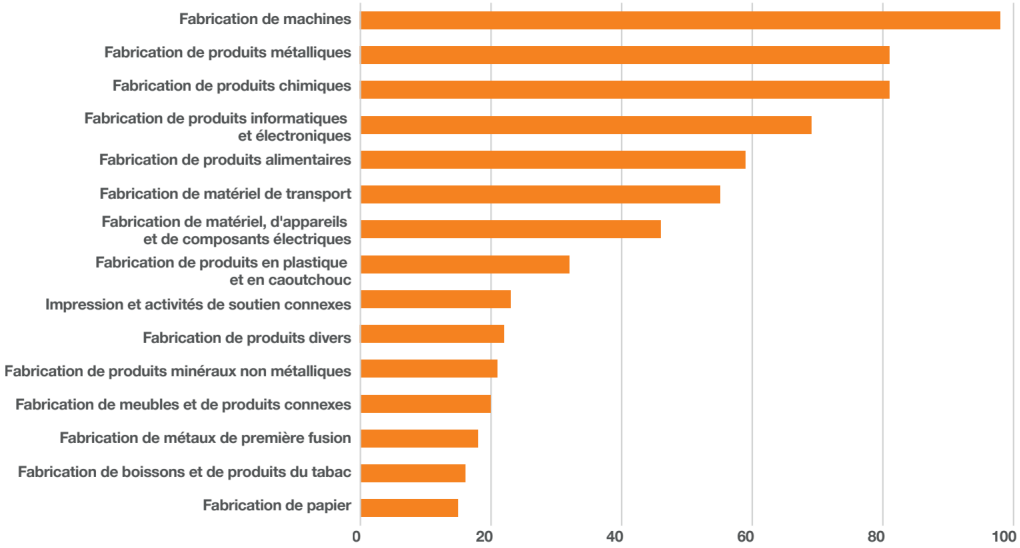
Définition

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.

— L'évolution du nombre de victimes de cyber-extorsion dans l'industrie a augmenté d'une année sur l'autre de **+ 42 %** ce qui représente près de 200 victimes supplémentaires.

— Le sous-secteur industriel de la fabrication de machines a enregistré la plus forte proportion d'attaques, devant les sous-secteurs de **l'industrie chimique et de l'industrie de la fabrication de produits métalliques.**

Incidents de sécurité, normalisés à l'aide du score de couverture



Source : Orange Cyberdefense, Security Navigator 2024

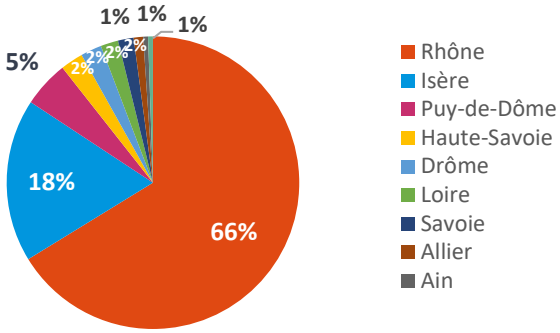
LA FILIÈRE CYBERSECURITÉ EN AUVERGNE-RHÔNE-ALPES

UN TERRITOIRE MOTEUR A L'ÉCHELLE NATIONALE, PORTÉ PAR LA DYNAMIQUE DE LA MÉTROPOLE LYONNAISE

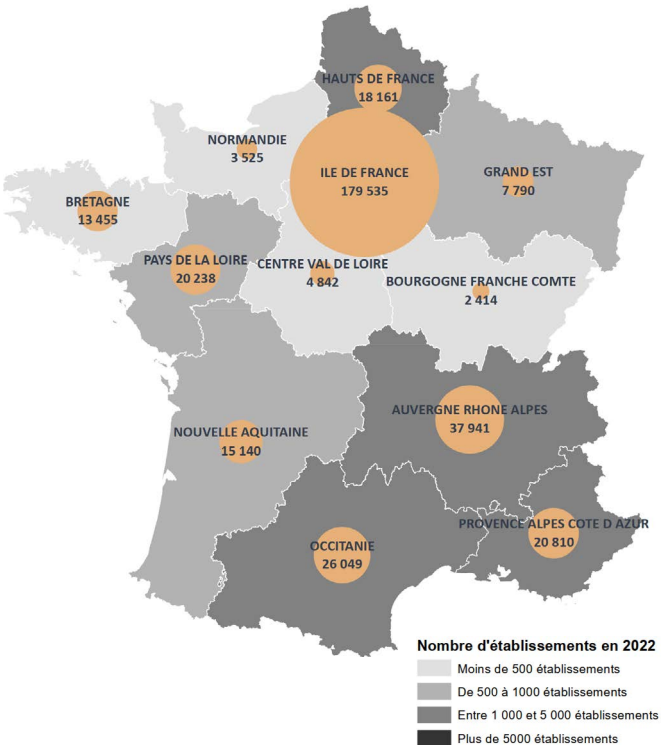
— En 2022, Auvergne-Rhône-Alpes comptait **38 000 salariés** dans le conseil en systèmes et logiciels informatiques soit **11%** des effectifs nationaux. Le territoire se positionne assez nettement comme **le second pôle national** (7% pour l'Occitanie, troisième région) en termes de poids économique et d'emplois dans la filière derrière l'Ile-de-France (51% des effectifs nationaux).

— A l'échelle de la région, l'emploi en conseil en systèmes et logiciels informatiques est particulièrement concentré dans le Rhône, (notamment dans la zone d'emploi de Lyon) avec **25 230** salariés soit **66 % de l'emploi** salarié privé régional. L'**Isère** avec **6 870** salariés (18 % des effectifs) et le **Puy-de-Dôme** avec **1 950** salariés (5 % des effectifs) complètent le tableau des principaux clusters régionaux en conseil en systèmes et logiciels informatiques.

Répartition des effectifs par département



Nombre de salariés dans le conseil en systèmes et logiciels informatiques



Source: Acoss-URSSAF, décembre 2022 NAF 6202A Conseil en systèmes et logiciels informatiques

De grands groupes et des PME innovantes en région	
Sopra Steria est un grand groupe français de services numériques qui mène des activités de conseil, de services numériques et d'édition de logiciels. Il propose une offre globale de services de conseil, d'intégration de solutions et de services managés pour accompagner les décideurs tout au long du cycle de vie de la cybersécurité : Prévention, Protection et Détection & Réponse face aux cyberattaques. Originaire de Haute-Savoie, le groupe est fortement implanté dans la région au travers de 7 établissements dont son siège social à Annecy.	sopra steria
Visiativ est un éditeur de solutions qui accélèrent l'innovation et la transformation des PME et ETI. Visiativ Innovation Engine identifie les principaux leviers de performance clés pour coconstruire une feuille de route de transformation numérique et réalise des diagnostics, des pentests et du pilotage RSSI au travers de sa plateforme digital « Cyber Pilot ». Le groupe possède 5 établissements en région.	visiativ
Serenicity développe des solutions matérielles et logicielles de cybersécurité de précision permettant d'identifier et de neutraliser les flux toxiques véhiculés sur les réseaux informatiques. Fondée en 2018, Serenicity une Jeune entreprise innovante (JEI) et a déjà déposé 10 brevets européens.	SERENICITY cybersécurité de précision
Cisco est un acteur majeur de la cybersécurité à l'échelle mondiale. Le groupe conçoit et commercialise des suites logicielles de sécurité : accès sécurisé des utilisateurs, sécurisation des applications et données sur le cloud, analyse et résolution des incidents cyber, pare-feu, solution Zero Trust. En 2019 le groupe américain a fait l'acquisition de Sentryo une start-up dont le siège était sur le campus de l'INSA, pionnières des solutions de Cybersécurité pour les environnements industriels. Villeurbanne est aujourd'hui le centre de R&D mondial pour la cybersécurité industrielle et l'IOT de CISCO.	CISCO
Stormshield, filiale d'Airbus Defense and Space, est un leader Européen dans les solutions de sécurité des réseaux des postes de travail et des données. Si le siège de la société s'est déplacé en région parisienne une grande partie des équipes de R&D sont toujours localisées à Lyon.	STORMSHIELD
Tenacy est une start-up lyonnaise qui propose une solution de gouvernance et de management de la cybersécurité en mode Saas. Après deux levées de fonds auprès d'investisseurs en capital-risque la société connait un développement très rapide en France et au niveau européen.	Tenacy
Hackuity est une start-up lyonnaise qui offre une solution de gestion des vulnérabilités se plaçant parmi les leaders mondiaux. La société, financée par des investisseurs en capital-risque se développe rapidement sur le marché mondial.	hackuity
Orange Cyber Défense, est une filiale du groupe Orange dédiée à la cybersécurité, elle dispose à Lyon d'une practice dédiée à la cybersécurité industrielle et d'un laboratoire de test spécialisé.	Orange Cyberdefense

UN TISSU ÉCONOMIQUE COMPOSÉ DE GRANDS GROUPES ET DE PME INNOVANTES

— Le recensement des acteurs régionaux de la cybersécurité a permis d'identifier **314 entreprises** soit **387 établissements** en Auvergne-Rhône-Alpes.

— Le département du Rhône concentre **207 établissements**, soit **58 %** des entreprises régionales notamment dans la zone d'emploi de Lyon qui compte 194 établissements (56 % des établissements régionaux).

— **La ville-même de Lyon** abrite près de **102 établissements** soit **29 %** de l'écosystème régional.

— Cette concentration d'entreprises sur le territoire lyonnais s'explique par plusieurs facteurs :

- **forte densité de formations spécialisées en cyber**,
- un écosystème bouillonnant d'ESN (entreprises de services du numérique),
- des politiques volontaristes d'accueil des entreprises informatiques,
- un **Campus Région du Numérique** qui crée de nombreuses synergies locales,
- un **fort dynamisme de l'industrie locale** qui booste la filière cybersécurité localement

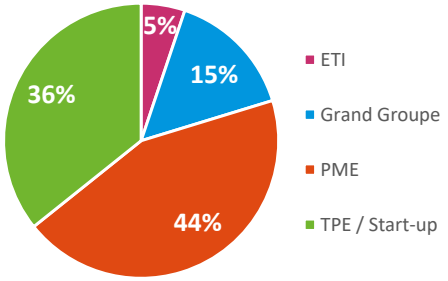
— L'**Isère** se positionne en tant que 2e centre névralgique de la cybersécurité en région avec près de **57** établissements avec notamment 51 sur la zone d'emploi de Grenoble.

— Enfin, le **Puy-de-Dôme** (**27**), la **Loire** (**24**) et la **Haute-Savoie** (**18**) ont aussi un rôle significatif à jouer dans le dynamisme actuel de l'écosystème cyber en région.

— L'analyse de la typologie des entreprises de la filière Cybersécurité en région Auvergne-Rhône-Alpes fait ressortir **une proportion importante de grands groupes**, avec près de 44 grands groupes recensés (15 % des entreprises).

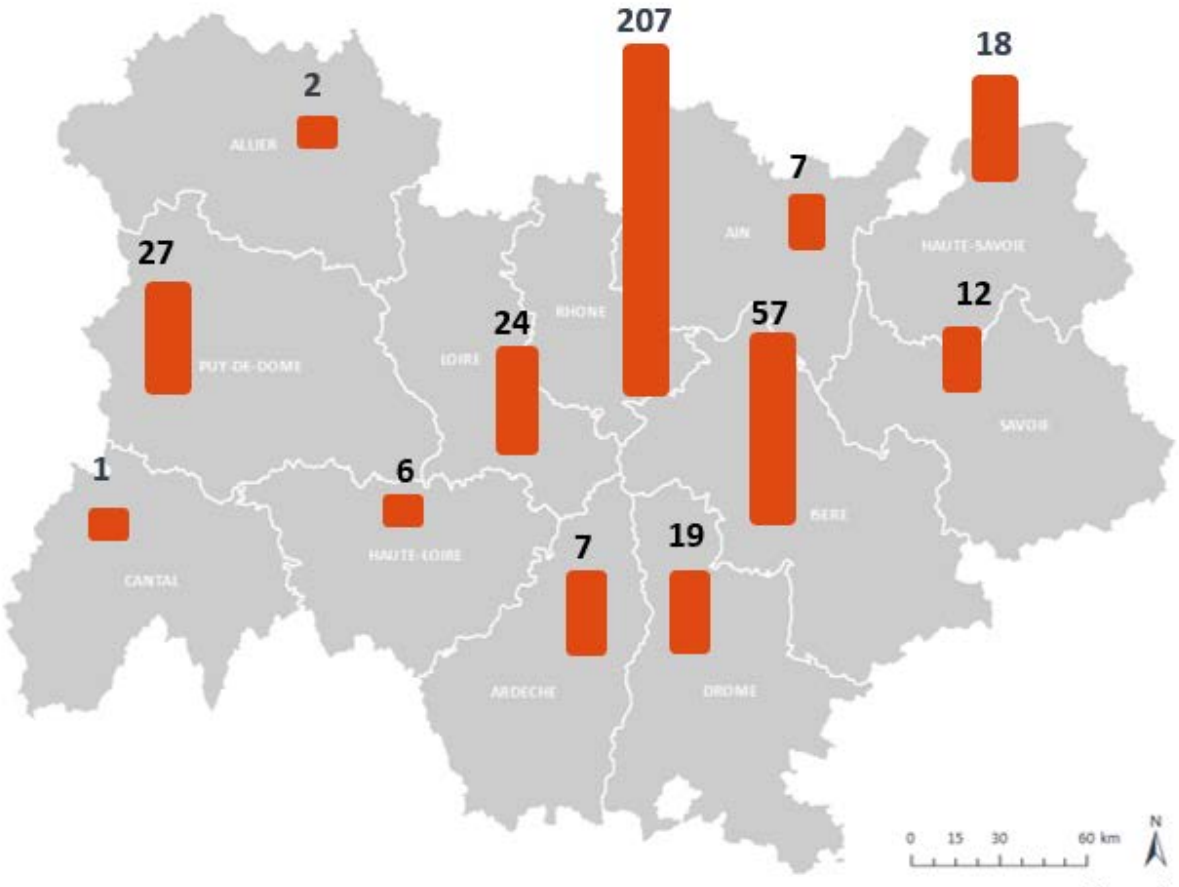
— A noter la proportion de TPE et de Starts-ups (36%) est aussi très importante notamment dans les bassins lyonnais et grenoblois.

Typologie des entreprises de cybersécurité recensées en Auvergne-Rhône-Alpes



Source : Recensement Auvergne-Rhône-Alpes Entreprises

Répartition géographique des acteurs régionaux de la cybersécurité en 2024
(en nombre d'établissements)



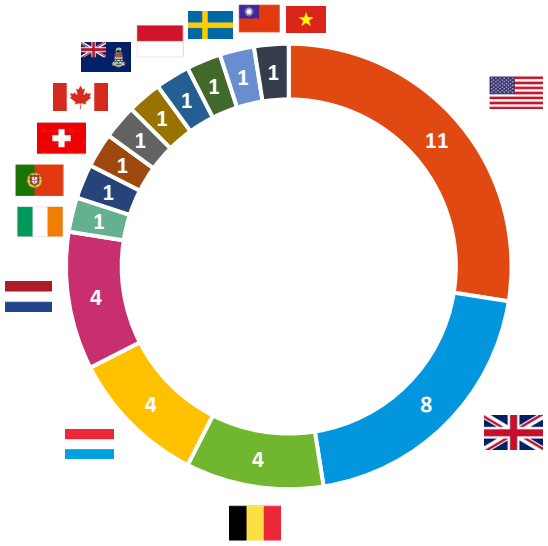
Source : Recenvsement Auvergne-Rhône-Alpes Entreprises

UN TISSU D'ENTREPRISES RICHE ET DIVERSIFIÉ

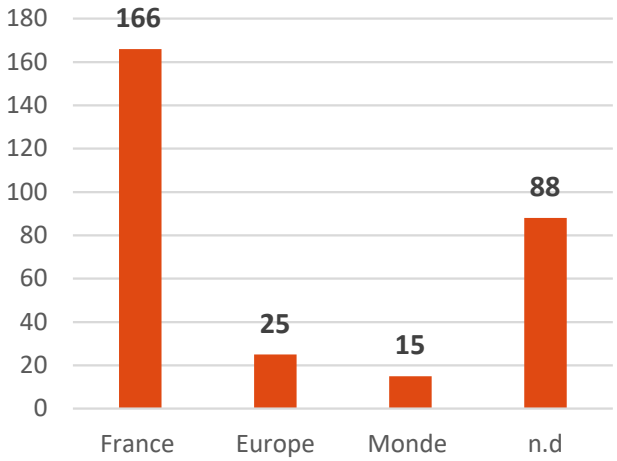
— Près de 80 % des acteurs de la cybersécurité en région sont des entreprises à capitaux français, tandis que les capitaux européens ne représentent que **12 %** des entreprises régionales et **8%** pour les capitaux mondiaux hors Europe.

— Les **Etats-Unis** apparaissent comme le 1er pays d'origine des capitaux étrangers pour les entreprises de la filière cybersécurité avec 11 entreprises. Le pays nord-américain est suivi par le **Royaume-Uni** avec 8 entreprises. Enfin, la Belgique, les Pays-Bas et le Luxembourg complètent le tableau avec une prise de contrôle de 4 entreprises en région.

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



Pays d'origine de la tête de groupe des entreprises de la cybersécurité



— A l'échelle macroéconomique, la région Auvergne-Rhône-Alpes accueille la plupart des leaders mondiaux des services numériques (ESN) et notamment les principaux leaders spécialistes de la cybersécurité : Accenture, Atos, Axians, CGI, Cisco, Computacenter, Devoteam, IBM, Inetum, Koesio, Microsoft, Orange Cyberdefense, SCC, Sopra Steria, Stormshield, Thales.

— Mais également des grands groupes de conseil spécialisés en cybersécurité : EY, Deloitte, Mazars.

Les grands groupes de la cybersécurité implantés en Auvergne-Rhône-Alpes

Source : Recensement Auvergne-Rhône-Alpes Entreprises

UNE EXPERTISE RÉGIONALE DANS L'AUDIT & LE CONSEIL ET L'INTÉGRATION DE SOLUTIONS

— **L'audit, planning et conseil compte 128 représentants** en Auvergne-Rhône-Alpes : il s'agit de l'activité principale la plus répandue chez les acteurs de la cybersécurité en région.

— Ces acteurs régionaux du conseil sont bien positionnés sur les segments de l'**audit technique, l'audit organisationnel, l'analyse de la surface d'attaque**, l'élaboration de politique de sécurité ou accompagnement vers la conformité.

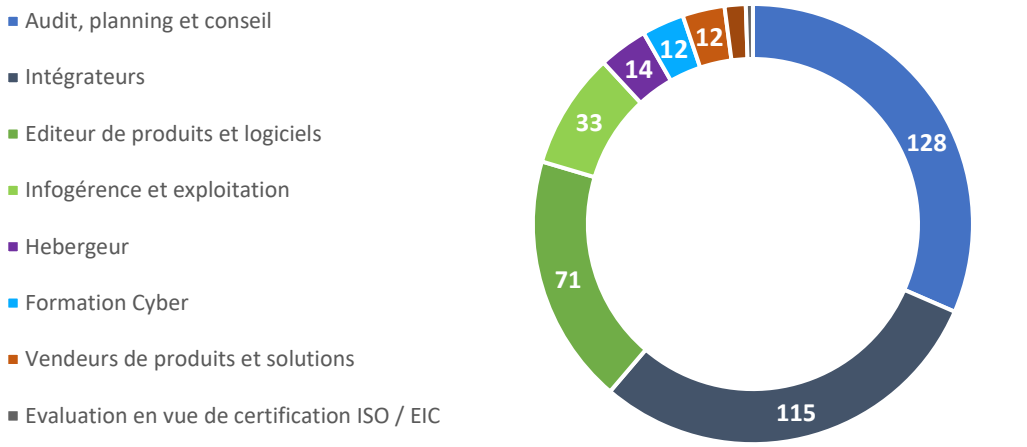
— A noter la part importante d'**intégrateurs** de solutions technologiques ou de logiciels (**115 établissements**).

— Globalement, ces acteurs se positionnent à la fois sur des activités d'intégration de solutions technologiques mais aussi sur du conseil et de l'audit en complément de leur activité principale.

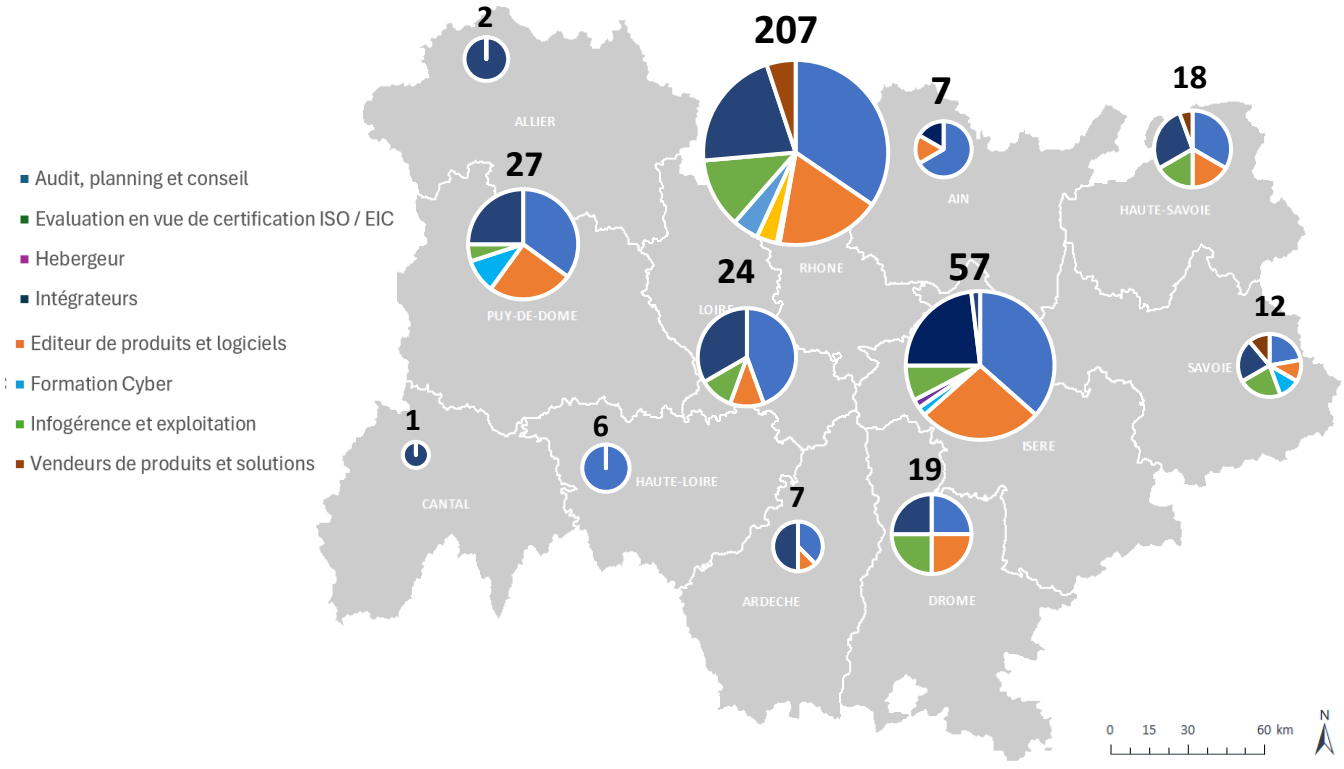
— La mise en œuvre de solutions pour **la sécurisation des infrastructures, des données, des communications et des réseaux** sont les expertises qui ressortent le plus chez ces acteurs.

— Enfin, les **éditeurs de produits et de logiciels** sont aussi bien représentés en région Auvergne-Rhône-Alpes avec **71 établissements**.

Activité principale des acteurs de la cybersécurité en Auvergne-Rhône-Alpes



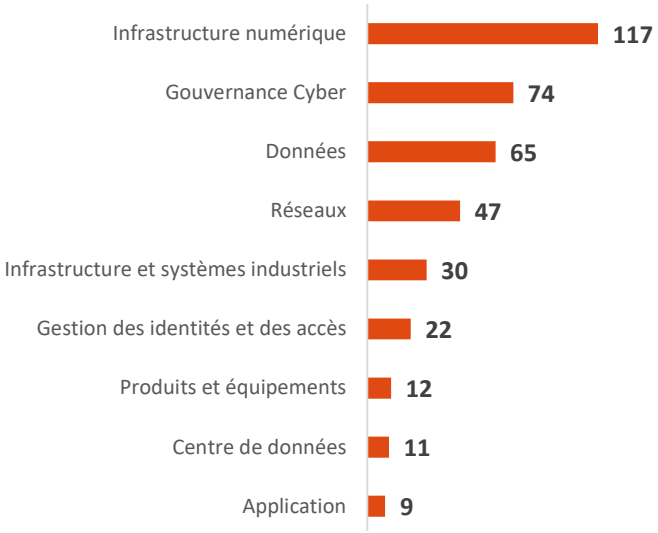
Localisation des acteurs de la cybersécurité en Auvergne-Rhône-Alpes



Source : Recenvsement Auvergne-Rhône-Alpes Entreprises

DES PRODUITS ET SERVICES CYBER POUR LES INFRASTRUCTURES NUMÉRIQUES ET LA GOUVERNANCE

Domaine d'application principal des acteurs de la cybersécurité en Auvergne-Rhône-Alpes

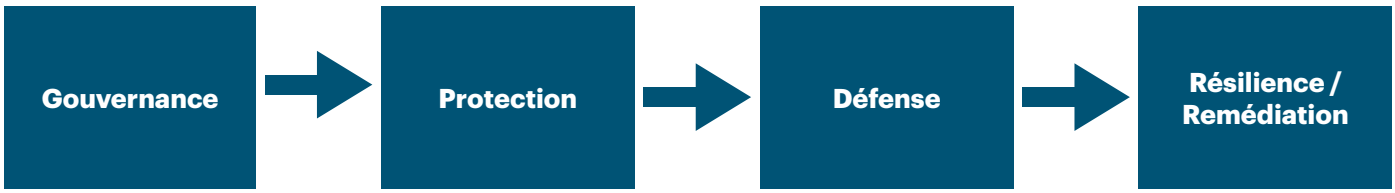


Près de **30 établissements** sont spécialisés dans les infrastructures et systèmes industriels, une véritable spécialisation régionale.

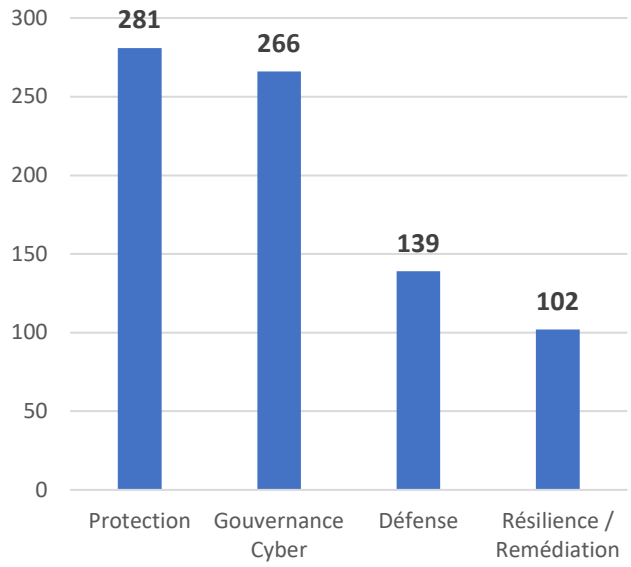
- **Les infrastructures numériques**, ou plus globalement appelées système informatique (SI) ou infrastructure IT est le principal domaine d'application des entreprises de la cybersécurité en région avec **117 établissements**.
- La gouvernance Cyber (élaboration de politique de sécurité, audits organisationnels, élaboration de PSSI, sensibilisation/formation) apparait comme le deuxième domaine d'application des entreprises régionales avec **74 établissements** recensés.
- La protection des données (cloud, serveur) arrive en troisième position avec **65 établissements** devant la protection des réseaux et des communications qui compte **47 établissements**.
- Enfin, **la gestion des identités et des accès (22), la protection des produits et des équipements (IoT) (12), les hébergeurs/centre de données sécurisés (11) et la protection des applications (9)**.

DES EXPERTISES EN PROTECTION ET GOUVERNANCE CYBER

Les 4 grands champs d'expertises en cybersécurité



Grands domaines d'expertises maitrisés par les établissements en région



- Le grand domaine d'expertise de la **Protection Cyber** regroupe près de **281 établissements** en Auvergne-Rhône-Alpes (73% des établissements) tandis que l'on retrouve **266 établissements** (69 % des établissements) dans le grand champ d'expertise de la Gouvernance Cyber.
- Ces deux grands champs apparaissent assez nettement comme les deux grandes spécialisations régionales en termes de compétences cyber, avec un positionnement conséquent de nombreux établissements sur ces deux segments et ce sur l'ensemble des territoires de la région.
- Par ailleurs, les compétences en **Défense Cyber** sont aussi bien représentées avec **139 établissements** (36 % des établissements) tout comme les compétences en Résilience et Remédiation avec **102 établissements** (26 % des établissements).

Source : Recenvsement Auvergne-Rhône-Alpes Entreprises

GOUVERNANCE CYBER — UNE SPÉCIALISATION DANS L'AUDIT ET L'ANALYSE DE RISQUES

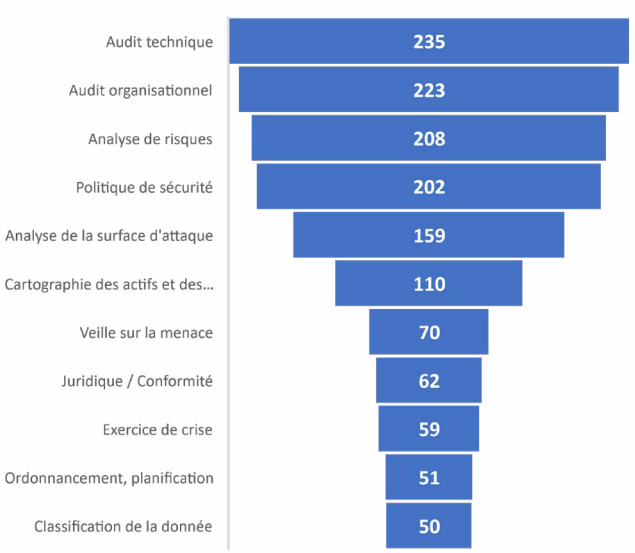
— Les expertises des entreprises régionales en Gouvernance Cyber sont principalement centrées sur l'audit avec notamment une spécialisation sur l'**audit technique** proposé par **235 établissements** (61 % des établissements) et l'audit organisationnel maitrisé par **223 établissements** (58 %).

— L'**analyse de risques** avec **208 établissements** (54 %) et le **conseil en politique de sécurité** (PSSI notamment) avec **202 établissements** (52%) sont bien représentés en Auvergne-Rhône-Alpes.

— L'**analyse de la surface d'attaque** avec **159 établissements** (41 %) ainsi que la **cartographie des actifs et des risques** avec **110 établissements** (28%) apparaissent également comme des expertises majeures pour les entreprises régionales.

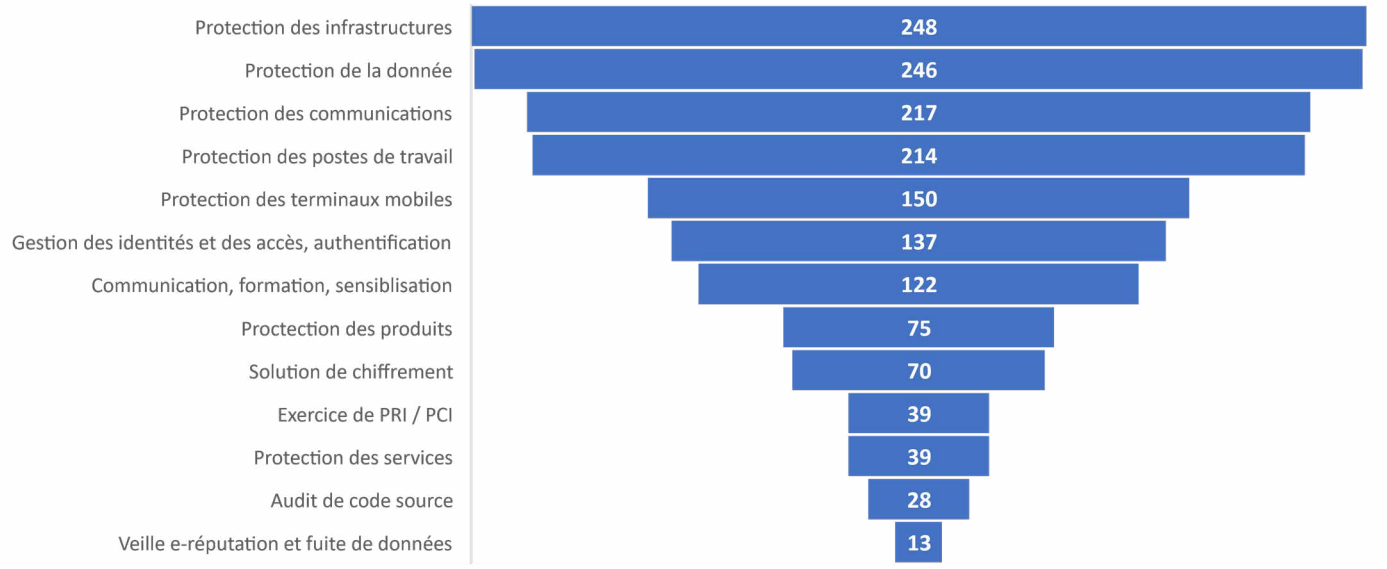
— Enfin, les compétences de **veille sur la menace** (**70**), de **conseil juridique et conformité** (**62**) et d'**exercice de crise** (**59**) sont présentes en région.

Principales compétences en Gouvernance cyber maitrisées par les établissements régionaux



PROTECTION CYBER — DES COMPÉTENCES EN SÉCURISATION DES INFRASTRUCTURES, DES DONNÉES, DES COMMUNICATIONS ET DES POSTES DE TRAVAIL

Principales compétences de protection cyber maitrisées par les établissements régionaux



Quatre grandes sous-expertises se distinguent dans le champ de la Protection Cyber :

— La **protection des infrastructures** avec notamment **248 établissements** (64 % des établissements) ainsi que la **protection des données** avec **246 établissements** (64 %) ;

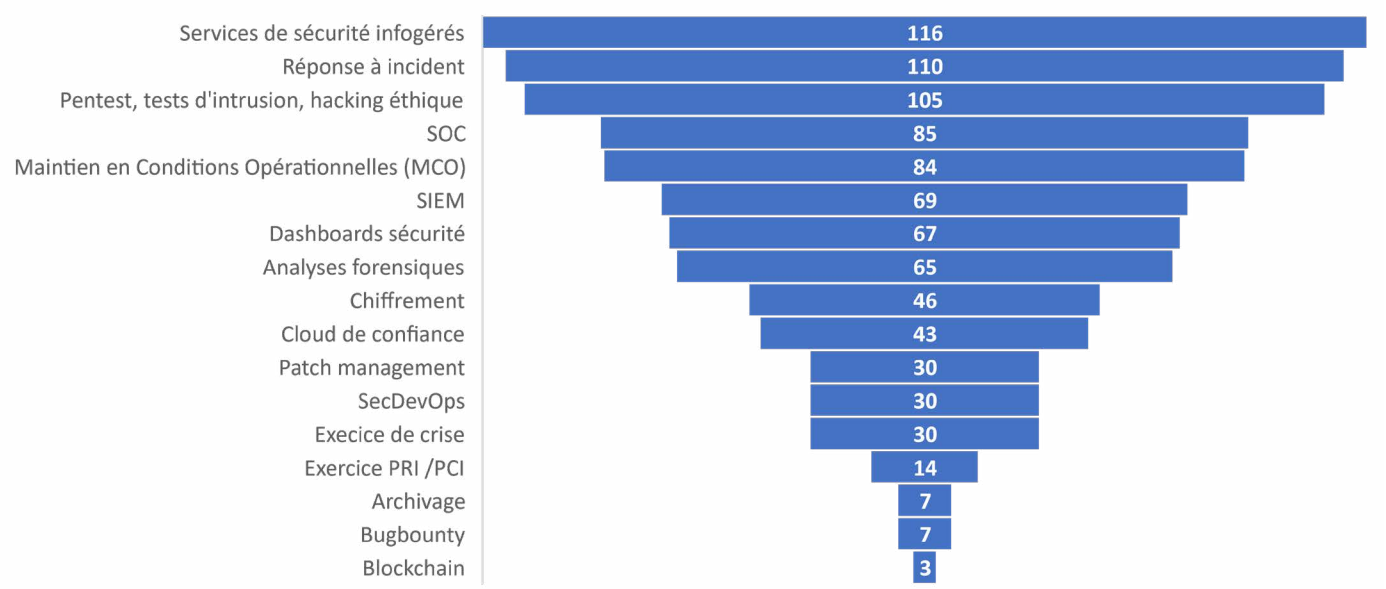
— **217 établissements** (56 %) possèdent des compétences en **protection des communications et réseaux** tandis que **214 établissements** maitrisent la protection des postes de travail (55 %) ;

— Les compétences de **protection des terminaux mobiles (150) , de gestion des identités et des accès et de l'authentification (137), de formation, sensibilisation et communication (122)**.

Source : Recensement et analyse d'Auvergne-Rhône-Alpes Entreprises

DÉFENSE DES COMPÉTENCES EN INFOGÉRANCE, RÉPONSE À INCIDENT ET PENTEST

Principales compétences en Défense cyber maitrisées par les établissements régionaux



— Les compétences des acteurs régionaux en Défense Cyber sont notamment concentrées sur des expertises de **services de sécurité infogérés** assurés par près **116 établissements** (30 % des établissements régionaux), de **réponse à incident** par **110 établissements** (28 %) et de **pentests, tests d'intrusion et hacking éthique** avec **105 établissements** (27 %).

— A noter, la proportion importante d'établissements positionnés sur les **Centres d'opérations de Sécurité : SOC** avec **85 établissements** (22 %) et **le Maintien en Conditions Opérationnelles (MCO)** avec **84 établissements** (22 %).

— D'autres compétences sont également bien représentées en région telles que **les SIEM (69), l'élaboration et le suivi de dashboards de sécurité (67) ou l'analyse forensique (65).**

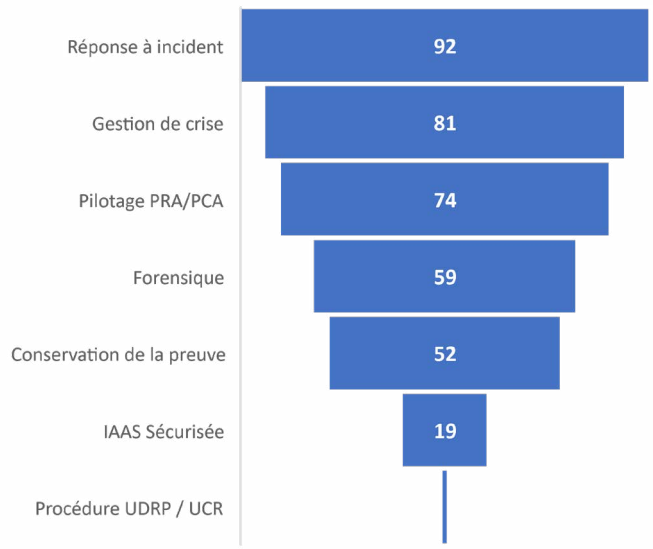
RÉSILIENCE ET REMÉDIATION DES COMPÉTENCES EN RÉPONSE À INCIDENT ET EN GESTION DE CRISE

— **La réponse à incident et la gestion de crise** apparaissent comme les deux principales expertises en résilience/ remédiation en région avec respectivement une prise en charge par **92 établissements** (24 % des établissements) et **81 établissements** (21 %).

— **Le pilotage/élaboration de Plan de Continuité d'Activité (PCA) ou de Plan de Reprise d'Activité (PRA)** est également très cité par les entreprises régionales avec **74 établissements** (19 %) tout comme **les travaux de forensique** avec **59 établissements** (15 %).

— Enfin, la **conservation de la preuve** représente **52 établissements** (13%) tandis que l'IAAS sécurisée (19 établissements) et les procédures UDRP et UCR (1 établissement) sont peu représentées.

Principales compétences en Gouvernance cyber maitrisées par les établissements régionaux



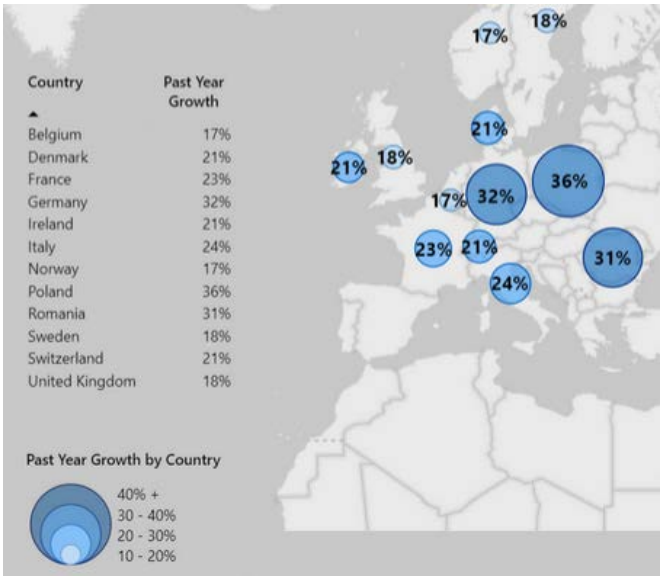
Source : Recensement et analyse d'Auvergne-Rhône-Alpes Entreprises

DES PROBLÉMATIQUES DE RECRUTEMENT MAJEURES EN FRANCE ET EN AUVERGNE-RHÔNE-ALPES

— Le besoin croissant de compétences en cybersécurité est notable et ce dans toute l'Europe : + 32 % en Allemagne, + 24 % en Italie et **+ 23 %** en **France entre 2021 et 2022**. Cela se traduit dans les faits par des difficultés de recrutement assez marquées malgré des politiques volontaristes engagés par les grands groupes du numérique et les pouvoirs publics des états européens.

— L'économie française tout secteur d'activité confondu fait également face à une **pénurie de talents** assez marquée en cybersécurité. Ainsi on estime que plus de **15 000 postes** sont disponibles mais ne sont pas couverts.

Croissance de la demande de compétences en cybersécurité par pays européen entre 2021 et 2022

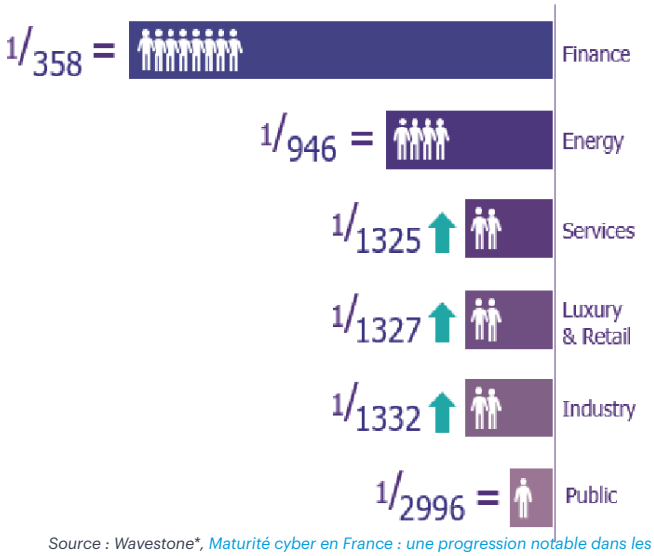


Source : Microsoft, The urgency of tackling Europe's cybersecurity skills shortage , mars 2022

— Le constat est similaire à l'échelle régionale où les postes d'**ingénieurs en informatique** se retrouvent en tête de liste des métiers les plus en tension sur l'Isère (3e métier où les difficultés de recrutements sont les plus importantes), sur le **Rhône** (4e) et sur le **Puy-de-Dôme** (3e).

— Les effectifs dédiés à la cybersécurité sont très inégaux en fonction des secteurs d'activité, avec en moyenne 1 personne dédiée pour 1 300 employés tous secteurs confondus. Ce chiffre peut monter à 1 personne pour 358 employés dans la finance et descendre à 1 personne pour 2 996 dans le secteur public, l'industrie se trouve dans la moyenne globale avec 1 personne pour 1 332 employés.

Proportion de personnel dédié à la cybersécurité sur le volume total de salariés par secteur d'activité



Source : Wavestone, Maturité cyber en France : une progression notable dans les grandes organisations qui se ressent sur la réussite des attaques cyber , avril 2023*

Les 5 métiers où les tensions de recrutement sont les plus fortes dans le Rhône en 2022

Libellé Familles Professionnelles (FAP 87)	Emploi Moyen*	Indice de tension
Techniciens et agents de maîtrise des industries mécaniques	9 370	7,64
Techniciens et agents de maîtrise de l'électricité et de l'électronique	5 327	4,89
Cadres du bâtiment et des travaux publics	7 990	4,39
Ingénieurs de l'informatique	20 863	4,23
Ouvriers qualifiés travaillant par enlèvement de métal	2 863	3,57

Les 5 métiers où les tensions de recrutement sont les plus fortes dans le Rhône en 2022

Libellé Familles Professionnelles (FAP 87)	Emploi Moyen*	Indice de tension
Techniciens et agents de maîtrise des industries mécaniques	9 370	7,64
Techniciens et agents de maîtrise de l'électricité et de l'électronique	5 327	4,89
Cadres du bâtiment et des travaux publics	7 990	4,39
Ingénieurs de l'informatique	20 863	4,23
Ouvriers qualifiés travaillant par enlèvement de métal	2 863	3,57

Sources : Dares, Pôle emploi, Données 2022

** Nombre d'emplois dans le département du Rhône et de l'Isère par métier : recensement de population*

LA FORMATION EN RÉGION

50 FORMATIONS DANS L'ENSEIGNEMENT SUPÉRIEUR EN CYBERSÉCURITÉ

Les formations de l'enseignement supérieur public de niveau bac +5

Etablissement	Diplôme	Spécialités	Métiers visés
Université de Lyon / ENS de Lyon	**Master mention Informatique parcours concepts et application**	• 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, cadres dans de grands établissements académiques et laboratoires de pointe
UGA Université Grenoble Alpes	**Master mention informatique : Cybersécurité et informatique légale**	• 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
UGA Université Grenoble Alpes	**Master mention informatique Cybersecurity** (en anglais, ouvert à l'international)	• 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
Grenoble INP Ensimag – UGA	**Master Réseaux Informatiques d'Entreprise**	• 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
Grenoble INP Esisar Valence – UGA	**Ingénieur Réseaux et Cybersécurité** Campus Région du numérique – SecNumedu – ANSSI	• Cryptographie • Sécurité des réseaux et des systèmes • Sécurité logicielle et sûreté de fonctionnement • Infrastructure Cloud • Architectures de réseaux • Méthodes de gestion de la sécurité informatique	Concepteur et développeur d'applications, Chef de projet en maitrise d'œuvre ou maitrise d'ouvrage, Architecte réseau (Pilotage), Expert/ consultant réseau
Clermont Auvergne INP Isima – UCA	**Ingénieur Filière Réseaux et sécurité informatique** SecNumedu – ANSSI	• Sécurité de l'électronique • Sécurité des systèmes d'exploitation • Sécurité des réseaux et protocoles • Cryptologie • Sécurité des bases de données • Tests d'intrusion	Architecte sécurité, Responsable de la sécurité des systèmes d'information (RSSI), Expert réponse à incident (CERT), Analyste SOC
INSA Institut National des Sciences Appliquées Lyon	**Mastère spécialisé Cybersécurité du numérique** SecNumedu – ANSSI	• Sécurité des systèmes et réseaux • Sécurité des applications • Cloud et sécurité • Cybersécurité industrielle et SCADA • Gestion opérationnelle • Audit • Gestion des identités • Tests de pénétration des infrastructures Certification ISO 27001, Lead Implementer	RSSI, Chef de projet Cybersécurité, Consultant organisationnel, Ingénieur et intégrateur de solutions en cybersécurité
Mines Saint-Étienne – Une école de l'IMT	**Mastère Spécialisé IoT : Designer of Secure Devices for IoT**	• 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
Université Lumière Lyon 2	**Master Organisation et protection des systèmes d'information en entreprise (OPSIE)** Campus Région du numérique – SecNumedu – ANSSI	• 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

Sources : Côté Formations, Recensement Auvergne-Rhône-Alpes Entreprises

Les formations de l'enseignement supérieur public/privé de niveau bac +3 et bac +5

Etablissement	Diplôme	Spécialités	Métiers visés
Université de Lyon – Lyon 1 – École Centrale Lyon	**Master Systèmes, réseaux et Sécurité** (bac+5)	• 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
IUT Annecy – IUT de Roanne – IUT1 Grenoble – IUT Valence – IUT Clermont Auvergne	**BUT spécialité réseaux & télécommunications parcours cybersécurité** (bac+3)	• Sécurité des systèmes et des réseaux, • Audit, • Analyse de risques, • Normes et cadre juridique	Administrateur de réseau, Architecte réseaux et systèmes de communication, Auditeur de sécurité (pentester, Responsable maintenance logicielle et matérielle pour les réseaux
MFR Campus du Beaujolais	**Titre professionnel d'administrateur d'infrastructures sécurisées**	• 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	**Titre professionnel administrateur d'infrastructures sécurisées**	• Sécurité du Système d'Information • Sécurité réseau • SGBD • Cybersécurité des logiciels et applications	Administrateur sécurité SI Administrateur réseaux et sécurité, Responsable sécurité informatique
Formation CCI Cantal	**Bachelor Infrastructures, Réseaux et Cybersécurité**	• Sécurité du SI • Architecture application • Administration système et virtualisation • Sécurité réseaux étendus, Haute Disponibilité	Responsable du SI, Chef de projet informatique
hexagone École Supérieure d'Informatique	**Mastère Cyberdéfense et sécurité des systèmes d'information**	• Gestion de crise cyber • Sécurité réseaux, des systèmes industriels • Cryptologie • Audit technique • Sécurité d'une architecture réseau • IA au profit du défenseur / de l'attaquant	Pentester, Cryptologue, Ingénieur Cybersécurité et Cyberdéfense, Consultant
epsi l'école d'ingénierie informatique	**Administrateur d'infrastructures sécurisées** (Lyon ou Grenoble)	• 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
epsi l'école d'ingénierie informatique	**Expert en cybersécurité** Qualiopi processus certifié – République Française	• Sécurité réseaux et systèmes • Data Architectures • Sécurité des données • Gestion de la sécurité et audit sécurité • Stratégie de sécurité SI et Normes	RSSI, Architecte SSI, Conseille en SSI auprès de décideurs, Consultant en cybersécurité, Analyste SOC
Akteap CFA CFC – Saint Michel Annecy Haute-Savoie	**Mastère Expert en architectures systèmes-réseaux et en sécurité informatique** SecNumedu	• 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	**Master Pro Expert réseaux, sécurité ou ingénierie Logicielle** Campus Région du Numérique	• Cybersécurité applicative • Introduction à la blockchain • Sécurité des architectures et tests d'intrusion • Cybersécurité industrielle	Chef de projet réseaux, sécurité, Responsable infrastructure et sécurité

Les formations de l'enseignement supérieur privé de niveau bac +3 et bac +5

Etablissement	Diplôme	Spécialités	Métiers visés
CSB .school	**Spécialiste en cybersécurité** (bac+3) CAMPUS RÉGION DU NUMÉRIQUE	• Pentest, tests d'intrusion éthiques • Architecture Sécurité Réseaux • Sécurité des données et des identités • Détection et analyse des événements de cybersécurité	Analyste de la menace, réponse aux incidents de sécurité, Architecte sécurité, Auditeur de sécurité organisationnelle, Consultant en cybersécurité, Spécialiste en cryptologie, Gestionnaire de crise de cybersécurité, Opérateur analyste SOC, RSSI PME-TPE, RSSI Grands groupes, Responsable du SOC, Délégué à la protection des données, Expert en cyber
	Responsable cybersécurité (bac+5) CAMPUS RÉGION DU NUMÉRIQUE	• Cybersécurité industrielle : évaluation de la criticité des sites et infrastructures • Sécurité opérationnelle : événements pouvant conduire à un incident • Gestion des risques et conformité	
EPITECH LEARN DIFFERENT*	**MSC Pro Cybersécurité** (bac+3)	• Audit de sécurité (pentester) • Sécurité des systèmes informatiques • Cryptographie • Forensic	RSSI, Auditeur cybersécurité, Consultant sécurité informatique, Administrateur sécurité, Pentester
WILD CODE SCHOOL	**Formation AIS : Administrateur Infrastructures Sécurisées** (bac+3)	• 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
ECAM LaSalle	**Bachelor Cybersécurité des systèmes industriels et urbains** (bac+3)	• 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, Consultant en cybersécurité IT/OT/IoT, Analyste Cybersécurité SI industriel, Automaticien cyber.
GUARDIA CYBERSECURITY SCHOOL	**Bachelor Cybersécurité** (bac+3)	• 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 pour une PME
GUARDIA CYBERSECURITY SCHOOL	**Master of Science Expert Cybersécurité** (bac+5)	• 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, Chef de projet sécurité
CESI ÉCOLE D'INGÉNIEURS	**Manager en infrastructures et cybersécurité des SI – option sécurité** (bac+5) CAMPUS RÉGION DU NUMÉRIQUE	• 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	**Formation en tronc commun en informatique, spécialisation possible en sécurité** (bac+5) CAMPUS RÉGION DU NUMÉRIQUE	• 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, Administrateurs réseaux Cloud, Security Analyst, Consultant en Cybersécurité, QA Engineer, Security Engineer,
institut des ressources industrielles · Les Chartreux · CFAI LYON CPE LYON LIVE AND DISCOVER	**Ingénieur en informatique et cybersécurité (ICS)** (bac+5)	• Conception, développement des systèmes informatiques ; DevOps • Sécurité informatique • Conception logicielle et gouvernance des données	Intégrateur de sécurité, Auditeur sécurité informatique, Administrateur de base de données, Consultant en sécurité informatique
<it/> akademy	**Expert en cybersécurité – Responsable de la sécurité du SI** (bac+5)	• 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** (bac+5) Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE · CAMPUS RÉGION DU NUMÉRIQUE	• 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

Sources : Côté Formations, Recensement Auvergne-Rhône-Alpes Entreprises

Les formations de l'enseignement supérieur privé de niveau bac +2 à bac +5

Etablissement	Diplôme	Spécialités	Métiers visés
mi Formation	**Technicien supérieur systèmes réseaux** (bac+2)	• 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** (bac+2)	• 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
mi Formation	**Administrateur d'infrastructures sécurisées** (bac+3) CAMPUS RÉGION DU NUMÉRIQUE	• 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
mi Formation	**Manager Cybersécurité** (bac+5)	• Audit et recueil des besoins • Administration et sécurité des réseaux • Cloud et virtualisation • Sécurité des objets connectés, IoT • Implémentation de techniques cryptographiques • Analyse de malware, Etudes de failles de sécurité • Hardening de système	Consultant en SI, Chef de projet sécurité, Analyste SOC, Forensic, Responsable Systèmes et Réseaux, RSSI, Consultant en informatique et cyber
Aktéap CFA CFC	**Bachelor Sécurité informatique** (bac+3)	• Stockage sur cloud • Mise en œuvre solution IoT robuste et sécurisée • Sécurité des systèmes communicants • Mécanismes cryptographiques • Attaques physiques	Chef de projet Logiciel et Réseaux, Expert en architectures systèmes-réseaux et en sécurité informatique
Cifep Chambéry & Lyon	**Titre professionnel d'Administrateur d'infrastructures sécurisées** (bac+3)	• 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	**Titre professionnel d'Administrateur d'infrastructures sécurisées** (bac+3)	• 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 / responsable systèmes et réseaux, Responsable infrastructure systèmes et réseaux
Jedha	**Concepteur-développeur en science des données – Cybersécurité** (bac+3)	• 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
LA MACHE - Supérieur -	**Certification professionnelle Technicien Supérieur Systèmes et Réseaux** (bac +2)	• Sécurité des applications • Virtualisation et cloud computing • Sécurité des infrastructures • Sécurité des systèmes, services et réseaux	Technicien Supérieur Systèmes et Réseau
LA MACHE - Supérieur -	**Certification Professionnelle Administrateur d'Infrastructures Sécurisées** (bac + 3)	• 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
ECORIS L'ÉCOLE DE L'ENTREPRISE	**Bachelor informatique et cybersécurité** (bac+3) Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE	• Sécurité des composants • Sécurité de l'infrastructure • Admin. et sécurité d'une infrastructure distribuée • Gestion opérationnelle de la cybersécurité	Administrateur d'infrastructures sécurisées
AFIP L'école de votre avenir	**Bachelor Administrateur d'infrastructures Systèmes et Réseaux** (bac+3)	• Sécurité réseaux • Sécurité base de données • Sécurité systèmes • Sécurité infrastructure distribuée • Analyse des risques	Admin. sécurité infor-matique ou infrastruc-tures sécurisées, Gestionnaire de réseau, Responsable réseaux et télécoms, Admin. systèmes et réseaux

Sources : Côté Formations, Recensement Auvergne-Rhône-Alpes Entreprises

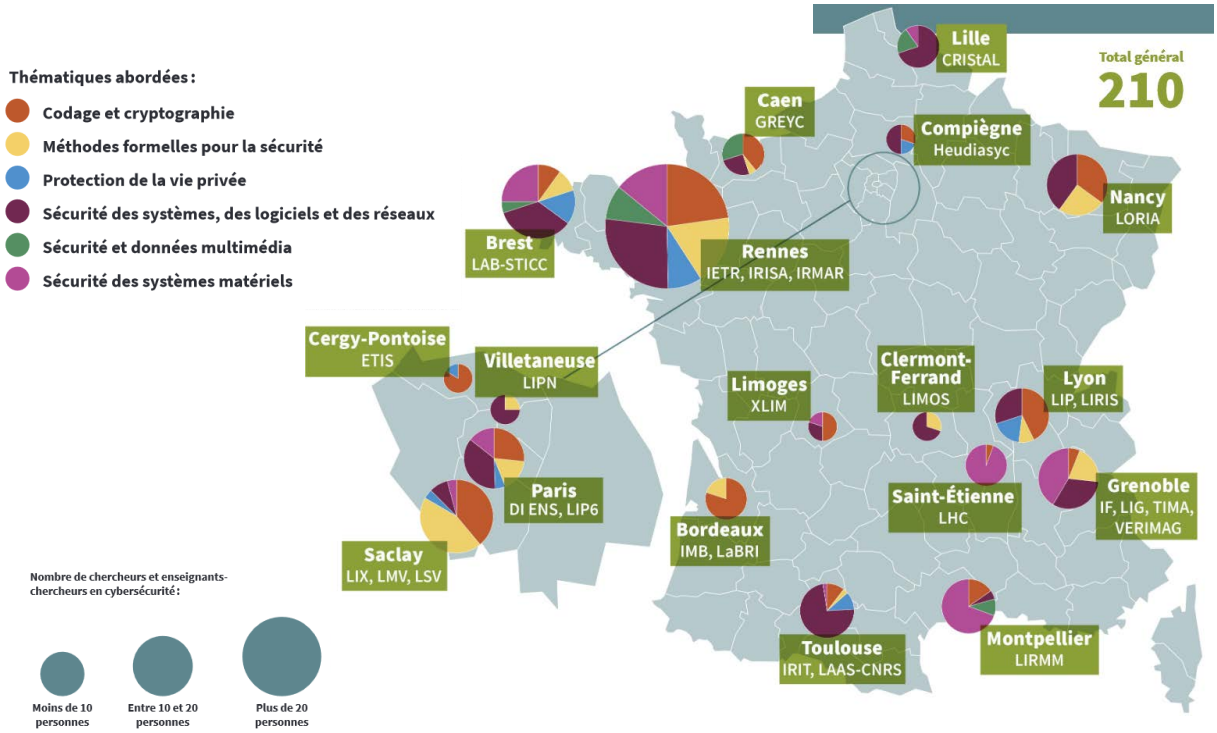
RECHERCHE ET INNOVATION

UN PÔLE DE RECHERCHE MAJEUR EN CYBERSÉCURITÉ

— La région Auvergne-Rhône-Alpes possède une forte densité de laboratoires de recherche en cybersécurité au CNRS avec pas moins de 8 centres académiques d'excellence. Le **pôle de recherche lyonnais** est reconnu pour ses **travaux académiques en codage et cryptographie** (LIP, LIRIS, Ecole Normale Supérieure).

— La région possède également une véritable spécialisation et une reconnaissance internationale pour son excellence dans **la recherche en sécurité des systèmes matériels** notamment au sein de l'écosystème de recherche bouillonnant grenoblois (IF, LIG, TIMA, VERIMAG), en lien notamment avec la « Silicon Valley Française », un territoire pivot de la microélectronique à l'échelle européenne (cf. Panorama des acteurs de la microélectronique en Auvergne-Rhône-Alpes 2023), le laboratoire Hubert Curien de Saint-Etienne est également une référence sur ce segment.

Les laboratoires de recherche en cybersécurité au CNRS



Source : CNRS Sciences informatiques, Dossier Thématique - La Cybersécurité au CNRS

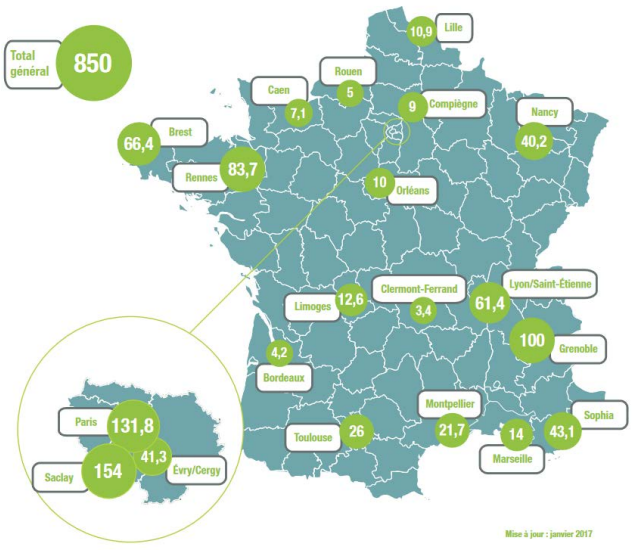
— La région en tant que **second pôle national de recherche en cybersécurité** (derrière l'Ile-de-France) héberge sur son territoire près de **165 équivalents temps plein** (ETP) consacrés à la recherche en cybersécurité ce qui correspond à **238 chercheurs** qui consacrent une partie ou la totalité de leurs travaux académiques sur des sujets relevant de la cybersécurité.

— Le pôle de recherche majeure du bassin grenoblois (CEA et CNRS) impulse cette dynamique régionale d'innovation en accueillant près de **100 ETP** (ce qui correspond à 118 chercheurs mobilisés).

- Le territoire régional compte par ailleurs :
- **61,4 ETP** (74 chercheurs) à Lyon et Saint-Etienne
- **3,4 ETP** (46 chercheurs) à Clermont-Ferrand

Source : La Société Informatique de France, Bulletin de la Société Informatique de France, numéro 11, Septembre 2017

Répartition géographique des ETP de la recherche académique française en cybersécurité (janvier 2017)



LES DOMAINES D'EXCELLENCE ACADÉMIQUE AU NIVEAU RÉGIONAL EN RECHERCHE CYBERSECURITÉ

LA SÉCURITÉ DU MATÉRIEL (HARDWARE SECURITY)

— L'utilisation de plus en plus massive d'objets connectés (IoT) de toutes sortes, notamment dans les secteurs industriels névralgiques (énergie, mobilité, santé) augmente leurs surfaces d'attaque et crée de nouveaux risques de cybersécurité.

— Les centres de recherche en Cybersécurité sur le territoire régional sont notamment reconnus en tant que pôle d'excellence sur le sujet en raison d'un certain nombre d'atouts:

- Une plateforme de conception de technologie de fabrication et d'encapsulation de circuits intégrés (salles blanches du CEA-Leti)
- Des expertises en modélisation et spécification de fonction en sécurité (laboratoire Hubert Curien, LCIS, TIMA, CEA-Leti) et sur l'implémentation et l'analyse de mécanismes cryptographiques pour les systèmes embarqués (CEA, Institut Fourier, TIMA, laboratoire Hubert Curien)
- Des plateformes technologiques de conception et de tests de circuits intégrés, en rassemblant un nombre important de moyens de développement, de test et caractérisation et un accès à des fonderies (CEA-Leti)
- Un ensemble de moyens d'évaluation de la sécurité au-delà de l'état de l'art public au sein du CESTI-Leti

LA CRYPTOGRAPHIE POST-QUANTIQUE ET LA MENACE QUANTIQUE

— L'évolution exponentielle de l'état de l'art des connaissances sur l'ordinateur quantique nécessite d'approfondir la connaissance et l'évaluation des nouveaux schémas de cryptographie asymétrique dit « post-quantiques proposés » et de concevoir une nouvelle génération d'algorithmes de chiffrement post-quantiques.

— L'excellence de la région Auvergne-Rhône-Alpes sur la sécurité du matériel, la cryptanalyse mais aussi en mathématique avec des laboratoires de renom international lui confère un positionnement unique sur cette thématique.

— L'ERC Prometheus (2018-2022) porté par le LIP de Lyon a pour objectif de fournir un ensemble d'outils cryptographiques efficaces permettant la protection de la vie privée dans un monde post-quantique.

LA SOUVERAINETÉ DES DONNÉES

— La protection des données (personnelles, industrielles) est un enjeu majeur de la transformation numérique en cours. La région Auvergne-Rhône-Alpes dispose d'experts de niveau internationaux que ce soit sur les versants technologiques (C.Castellucia) qu'en droit international et sur le sujet de la souveraineté numérique (K.Bannelier, T.Christakis).

— La région dispose d'experts dans la technologie blockchain : le laboratoire LIMOS (Clermont-Ferrand), le laboratoire LIK (Grenoble) ainsi que son utilisation dans l'IoT (CEA-Leti). Enfin des collaborations ont été conduites avec l'ANSSI.

— Les centres de recherche en Cybersécurité sur le territoire d'Auvergne-Rhône-Alpes sont notamment reconnu pour la portée scientifique de leurs publications éditées dans les meilleurs journaux scientifiques.

Fédération Informatique de Lyon

La Fédération d'informatique de Lyon (FIL) regroupe 970 membres répartis sur cinq laboratoires de recherche : CITI, CREATIS, LabHC, LIP, LIRIS), et soutenu par les EPST CNRS et INRIA. L'activité du FIL est organisée selon six thèmes principaux et deux défis dont un sur la Cybersécurité : du composant à la donnée.

Cybersecurity Institute Univ. Grenoble Alpes

Le CyberAlps ou Grenoble Alpes Cybersecurity Institute mis en place en 2018 fédère les chercheurs de 16 laboratoires de recherche du périmètre de l'IDEX Université Grenoble Alpes : Institut Fourier, CESICE, CEA-LETI, Inria, VERIMAG, LCIS, LIG, TIMA, LJK, CREG, LISTIC, CERAG, G2Elab, G-SCOP, GIPSA, PACTE). Cette communauté de recherche travaille sur les domaines de la cybersécurité et de la protection de la vie privée.

NANOELEC.

L'institut de recherche technologique (IRT) Nanoelec, est un consortium d'acteurs des secteurs privé et public porté par le CEA. Ce consortium est chargé d'aider les entreprises à créer de la valeur et à différencier leur offre dans les domaines de la transition numérique. Son programme Usage des Technologies de liaison en soutien des entreprises (PULSE) qui réunit les industriels ST Microelectronics et Schneider Electric et les acteurs de la recherche CEA, INRIA, Grenoble INP et UGA conduit des actions de recherche technologique sur le sujet de la cybersécurité depuis 2016.

LE CEA, UNE RÉFÉRENCE MONDIALE DANS LA RECHERCHE EN ANALYSE DE VULNÉRABILITÉS ET EN PROTECTION DES SYSTÈMES

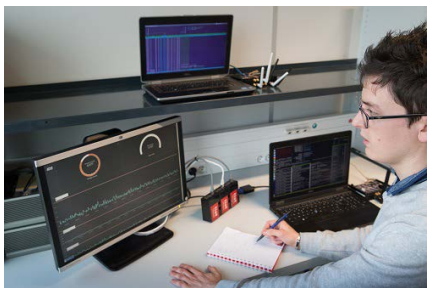
— **Le CEA (Commissariat à l'Energie Atomique)** est un acteur majeur de la recherche à l'échelle nationale et mondiale dans le numérique. Depuis 2019 ses activités de recherche en cybersécurité dans un grand programme piloté par les directions des applications militaires (DAM) et de la recherche technologique (DRT) du CEA, 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 sécurisées de type HSM ou capteurs d'empreintes digitales... peuvent être analysés.

— Afin de traiter l'**analyse de vulnérabilités des lignes de code des programmes exécutés par le produit**, le CEA-List a développé des outils logiciels dont Frama-C qui est régulièrement utilisé par les laboratoires d'évaluation et livré aux équipes de validation et de production d'industriels comme Airbus ou EDF.

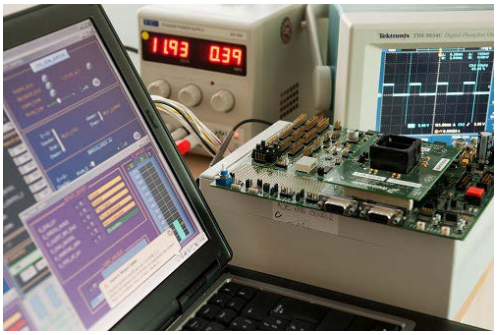
Source : CEA, Les R&D du CEA en cybersécurité
CEA-LIST, Cybersécurité : Garantir la sûreté et la confidentialité par conception
CEA, Cybersécurité quantique



Le système de détection d'intrusion réseau de l'institut CEA List détecte en temps réel des attaques inconnues complexes. Chaque sonde de détection embarque plusieurs réseaux de neurones spécialistes des protocoles et collabore également avec les autres sondes, afin d'offrir la meilleure acuité globale de détection. © Cyrille Dupont / The Pulses

— Au-delà de l'expertise pointu sur l'analyse et la mise à nu des vulnérabilités, les instituts List et Leti du CEA sont aussi **pourvoyeurs de solutions pour sécuriser les systèmes en réseaux embarqués, ainsi que les données associées**. Ils travaillent avec des industriels de la défense, de la sécurité et de l'automobile, ou encore de l'énergie et de la santé.

— En fonction des attaques à contrer, les technologies inventées par le CEA forment un panel très large de réponses, notamment sur la conception de nouvelles fonctions pour sécuriser les circuits intégrés : mémoires à effacement rapide, générateur de nombre aléatoire, fonction physiquement non clonable. Ces dernières visent aussi à assurer la sécurité des systèmes comme avec la technologie iMRC qui permet de détecter les attaques et reprendre le contrôle du système en cas d'attaques.



Performances et sûreté de fonctionnement des systèmes embarqués temps-réels avec la méthode de conception PharOS : démonstration sur un calculateur habitacle embarqué automobile bi-cœur © Philippe Stroppa / CEA (StudioPons)

— Les chercheurs du CEA aident les **industriels** à comprendre d'où viennent leurs failles de sécurité et leur propose des solutions de sécurisation.

— Le CEA réfléchit notamment aux différentes solutions permettant de **sécuriser les processeurs** de demain, la cybersécurité devenant progressivement la quatrième problématique lors de la conception d'un processeur (avec la performance, le coût du silicium et la faible consommation), un axe de R&D notamment dynamisé par l'émergence de processeurs open source comme RISC-V.

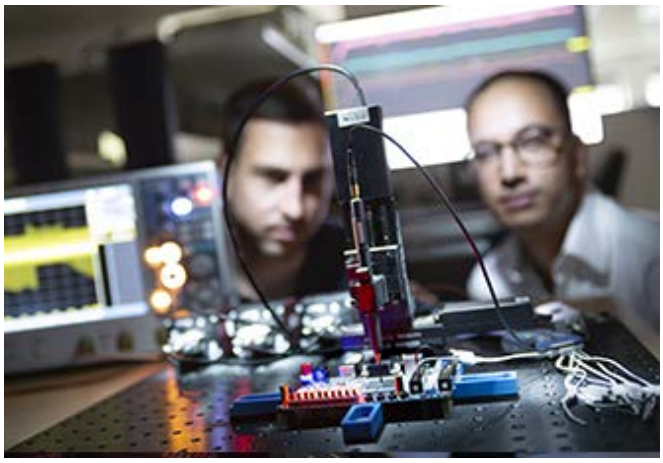
— L'arrivée imminente de l'ordinateur quantique sur le marché va profondément bouleverser le monde de la cybersécurité, puisque cette technologie permettra de casser les clés de chiffrement sur lesquelles reposent la sécurité de certaines de nos communications et opérations bancaires actuelles.

LA SOUVERAINETÉ DES DONNÉES

— La **plateforme du CEA-Leti travaille sur quatre thématiques de recherche principale**. Elle répond au défi soulevé par les attaques qui visent les circuits intégrés, des équipements électroniques ou des systèmes industriels. Elle mobilise près de 80 experts pour tenter d'identifier les vulnérabilités des produits et développer des protections innovantes. La plateforme héberge notamment l'un des trois centres officiels français (CESTI) d'évaluation de sécurité de produits matériels commerciaux.

— **Activités majeures** : évaluations sécuritaires pour certification (CETI), identification et caractérisation des vulnérabilités logiques et physiques ; conception et implémentation de protections.

— **Deux schémas de collaboration avec les entreprises de toutes tailles** : Caractérisations et évaluations sécuritaires de haut-niveau pour les systèmes électroniques et les composants (rétro-ingénierie et modification physique des composants, mise en œuvre et exploitation des attaques par canaux auxiliaires et injection de fautes, analyse de codes logiciels) / Sécurisation des composants, des systèmes et de leurs données grâce à : de nouvelles architectures de processeurs sécurisées ; des fonctions matérielles et logicielles de sécurité pour futurs composants (génération d'aléas, cryptographie) ; des stratégies de résilience des composants actuels et des techniques de sécurisation de fonctions critiques (IA, cryptographie)



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

— **Expertises mises à dispositions des industriels** : analyses de risques spécifiques aux technologies et aux cas d'usage des partenaires, nouvelles stratégies d'attaques matérielles et logicielles, Etude 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

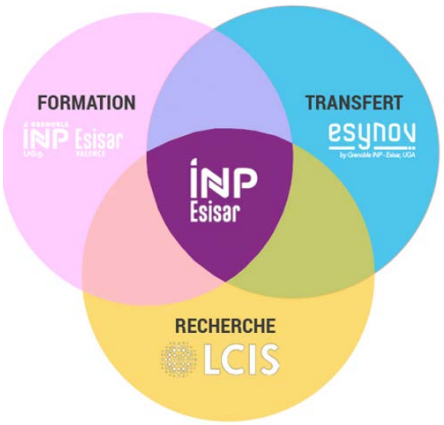
— **Des équipements à la pointe** : bancs d'investigations sécuritaires par observations (courant, EM, temps) et par injections de fautes (EM, lasers), bancs d'investigation sécuritaire via les interfaces de communication (BLE, Wifi, Zigbee, CA, ethernet) à travers du scanning et du fuzzing, plateformes de conception matérielles et logicielles de fonctions de sécurité pout technologies futures, plateforme de démonstration et d'investigation de vulnérabilités pour systèmes industriels

UN PÔLE DE FORMATION ET DE RECHERCHE MAJEUR EN CYBERSÉCURITÉ À VALENCE

— De nombreux projets collaboratifs menés par l'équipe CTSYS :
  - **Projet Anaconda (AURA R&D Booster)** : Démonstrateur d'un équipement de diagnostic de vulnérabilités IoT
  - **Projet Detoxio-s (Aura R&D)** : Application de cybersécurité souveraine développée sur FPGA pour analyser le blocage de flux numériques toxiques
  - **Projet Emness (AURA et UE/Erasmus+)** : Création d'un réseau international d'universités européennes et d'enseignants chercheurs spécialisés dans les domaines de la sécurité des systèmes embarqués
  - **Cyberskills (AMI CMA France 2030)** : Développer et renforcer les formations en cybersécurité sur les sites de Grenoble et Valence (nouvelles plateformes partagées, nouveaux contenus pédagogiques, sensibilisation collèges/lycées

— Le **LCIS – Laboratoire de Conception et d'Intégration des Systèmes** rassemble plus de 60 chercheurs en informatique sur Valence.

— **L'équipe du CTSYS travaille notamment sur la Sûreté et Sécurité des Systèmes embarqués et distribués. Axes de recherche CTSYS** :
  - Sécurité matérielle des systèmes intégrés
  - Vérification et test logiciel
  - Sûreté de fonctionnement des systèmes embarqués
  - Sûreté et sécurité dans les réseaux de systèmes connectés
  - Sûreté et sécurité des applications pervasives



LE CSAW EUROPE : UN ÉVÉNEMENT ACADÉMIQUE DE PORTÉE MONDIALE À VALENCE

CSAW'23 EUROPE

— **Le CSAW Europe – Cyber Security Awareness Week, est la plus grande compétition académique mondiale** sur le thème de la Cybersécurité qui se déroule tous les deux ans à Valence dans la Drôme pour les candidats européens.

— Depuis 2017 Grenoble INP – Esisar, UGA accueille à Valence le Hub Europe de CSAW avec le soutien de la Région Auvergne-Rhône-Alpes, et rassemble à cette occasion **100 finalistes de prestigieux laboratoires/ universités européens autour de 4 épreuves**, mobilise des partenaires industriels de renom, et reçoit plusieurs centaines de visiteurs chaque année.

LES PRINCIPAUX CENTRES DE RECHERCHE EN RÉGION

Etablissement	Lieu/effectif	Thèmes de recherche
	Grenoble	**Laboratoire d'Informatique de Grenoble** • E**quipe Construction de Systèmes Concurrents Vérifiés** – Conception fiable des systèmes concurrents et critiques contenant du parallélisme asynchrone. • E**quipe Validation de Systèmes, Composants et Objets logiciels** –Validation du logiciel et des modèles, validation de la sécurité des systèmes informatiques. • **Equipe DRAKKAR Réseaux, IoT et Sécurité** – Etudie tous les aspects des réseaux informatiques et d'explorer de nouvelles opportunités ouvertes par les réseaux tout-IP, comme les futurs réseaux sans fil et l'intégration des capteurs et des objets intelligents dans l'internet des Objets (IoT).
	Lyon **25 chercheurs** **22 doctorants**	**Laboratoire d'Informatique en Image et Systèmes d'information** • **Equipe SOC (Service Oriented Computing)** – Fondements et modèles théoriques pour les services : SOC modèles pour l'intégration et le traitement de la sémantique, l'incertitude, l'interopérabilité et des propriétés non fonctionnelles (sûreté de fonctionnement, sécurité, qualité) • **Equipe DRIM (Distribution Recherche d'information et Mobilité)** – Gestion robuste et partage de données dans les systèmes répartis et mobiles
	Lyon et Grenoble **25 chercheurs** **22 doctorants**	**Institut National de Recherche en sciences et technologies du numérique** • **SPADES, Programmation de systèmes embarqué sûrs et adaptatifs** – Conception et la programmation de systèmes embarqués fiables. • A**RIC, Arithmétiques des ordinateurs, méthodes formelles et génération de code** – Cryptographie conventionnelle, cryptographie basée sur les treillis...
	Clermont-Ferrand **17 chercheurs** **9 doctorants**	**Laboratoire d'Informatique de Modélisation et d'Optimisation des Systèmes** • **Sécurité pour la 5G** – Etudes afin de sécuriser les protocoles de communications pour la 5G, étudier comment établir des clefs de sessions entre objets connectés, sécurité de protocole • **Sécurité des chiffrements symétriques** via le projet ANR DECRYPT – analyse de la sécurité des chiffrements symétriques, objectif est d'utiliser des méthodes d'IA pour cryptanalyses automatiquement les chiffrements
	Lyon	**L'Ecole Normale Supérieure de Lyon** travaille en étroite collaboration avec le **Laboratoire de l'Informatique du Parallélisme** de Lyon sur de nombreux sujets de recherche en cybersécurité. (cf. encadré LIP)
	Saint-Étienne **10 chercheurs** **13 doctorants**	Spécialisé dans les **Systèmes Embarqués Sécurisés et les Architectures Matérielles**. 4 aspects principaux de la sécurité du matériel sont explorés : • La génération de nombre aléatoires et l'implémentation de fonctions physiques non clonables dans des dispositifs logiques • La conception d'architectures matérielles résistantes aux attaques cryptographiques passives et actives • Implémentations sécurisées de schémas post-quantiques • Sécurité des systèmes sur puce (SoC)
	Grenoble	**Techniques de l'Informatique et de la Microélectronique pour l'Architecture des systèmes intégrés** • **Equipe AMfoRS** – sûreté de fonctionnement et à la confiance des systèmes numériques à plusieurs niveaux d'abstraction pour des domaines d'application spécifiques (automobile, avionique, les cartes à puce, l'IdO
	Grenoble **35 chercheurs** **22 doctorants**	• **Validation formelle des systèmes** – Interprétation abstraite, preuves formelles et analyse de vulnérabilité • **Conception et importation correctes par construction** – Rigorous System Design (RSD) langage et outils permettant de spécifier des systèmes distribués avec plusieurs mécanismes de synchronisation + travail sur les protocoles cryptographiques)
	Grenoble	• **Cryptologie en boîte blanche et offuscation** – Conception et analyse de généra-teurs aléatoires cryptographiques et performances des primitives cryptog. • **Cryptographie post-quantique** – Algorithmes de recherche de solutions de systèmes polynomiaux sur corps finis, construction et sécurité de primitives cryptog., travail sur les attaques physiques utilisant du machine learning.
	Saint-Étienne	• Le **département Informatique et systèmes intelligents** : modèles, algorithmes et architectures informatiques pour l'interconnexion des mondes physiques, numériques et sociaux ; représentation des connaissances, raisonnements et ontologies, simulation multi-agents, fouille de données et sécurité informatique. • Les Mines de Saint-Etienne pilote également le centre de recherche en **Systèmes et Architectures** (Bouches-du-Rhône) – Intégrité des composants électroniques et données qu'ils contiennent (clefs de cryptographie, logiciels, blocs de propriété intellectuelle...) vis-à-vis de manipulations frauduleuses

LA DIRECTIVE EUROPÉENNE NIS 2

VERS UN ÉLARGISSEMENT DES ENTITÉS CONCERNÉES

— L'augmentation de la fréquence et des impacts des incidents a mis en évidence des lacunes au sein de nombreuses entités qui n'étaient pas concernées par NIS 1 (Network and Information Security).

— Les critères de définition de NIS 1 excluaient des entités dont le dysfonctionnement pouvait porter atteinte à la sécurité du système économique en particulier les chaînes d'approvisionnement, les PME, les TPE qui deviennent progressivement des cibles privilégiées par les cyberattaquants.

— La directive NIS 2 élargit le champ d'application de NIS 1 dans le but de sécuriser l'ensemble des systèmes d'information vulnérables.

— Les opérateurs de services essentiels (OSE) et les fournisseurs de services numériques (FSN) définis dans NIS 1 sont recatégorisés en entités essentielles et entités importantes. Le niveau important permet d'inclure davantage d'entités en ne se limitant plus aux services essentiels.

— La mise en œuvre de la directive européenne NIS2 élargit ses objectifs et son périmètre de protection.

Entités rentrant dans le champ d'application de NIS 2 selon le critère de taille

— La directive NIS2 continuera de s'appliquer aux secteurs déjà concernés par NIS1 mais s'étendra à de nouveaux secteurs d'activité : administrations publiques, télécommunications, plateformes de réseaux sociaux, services postaux, secteur spatial...

— L'extension du périmètre d'application de NIS2 concernera également les entreprises du secteur privé.

Entités entrant dans le champ d'application de NIS2 selon le domaine d'activité

	Entités essentielles (EE)	Entités importantes (EI)
NIS1	• Energie : électricité, pétrole, gaz • Transports : aériens, ferroviaires, par voie d'eau, routiers • Secteur bancaire • Infrastructures des marchés financiers • Santé • Traitement des eaux usées • Fournisseurs de points d'échange internet • Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine • Registre de noms de domaine de premier niveau	

NIS 2+	• Administration publique
	• Energie : réseaux de chaleur et de froid, hydrogène
	• Fournisseurs et distributeurs d'eau potable pour lesquels la distribution constitue une partie essentielle de leur activité générale
	• Gestion des services de technologie de l'information et de la communication interentreprises
	• Espace et entreprises du spatial à l'exclusion des fournisseurs de réseaux de communications électroniques publics
	• Infrastructure numérique
	  • Fournisseurs de services d'informatique en cloud
	  • Fournisseurs de services de centres de données
	  • Fournisseurs de réseaux de diffusion de contenu
	  • Prestataires de services de confiance
	  • Fournisseurs de réseaux de communications électroniques publics
	  • Fournisseurs de services de communications électroniques accessibles au public
		• La poste et services postaux
		• Alimentation (fabrication, production et distribution)
		• Recherche : établissements d'enseignement, organismes de recherche
		• Gestion des déchets
		• Marchés en ligne
		• Réseaux sociaux
		• Moteurs de recherche
		• Dispositifs de santé intelligents
		• Production industrielle : fabricants de dispositifs médicaux et de diagnostic in vitro, fabricants de produits informatiques, électroniques et optiques, fabricants d'équipements électriques fabricants de machines et équipements, constructeurs de véhicules automobiles, remorques et semi-remorques, fabricants d'autres matériels de transport
		• Produits chimiques (fabrication, production et distribution)
		• Fournisseurs et fabricants numériques

LES OBLIGATIONS DE NIS 2 POUR LES ENTREPRISES

— Les entités doivent **évaluer leurs risques en matière de cybersécurité** et adopter des mesures techniques et opérationnelles.

— Les obligations pour les entités régulées :
  - Notification, contact et déclaration des incidents majeurs ;
  - Notification à l'ANSSI : la France envisage de mettre en place un mécanisme permettant aux entités de se notifier auprès de l'ANSSI ;
  - Communication des informations de contact et mise à jour a minima : nom de l'entité, adresse et coordonnées actualisées, secteurs d'activité, liste des Etats membres de l'UE dans lesquels sont fournis les services ;
  - Déclaration à l'ANSSI des incidents majeurs avec une déclaration qui s'effectue en plusieurs étapes :
    - Notification,
    - Rapport d'avancement,
    - Rapport final.

— Ces mesures de sécurité sont comparables à celles contenues dans les normes de la famille ISO 27000 et de la norme américaine NIST.

— **Tests et audits de sécurité** : NIS 2 imposera aux entités de mener régulièrement des tests et des audits techniques dont des tests d'intrusions et scans de vulnérabilités pour évaluer l'efficacité des mesures de sécurité déployées.

— **Sécurité de la supply chain** : les entreprises devront effectuer des travaux de due diligence sur la chaine d'approvisionnement.

— **Signalement des incidents de sécurité** : Les entités entrant dans le champ d'application de NIS 2 doivent signaler sous 24 heures à compter de la survenance de l'incident tout incident de sécurité ayant un impact important sur son activité via un premier signalement à envoyer à l'ANSSI via un rapport préliminaire, ce dernier devra être complété par un rapport final sous un délai maximum d'un mois.

— Gestion des risques cyber : les entités devront porter une attention particulière à la formation de leurs décideurs à la gestion des risques. Les managers de ces entités auront l'obligation de contribuer au processus de validation des mesures de gestion des risques cyber.

— Mesures de sécurité prévues pour les entités rentrant dans le champ d'application NIS 2 :
  - Les politiques relatives à l'analyse des risques et la PSSI
  - La gestion des incidents
  - Les plans dédiés à la continuité de l'activité, à sa reprise, à la gestion des sauvegardes et des crises
  - Une obligation de sécurité de la chaîne d'approvisionnement (fournisseurs et prestataires) pour les entités essentielles et importantes. Les entités soumises à NIS 2 devront encadrer contractuellement les aspects cybersécurité avec leurs fournisseurs et prestataires directs
  - La sécurité de l'acquisition, du développement et de la maintenance des SI notamment le traitement et la divulgation des vulnérabilités
  - Des politiques et des procédures pour mesurer l'efficacité des mesures de gestion des risques en matière de cybersécurité
  - La mise en œuvre de pratiques de base (cyber hygiène et formation à la cybersécurité)
  - Des politiques et des procédures liées à l'utilisation de la cryptographie
  - La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
  - L'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue,
  - L'utilisation de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins

Calendrier d'application de NIS 2

L'ACCOMPAGNEMENT DES ENTREPRISES

LES PROGRAMMES CYBER RÉGIONAUX

La Région Auvergne-Rhône-Alpes ENTREPRISES

ene experts du numérique en entreprises Auvergne-Rhône-Alpes

CAMPUS RÉGION DU NUMÉRIQUE

Conseil Performance Industrie du Futur - volet Numérique :

- La thématique cybersécurité est traitée dans le cadre du dispositif régional « Industrie du Futur ». Ce dispositif est géré par l'Agence Auvergne-Rhône-Alpes-Entreprises et l'ENE.
- Les entreprises régionales peuvent bénéficier via ce dispositif d'accompagnements notamment la prise en charge de diagnostics et plan d'action.
- Parmi les axes du programme, l'axe Piloter / Usine Numérique ou connectée peut comporter un volet « Sécurité des données et Cybersécurité » pour sécuriser l'accès de l'information de l'entreprise et améliorer la fiabilité de votre SI.
- **La thématique de la cybersécurité dans le dispositif est renforcée en 2024** avec le lancement du nouveau dispositif « **Performance Industrie du Futur** ».
- **Plaquette du programme IDF**
  - 5 à 20 jours de **conseil** par des experts numérique
  - **Prise en charge à 50 %** sous forme de subvention
  - Aide plafonnée à 16 000 € HT
- **Critères d'éligibilité :**
  - Siège social en Auvergne-Rhône-Alpes
  - PME de 5 à 5000 salariées
  - Entreprise industrielle ou avec une activité de production
  - Projet informatique / Numérique autour de la production

Programme « Atouts Numériques » :

ATOUTS NUMÉRIQUES

- Ce programme vise **à accompagner les entreprises, en priorité celles de moins de 10 salariés** et ayant au moins deux ans d'activité, dans leurs projets numériques.
- Cet accompagnement gratuit, neutre et personnalisé permet notamment de traiter des sujets tels que la sécurité informatique des PME. Ce programme comporte par ailleurs un volet sensibilisation qui alimente régulièrement en contenus utiles le portail web du Campus Région du Numérique.

L'Usine du Campus Région du Numérique

- Le Campus Région du Numérique situé à Charbonnières-les-Bains (69) accueille une « Usine » digitalisée de 2 000 m² regroupant quatre plateformes technologiques et plus de cent équipements consacrés à l'industrie 4.0.
- Les consortia **SWARM*** (une entreprise à mission portée par les entreprises MGA technologies, Visiativ, Pixminds Innovation, Waoup, Moment Up en tant qu'actionnaires) et DIWII (un consortium porté par l'Ecole des Mines de Saint-Etienne avec 10 partenaires experts impliqués (Bosch Rexroth, Orange, Siemens, Atos, Equans Digital, Astrée Software, 1life, Quaternaire, Dative, Spectral et Kphitaine) proposent une offre de services dédiée pour accompagner les entreprises sur le sujet de la cybersécurité.
- L'Usine propose des prestations en cybersécurité telles que :
  - Un **escape game** « Nos moyens de production sont attaqués » qui sensibilisent les entreprises de façon ludique, aux enjeux et conséquences d'une cyberattaque (prestation SWARM)
  - Une **formation « Cybersécurité industrielle »** sensibilise les entreprises aux risques et menaces, aux bonnes pratiques et aux nouvelles méthodes des sécurisation afin d'initier une démarche de cybersécurité industrielle
  - Des **démonstrateurs et cas d'usages** présents en permanence sur la plateforme SWARM sur le sujet de la sécurité IT/OT
  - Des **diagnostics et audit** « cybersécurité » pour évaluer les risques, identifier les installations à sécuriser et moyens à mettre en place pour améliorer sa cyber-résilience
  - Trois parcours d'accompagnement pour permettre aux entreprises d'aller plus loin dans leurs démarches : « Cybersécurité industrielle » (3 à 5 jours par DIWII), « Cybersécurité en milieu industriel » (5 jours par SWARM) et « Cybersécurité COMEX » (SWARM)
- Le **Portail Digitalisation** :
  - Dans le cadre de sa mission d'animation de la transformation numérique des entreprises, le Campus référence sur son site internet https://campusnumerique.auvergnerhonealpes.fr/portail-transformation-digitale/ des dispositifs d'aide et d'accompagnement et des diagnostics. De même, des contenus autour de la cybersécurité ont été produits et sont désormais regroupés dans un dossier thématique: https://campusnumerique.auvergnerhonealpes.fr/dossier-special/cybersecurite/.

L'ÉCOSYSTÈME D'ACCOMPAGNEMENT DE LA CYBERSECURITÉ EN REGION

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

— Créée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Son action pour la protection de la Nation face aux cyberattaques se traduit en quatre grandes missions : défendre, connaître, partager, accompagner.

— Les délégués de l'ANSSI en Auvergne-Rhône-Alpes, en tant que spécialistes de la sécurité du numérique, œuvrent en synergie avec les structures et les autorités régionales existantes pour prévenir les incidents et sensibiliser les acteurs locaux du public et du privé aux bonnes pratiques informatiques

Le CLUSIR : le Club de la Sécurité des Systèmes d'Information Régional

— Le CLUSIR est une association ayant pour vocation de réunir les différents acteurs des filières de la cybersécurité en région Auvergne-Rhône-Alpes.

— L'association est organisée en clubs se réunissant mensuellement autour d'une thématique donnée.

— Le Club Ethical Hacking propose chaque mois aux membres des séances de travail sur les techniques utilisées par les pirates afin de mieux comprendre celles-ci et de mieux s'en prémunir

Digital League

— Digital League est un cluster qui réunit un écosystème de 452 adhérents en Auvergne-Rhône-Alpes, des entreprises, des écoles, des laboratoires et des investisseurs.

— Digital League a pour mission de favoriser le développement des entreprises du numérique en région, de promouvoir l'écosystème et de soutenir l'innovation et la croissance de l'industrie numérique dans la région. Un club cybersécurité permet de réunir les Référents Cybersécurité et Responsables SSI à échéances régulières.

— La cybersécurité est avec l'IA et le GreenIT un des vecteurs de développement de l'association qui est très active dans ce domaine : club cyber, co-organisation des Journées Cyber, organisation d'une délégation à la RSA

L'ENE : Les Experts du Numérique en Entreprises

— 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. La structure mène des missions d'information, d'accompagnement, d'expérimentation, d'anticipation, de pilotage et de partage.

— L'ENE pilote le programme régional Industrie du Futur et propose un Diag Cyber aux entreprises de la métropole lyonnaise de moins de 50 salariés pour les accompagner vers un renforcement du niveau de protection cyber de leur entreprise

Minalogic

— 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.

— Minalogic se veut être le fer de lance de l'innovation en matière de cybersécurité, mais aussi de l'appropriation des risques cybers par ses adhérents.

— Porté par les enjeux stratégiques et forts de son partenariat avec le Ministère des Armées, le pôle développe une activité dédiée aux domaines de la défense et de la cybersécurité, au cœur des nouveaux objectifs actuels de souveraineté. Minalogic intervient notamment sur 5 compétences : audit, analyse et gestion des risques ; IoT – Security by Design ; Cyber Physical System ; IA et Machine Learning ; Formation et Serious Game. Le pôle a par ailleurs publié un annuaire des sociétés adhérentes, intervenant sur le sujet large de la sûreté – sécurité

L'ADIRA : Association pour le Digital et l'IT en Région Auvergne-Rhône-Alpes

— Née en 1969, l'ADIRA rassemble aujourd'hui 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 Recrutements & Rémunérations, 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.

— Groupe de Travail ADIRA RSSI : Constitué uniquement de Responsables Sécurité des Systèmes d'Informations de PME, ETI et grands groupes, ce groupe de travail se réunit mensuellement pour partager une veille et des retours d'expériences. Il constitue une communauté de partage pour les RSSI, permettant de maximiser leurs connaissances de la menace cyber et les préconisations de gouvernance, organisationnelles et techniques pour protéger leurs structures.

— **GT Cyber** : rassembler les experts Cyber de l'association aussi bien issus d'entreprises utilisatrices, prestataires ou encore institutionnels.

Le CyberCercle Auvergne-Rhône-Alpes

— Le CyberCercle est un cercle de réflexion lyonnais sur la cybersécurité, et animateur d'une communauté locale sur ce sujet

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

MINALOGIC Auvergne-Rhône-Alpes
DIGITAL LEAGUE Auvergne-Rhône-Alpes
cea
CLUSIR Auvergne-Rhône-Alpes
ene experts du numérique en entreprises Auvergne-Rhône-Alpes
CAMPUS RÉGION DU NUMÉRIQUE
ADIRA
GRENOBLE INP UGA
Esisar VALENCE
LCIS Laboratoire de Conception et d'Intégration des Systèmes

Sources complémentaires

orange Cyberdefense
ACN Alliance pour la confiance numérique
CESIN
Microsoft

Réalisé par :
Corentin Bonnefois
Analyste sectoriel et territorial | cbonnefois@arae.fr

Avec le soutien de :
Hervé Mialon
Chef de projet Cybersécurité | 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