



LES JEUNES

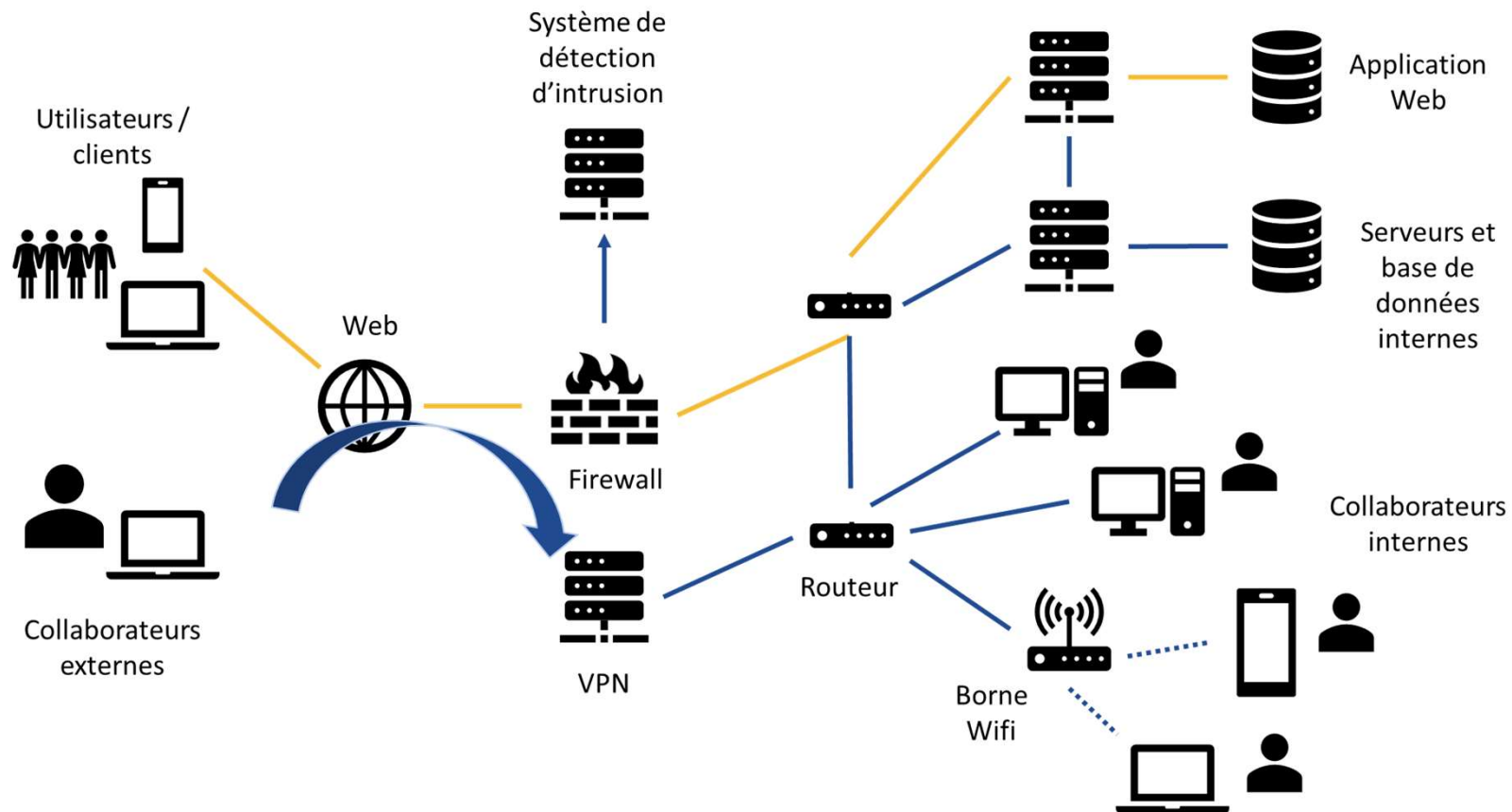
IHEDN

L'association

Les métiers de la cybersécurité

PRÉSENTÉS PAR QUENTIN BÉDÉNEAU, VINCENT BRIFFAUX ET NOÉMIE TOSI

Modélisation d'un système d'information



Jeune

Intermédiaire

Expérimenté

Connaissance technique

Développeur

Technicien

Administrateur

Cryptologue

Expert réponse
à incident

Chef de Projet

Analyste SOC

Intégrateur

Auditeur

Ingénieur
Cybersécurité

Architecte
système

Consultant
fonctionnel

Correspondant
sécurité

Analyste
threat intel

Consultant
technique

RPUPA

RSSI

Commercial

Assureur

DPO

Juriste

RH

Achat

Chargé de
communication

Formateur

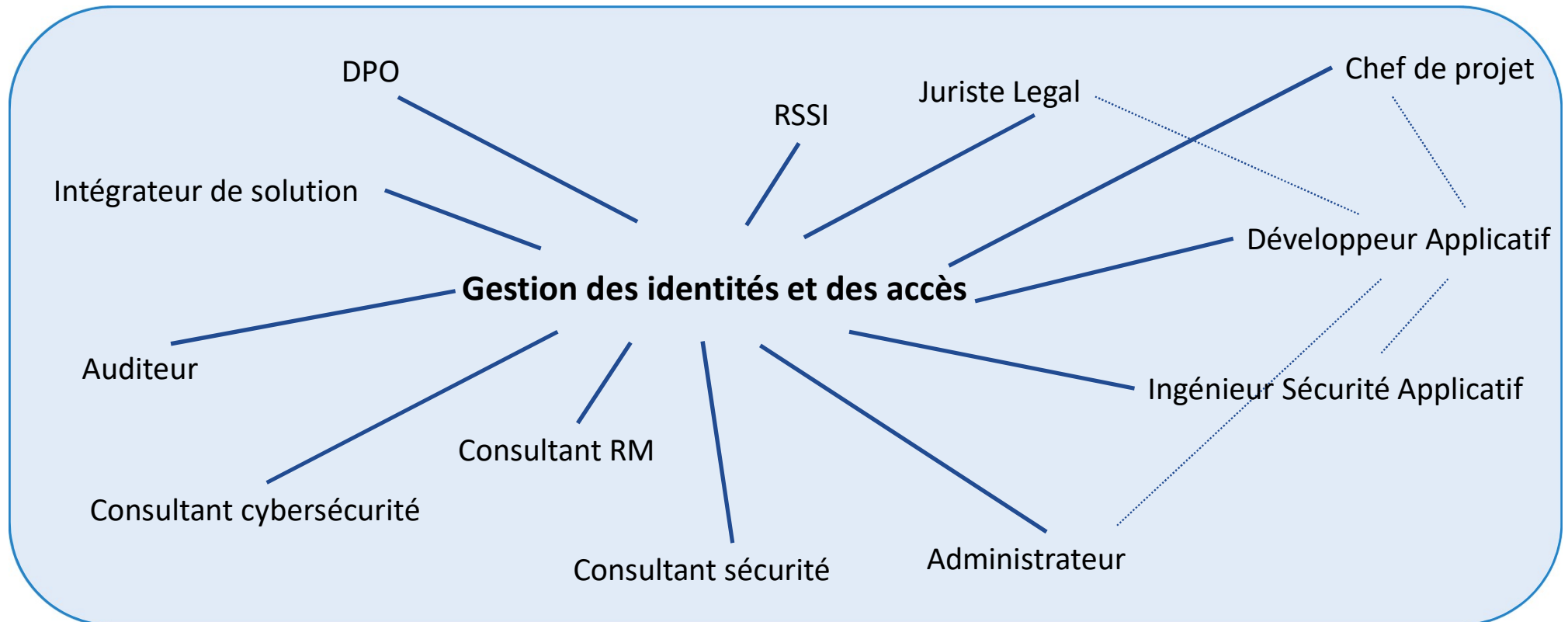
Cartographie des métiers

Intégrateur(e)



- Met en place un système logiciel ou composant dans le SI de l'entreprise

Noémie Tosi : Consultante IAM

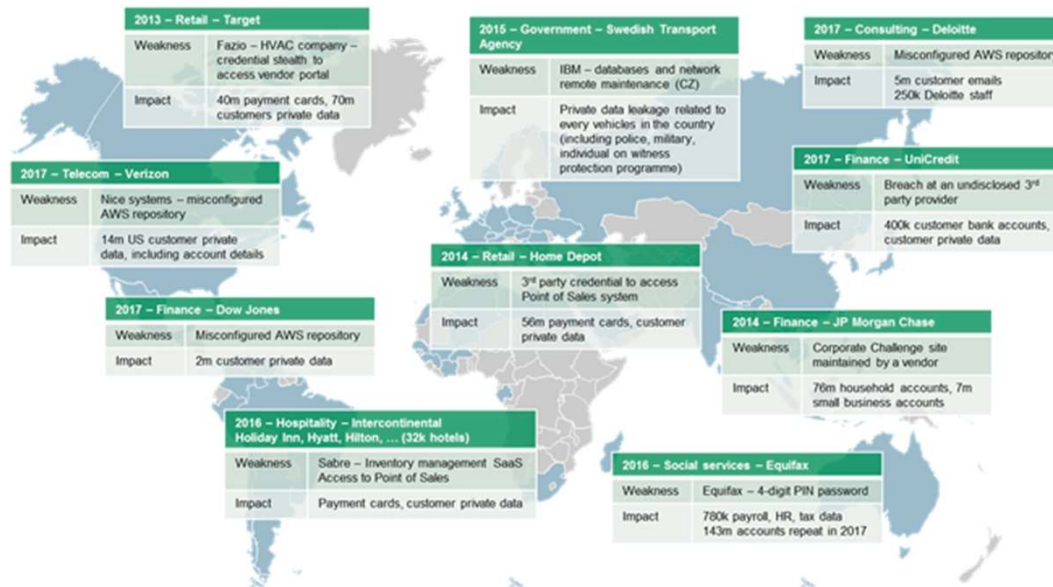


Vincent Briffaux : Gestion de risques

Contexte

- Projets de transformation
- Audits Sécurité de l'information
- **Projet de cybersécurité**
définition, d'opération et amélioration d'une politique de gestion de risques fournisseurs pour un grand groupe d'une trentaine de localisations (worldwide) et métiers

Pourquoi la gestion de risques fournisseurs ?



Quels challenges ?

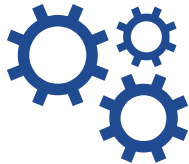
Quelle démarche et quels acteurs ?

Vincent Briffaux : Gestion de risques

Risque

ISO 31000

Effet de l'incertitude sur les objectifs



Activités

- Définir les exigences à couvrir *régulations, standards*
- Déployer, opérer et vérifier la couverture effective



Gains

- Couverture des risques
- Respects des réglementations
- Amélioration de la maturité



Challenges

- Changements réglementations
30+ pays / secteurs
- Techniques et outils du marché peu matures

Identifier

ce qui doit être protégé, pourquoi, par qui, où

Protéger

au travers d'activités (éviter, prévention, transfert ...)

Détecter

les événements (incidents, non-conformité, anomalies...) au travers d'audits, d'évaluations d'outils de supervision ...

Répondre aux incidents

Rétablir dans les conditions normales

Analyste SOC

Assureur

Juriste

RH

Achat

Chargé de communication

Formateur

Cryptologue

Expert réponse à incident

Chef de Projet

Consultant technique

Auditeur

Ingénieur Cybersécurité

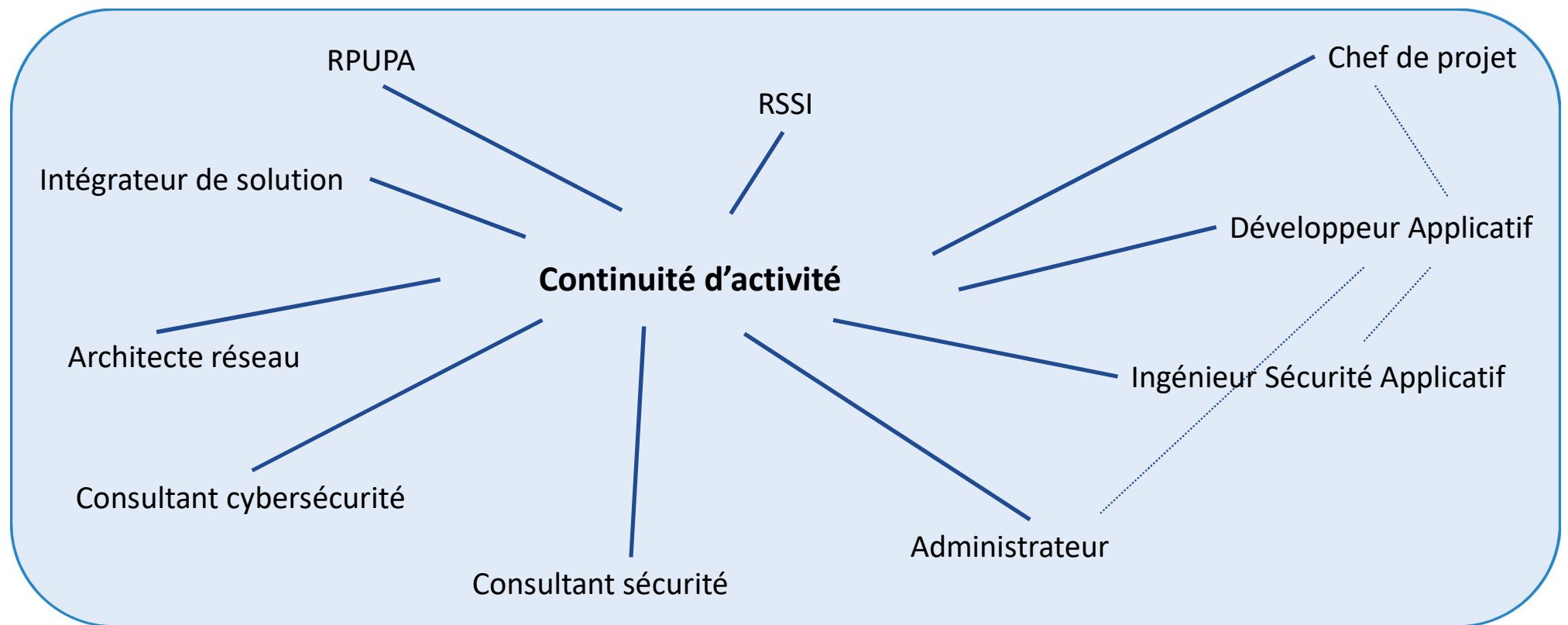
Consultant fonctionnel

Correspondant sécurité

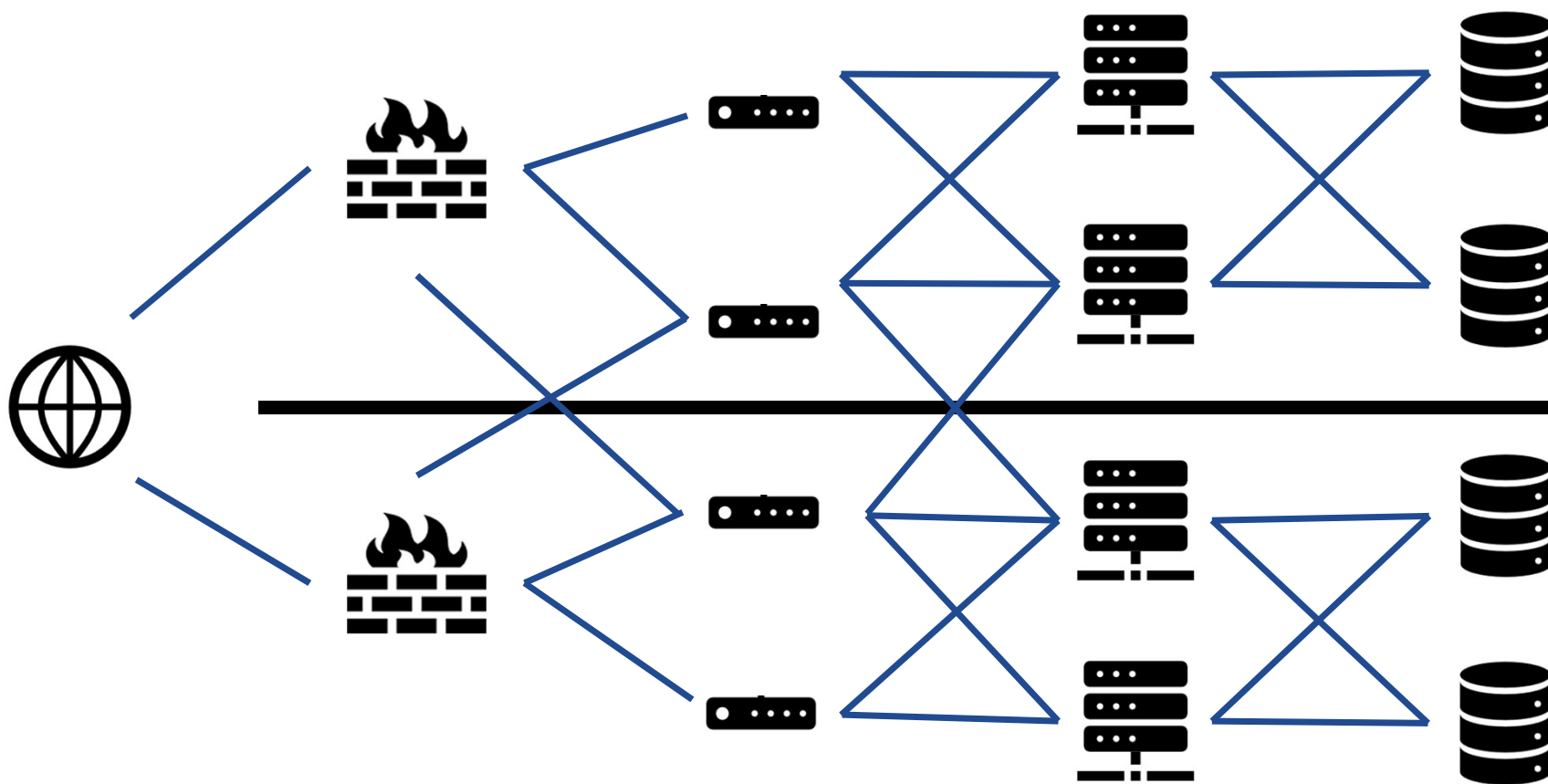
RSSI

DPO

Quentin Bédéneau : Continuité d'activité



Plan de reprise d'un datacenter



Contacts



**LES JEUNES
IHEDN**

L'association

Comité Cyber:

- Mail cyber@anaj-ihedn.org

Comité Nord :

- Mails nord@anaj-ihedn.org ou fthieffry.pro@gmail.com

Quentin Bédéneau

- Twitter : @QuentinBBd
- Mail : quentin@datatemplar.fr

Vincent Briffaux

- Mail : vincent@briffaux.com

Noémie Tosi

- Mail: noemie.tosi@gmail.com

Baseline Skills

1 You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Techniques | Prevent, Defend, Maintain

Every Security Professional Should Know

Security Essentials SEC401 Security Essentials Bootcamp Style | **GSEC**

Hacker Techniques SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling | **GCHN**

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attackers work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

New to Cybersecurity SEC301 Introduction to Cyber Security | **GISC**

1b You will be responsible for managing security teams or implementations, but you do not require hands-on skills

Security Management | Managing Technical Security Operations

Every Security Manager Should Know

Leadership Essentials MGT512 Security Leadership Essentials for Managers | **GSLC**

Critical Controls SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Focus Job Roles

2 You are experienced in security, preparing for a specialized job role or focus

Monitoring & Detection | Intrusion Detection, Monitoring Over Time

Scan Packets & Networks

Intrusion Detection SEC503 Intrusion Detection In-Depth | **GICIA**

Monitoring & Operations SEC511 Continuous Monitoring and Security Operations | **GMON**

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Penetration Testing | Vulnerability Analysis, Ethical Hacking

Every Pen Tester Should Know

Networks SEC560 Network Penetration Testing and Ethical Hacking | **GPEN**

Web Apps SEC542 Web App Penetration Testing and Ethical Hacking | **GWAPT**

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking, and different tools, but is essential for defense specialists to improve their defenses.

Incident Response & Threat Hunting | Host & Network Forensics

Every Forensics and IR Professional Should Know

Endpoint Forensics FOR500 Windows Forensic Analysis | **GCFE** | FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting | **GICIA**

Network Forensics FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | **GNFA**

Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

CISSP® Training MGT414 SANS Training Program for CISSP® Certification | **GISP**

Crucial Skills, Advanced, or Specialized Roles

SANS comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

3 You are a candidate for specialized or advanced training

Cyber Defense Operations | Harden Specific Defenses

Specialized Defensive Area

Advanced Generalist SEC501 Advanced Security Essentials – Enterprise Defender | **GCED**

Cloud Security SEC545 Cloud Security Architecture and Operations

Windows/PowerShell SEC505 Securing Windows and PowerShell Automation | **GCWN**

Linux/Unix Defense SEC506 Securing Linux/Unix | **GCIUX**

Virtualized Data Centers SEC579 Virtualization and Software-Defined Security

SIEM SEC555 SIEM with Tactical Analytics | **GCDA**

Other Advanced Defense Courses

Critical Controls SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**

Security Architecture SEC530 Defensible Security Architecture

Threat Defense SEC599 Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses | **GDAT**

Specialized Penetration Testing | Focused Techniques & Areas

In-Depth Coverage

Vulnerability Assessment SEC460 Enterprise Threat and Vulnerability Assessment

Networks SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GPWN**

Web Apps SEC760 Advanced Exploit Development for Penetration Testers

Mobile SEC642 Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques

Wireless SEC575 Mobile Device Security and Ethical Hacking | **GMOB**

Hands-On Ranges SEC617 Wireless Penetration Testing and Ethical Hacking | **GAWN**

Python Coding SEC573 Automating Information Security with Python | **GPYC**

Digital Forensics, Malware Analysis, & Threat Intel | Specialized Investigative Skills

Malware Analysis

Malware Analysis FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM**

Threat Intelligence

Cyber Threat Intelligence FOR578 Cyber Threat Intelligence | **GCTI**

Digital Forensics & Media Exploitation

Smartphones FOR585 Advanced Smartphone Forensics | **GASF**

Memory Forensics FOR526 Memory Forensics In-Depth

Mac Forensics FOR518 Mac Forensic Analysis

Advanced Management | Advanced Leadership, Audit, Legal

Management Skills

Planning, Policy, Leadership MGT514 Security Strategic Planning, Policy, and Leadership | **GSTRY**

Project Management MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM**

Audit & Legal

Audit & Monitor AUO507 Auditing and Monitoring Networks, Perimeters & Systems | **GSNA**

Law & Investigations LEG523 Law of Data Security and Investigations | **GLEG**

Industrial Control Systems

ICS Security Professionals Need

Essentials ICS410 ICS/SCADA Security Essentials | **GICSP**

ICS Defense & Response ICS515 ICS Active Defense and Incident Response | **GRID**

NERC Protection

NERC Security Essentials ICS456 Essentials for NERC Critical Infrastructure Protection | **GCIPI**

Development & Secure Coding

Every Developer Should Know

Secure Web Apps DEV522 Defending Web Applications Security Essentials | **GWEB**

Secure DevOps DEV540 Secure DevOps and Cloud Application Security

Language-Specific Courses

JAVA/JEE DEV541 Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA**

.NET DEV544 Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET**

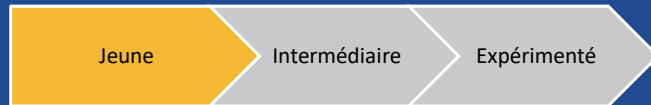
Roadmap des certifications

Roadmap des certifications techniques du SANS institute



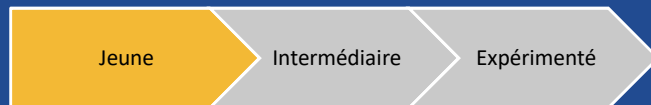
Métiers Techniques

Développeur (e)



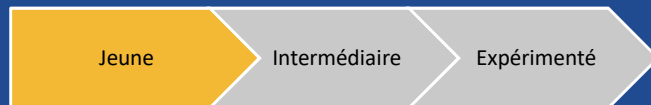
- Développe les logiciels dédiés à la sécurité ou non
- Connaissances en langages de programmation

Technicien(ne)



- Gère l'administration du parc informatique avec des tâches courantes

Analyste SOC



- Suit les alertes relevées par les systèmes de sécurité
- Peut faire de l'investigation

Consultant (e) technique



- Expert dans un domaine ou produit spécifique
- Vend son expertise

Administrateur système

Jeune

Intermédiaire

Expérimenté



- Maintien en condition le parc informatique.
- Expert en système d'exploitation (Linux, Windows)

Cryptologie

Jeune

Intermédiaire

Expérimenté



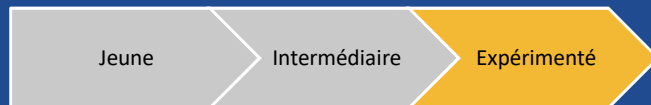
- Travaille sur des problèmes mathématiques
- Peut chercher la meilleur solution de chiffrement ou
- Attaquer un système de chiffrement

Intégrateur (e)



- Met en place un système logiciel ou composant dans le SI de l'entreprise

Expert (e) Réponse à incident



- Intervient en cas d'attaque informatique pour déterminer la cause et proposer un plan de remédiation
- En anglais le poste est lié au Forensic

Auditrice - Auditeur



- Valide la conformité d'un système d'information
- Si très technique = pentester

Ingénieur (e) Cybersécurité Cyberdéfense

Jeune

Intermédiaire

Expérimenté



- Supervise la gestion des systèmes de sécurité du SI

Architecte de systèmes

Jeune

Intermédiaire

Expérimenté



- Défini les interactions entre chaque composant du SI



Métiers Fonctionnels

Chargé(e) de communication / gestion de crise

Jeune

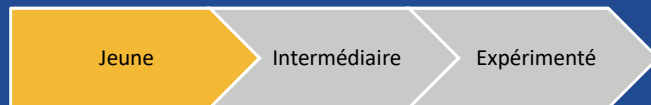
Intermédiaire

Expérimenté



- Gère la communication interne comme externe liée à la gestion de crise

Consultant (e) fonctionnel



- Expert dans des sujets d'organisation ou de processus

Chef (fe) de projet

Jeune

Intermédiaire

Expérimenté



- Gère le suivi d'un projet sécurité

Correspondant (e) sécurité



- Travaille sur d'autres sujets dans l'entreprise
- Sensibilise ses collègues à la cybersécurité
- Echange avec le RSSI

Analyste threat intel

Jeune

Intermédiaire

Expérimenté



- Echange sur des réseaux spécialisés sur des indicateurs de compromissions
- Transmet ses analyses à l'ingénieur cybersécurité pour intégrer les indicateurs dans les outils de sécurité

Officier de protection des données

Jeune

Intermédiaire

Expérimenté



- Responsable de la protection des données personnelles
- Assure la mise en conformité du GDPR

Responsable du plan d'Urgence et de la Poursuite d'Activité

Jeune

Intermédiaire

Expérimenté



- Prépare le plan de continuité d'activité en cas d'une panne informatique

Responsable de la Sécurité du Système d'Information

Jeune

Intermédiaire

Expérimenté



- Coordonne les actions pour améliorer le niveau de sécurité du SI



Métiers supports

Juriste

Jeune

Intermédiaire

Expérimenté



- Suit les réglementations liées à la cybersécurité

Commercial(le) / Business developer

Jeune

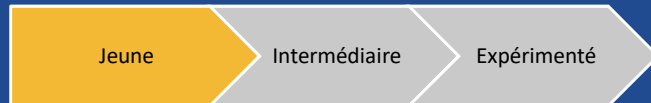
Intermédiaire

Expérimenté



- Recherche des clients pour les produits ou services qu'il vend

Responsable de ressource humaine / Recruteur



- Supervise la carrière du personnel en proposant des formations, des augmentations ou des changements de poste

Formateur / autorité de certification

Jeune

Intermédiaire

Expérimenté



- Donne des cours pour passer une certification en cybersécurité

Assureur



- Propose des assurances liées au risque cyber. Eg: Suite à une attaque ou une défaillance du SI, peut apporter une compensation financière

Responsable achat



- Valide les contrats liés à l'achat de produits ou services vendu par un commercial

Sources



<https://www.ssi.gouv.fr/particulier/formations/profils-metiers-de-la-cybersecurite/>

<https://www.cybrary.it/wp-content/uploads/2017/07/Interactive-Cyber-Security-Career-Roadmap.pdf>

<https://www.sans.org/cyber-security-skills-roadmap>

<https://certification.comptia.org/why-certify/roadmap>

<https://www.cybersecurityeducation.org>

