CYBER DEFENSE SERVICES OVERVIEW

MICROSOFT SENTINEL

CAPGEMINI CYBERSECURITY

June 2022

CYBER DEFENSE SERVICES

SOC, Monitor your risks from everywhere on everything and respond to security incident

What kind of SOC do you want?

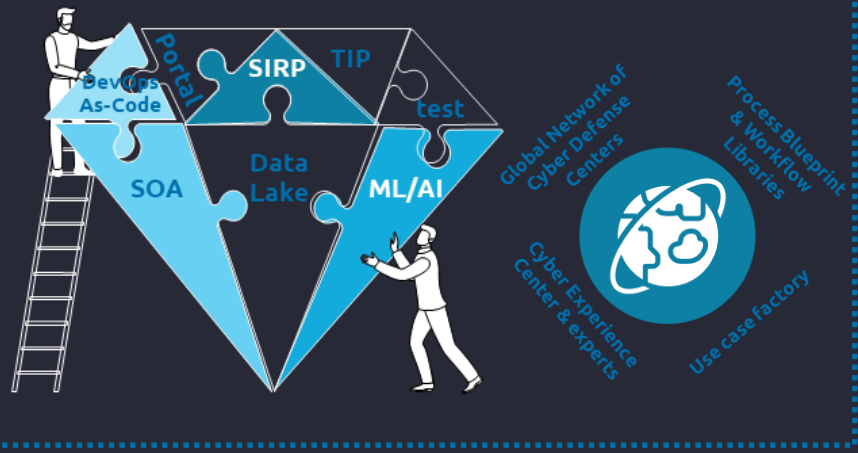
Our clients' challenges

- Get and maintain **the right visibility** over heterogenous environments to quickly and accurately detect data breaches and security incidents
- Deploy an efficient, intelligence driven, business risk driven, and measurable incident analysis and response process being able to spot on and **manage critical security incidents** before they impact the organization on its business.
- Ability to detect advanced threats and anticipate the next hacker's move.
- Get access to highly skilled security professional

Capgemini Group Service line

Capgemini, thanks to more than **1600 analysts** based around the world (India, Spain, Poland, France, …), can provide an end-to-end service tailored for each client with on-near-offshore delivery model to ensure :

- SOC Transformation
- Incident anticipation
- Incident detection
- Incident response



Service components on this service line

- **24/7** or **8/5+on-call** duty security monitoring service
- Monitoring on IT / IoT / OT / Cloud
- Advanced monitoring capabilities with UEBA and IA
- Use-Case Factory to enhance detection capabilities
- Mutualized, Dedicated, Hybrid delivery model
- Threat Intelligence driven investigation and detection
- Internal **Capgemini CERT** to feeds our Threat Intelligence platform
- **Threat Hunting**, investigation and forensics service
- Incident coordination and **breach management**
- Standard and complex incident remediation support
- **Automation** (SOAR) to enhance remediation tasks
- Business driven **prioritization**
- **Qualified and certified analysts** and **proven** security processes

AGENDA

1. Introduction to CAPGEMINI Cyber-Security
2. Cyber Defense Service OVERVIEW
3. CAPGEMINI and MICROSOFT Partnership
4. Next Step

1

INTRODUCTION TO CAPGEMINI CYBER-SECURITY

CAPGEMINI, A GLOBAL LEADER IN CYBERSECURITY

OUR NATIONAL EXPERTISE

Global presence with 11 point of presence

800 consultants and experts deployed in France

- Advisory
- Cyber Defense Centers (SOC, CERT, SWAT)
- Digital identity
- Risk management
- Audit & offensive security
- OT security
- Infrastructure and cloud sec

OUR FRENCH LABELS

VISA DE SÉCURITÉ – ANSSI

PDIS, PASSI et PASSI LPM

EXPERT CYBER – LABEL SÉCURITÉ NUMÉRIQUE – Cybermalveillance.gouv.fr – RÉPUBLIQUE FRANÇAISE

CAMPUS CYBER

Founding Member

OUR WORLDWIDE NETWORK

5 000+ experts worldwide

For broader protection

A worldwide network of Cyber Defense Centers & SOC « Follow-the-Sun »

- **Innovation center & cyber range**
- **Local expertise** connected with our clients teams

AN END TO END CYBERSECURITY PORTFOLIO

Core GTM Areas

- Assess, Test, & Advise
- Identity & Access Management
- Application Security & DevSecOps
- Cloud Security
- OT/IoT Security
- Data Protection
- Managed Detection & Response
- Infrastructure Security

Services and Expertise

Define

- Maturity Evaluations & Framework Assessments
- *Security Architecture & Technology Roadmaps*
- Governance, Risk, and Compliance
- Security Testing and Threat Simulation
- Strategic Consulting & Transformation Planning

Protect

- Security Architecture, Engineering, & Deployment
- Security Orchestration, Automation, and Analytics
- OT-IoT Security Engineering
- IAM Operations
- Application & Data Security

Defend

- Cyber Defense Center and MDR (Managed Detection & Response)
- Threat Intelligence
- Threat Hunting
- Incident Response & Remediation
- Vulnerability Management
- *Specialized SOC (V-SOC, OT-SOC, etc.)*

Safeguard

- Intelligent Industry & 5G/IoT
- ERP Security
- Security Platform Services
- Industry focused solutions

Accelerators and enablers

- Global Network of Cyber Defense Centers
- Factory Delivery Models (IAM, UC, etc.)
- Process Blueprint & Workflow Libraries
- Custom Methodologies & Frameworks
- Cyber Experience Center

2

CYBER DEFENSE SERVICE OVERVIEW

SOC Customer challenges

Combines integrated technology and human expertise to address the threat landscape

Lack of visibility over the data breaches

Slow and inefficient incident analysis and Response process

Too many tools and difficulty in **securing all the endpoints**

Too many data and alerts making difficult in **identifying critical incidents**

Threat feeds with **ad-hoc** and **missing business context**

Lack of actionable **security metrics** without effective prioritization and context

Adoption of **latest digital technologies**

Lack of dedicated and highly **skilled team**

CAPGEMINI CYBER DEFENSE SERVICES – DELIVERY MODEL

Our Services are offered as a Dedicated Customer Service or through a Multi-tenant Platform with a range of Managed Service Levels

Mutualized

- **Industrialized CDC services** capability through the **Global Network** of **CDCs**
- Allows **Easy** & **Quick** access to **Comprehensive Security Solutions**
- Supports **Security Operations** in **Local Language** & **Local Presence**
- **Best ROI –** results- and KPI driven

Dedicated

- Tailored and exclusively **Designed CDC** to suit a **Client's Security Needs** & **Individual Risk Profile**; Operated either **In-house** or in a **Capgemini Location**
- Protects **Sensitive Data**
- Supports **Compliance** with **Local Legal** & **Regulatory Mandates**

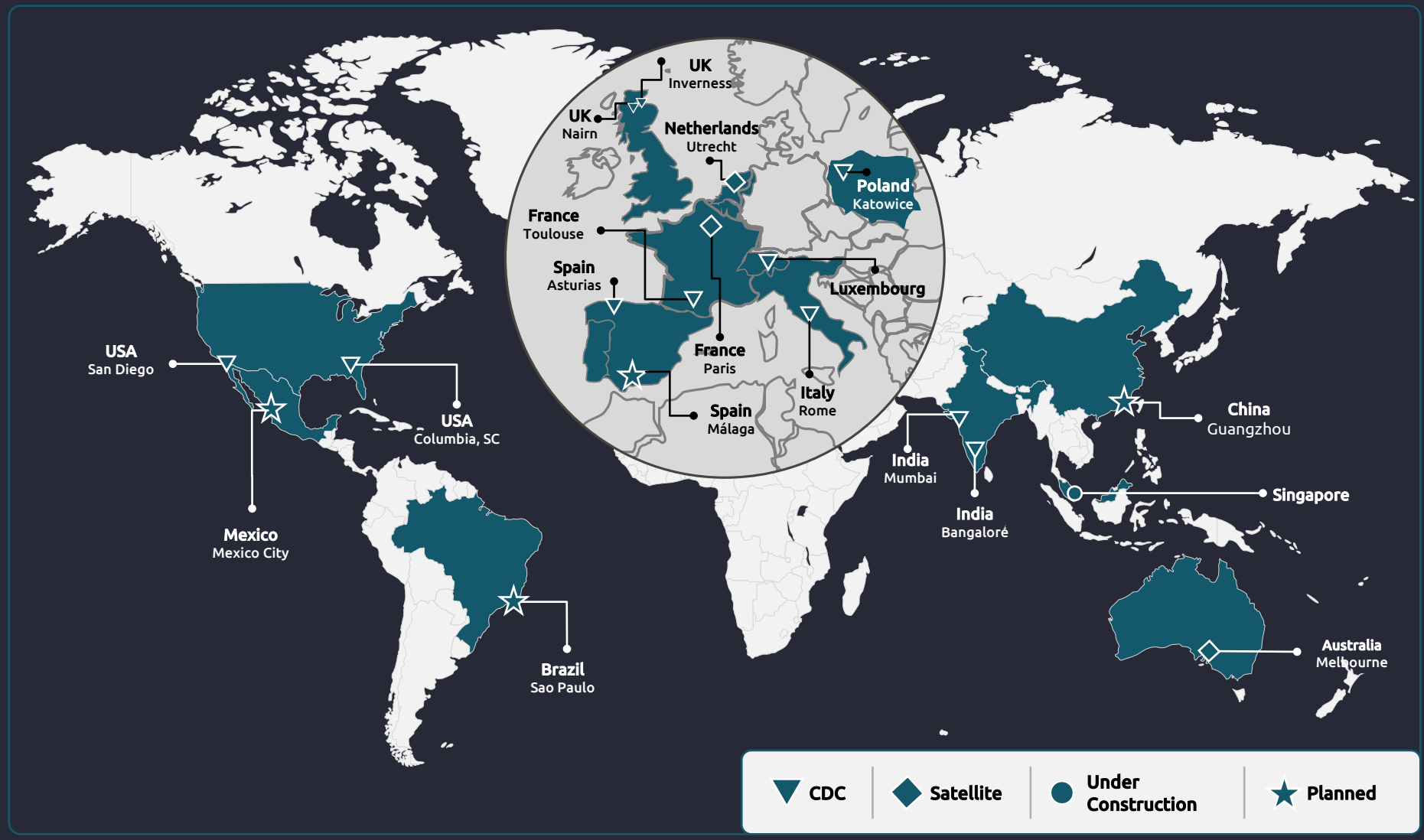
Hybrid

- Uses both **Off-Near shore** and **Mutualized** and/or **Local Resources** in a single seamless **CDC** after determining the best balance between **Client's Resources** and **Our 0wn**
- Improves a **Client's Productivity**, **Predictability** and **Responsiveness**, while reducing **Costs**, **Risks** and **Workload** for their teams

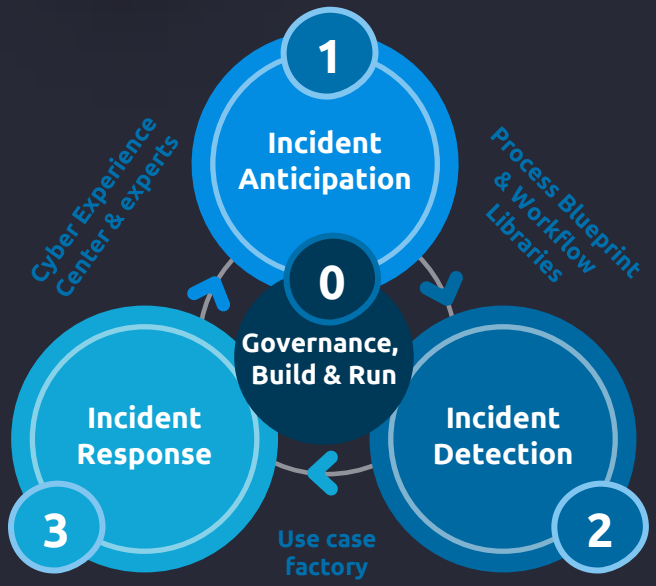
GLOBAL SECURITY OPERATION CENTER (SOC) NETWORK

We Deliver the Advice and Managed Services Tailored to our Clients' needs, anywhere in the World.

- Global Network of **13** connected CDCs and Research Labs
- Presence in more than **50+** Countries
- Vast Experience with Businesses of all Types and Sizes in Every Industry
- **5000+** cybersecurity professionals Globally



CAPGEMINI CYBER DEFENSE SERVICES – SERVICE COMPONENTS



Security Operations Centers (SOCs) orchestrate the multiple roles, processes and technology needed to enable efficient incident anticipation, detection, analysis and response.

Governance & Operations

- SOC Governance & Reporting
- SOC Platform build & run
- SOC Transformation & Maturity Assessment

Incident Anticipation

- Threat Management
- Vulnerability Management
- Incident Management readiness

Incident Detection

- Use case management (Use case factory)
- Security supervision (IT, OT, IoT, Cloud)
  - SIEM / EDR / NDR / Machine learning / UEBA
- Analysis & Analytics

Incident Response

Capgemini CERT

- Response Management
- Digital Forensics & Investigation
- Incident Remediation

Automation & Orchestration
Continuous Improvement & Innovation

IT Systems | Cloud | OT & IoT Systems

Capgemini CDC architecture overview

Service and Capability model

CDC Services

Governance & Operations

Incident Anticipation

Incident detection

Incident Response

24/7

CDC Services

CLIENT

- Business Executive
- CISO office
- Security operations
- Security SMEs
- IT operations

Customer portal

Search Engine

Analytic Engine

Playbook Factory

Use Case Factory

Ticketing

Security Orchestration and Automation platform (SOAP)

Security Incident response, Knowledge & Case Mgmt. Platform. (SIRP)

Threat Intelligence Platform (TIP)

Dark/Deep/Clear web indexes

Internal / External Feeds

Data Lake

DevOps

Test

As-Code

CDC Capabilities

SIEM

Multi-platform Protection & Detections

UEBA

Endpoint Detection & Response (EDR)

Network Detection & Response (NDR)

CDC Visibility

IT Systems

Cloud

OT & IoT Systems

Capgemini CDC architecture overview

CDC Service component catalogue – MICROSOFT SENTINEL

0.1 SOC Governance and reporting
- Security Governance
- Security Operational Reporting

0.2 SOC Platform build & run
- Design and build
- Maintenance of operational conditions
- Maintenance of security conditions

0.3 SOC Transformation
- Maturity assessment
- Transformation roadmap
- Technology POV/POC

1.1 Threat management
- Threat Intelligence Management
- Dark/Deep/Clear web watch
- Threat hunting

1.2 Vulnerability management
- Vulnerability scan
- Vulnerability watch
- Application security testing
- Pen-testing & attack simulation
- Bug bounty
- Patch management

1.3 Incident management readiness
- Security awareness & wakefulness
- Red-Blue-Purple teaming
- Crisis and breach exercises
- Crisis mgt. process update
- Incident remediation checklist
- Incident remediation process testing

2.1 Security supervision (IT, OT, IoT, Cloud)
- Log management
- Use case management

2.2 Analysis & Analytics
- Incident analysis & qualification
- Business risk-based security incident handling
- Behaviour analysis
- Extended analytic based Incident analysis
- Playbook management

3.1 Response management
- Incident coordination
- Breach & security crisis management

3.2 Forensics & investigation
- Digital investigation & forensics
- Malware analysis

3.3 Incident remediation
- Standard incident remediation
- Complex incident remediation

MICROSOFT based service component

Optional CDC service component

KEY METRICS

15%

False positive

In average, thanks to CAPGEMINI use case factory, playbook factory and delivery feedback loop, CAPGEMINI reach the score of **15% alert false positive across all our clients**

10 min

Efficiency

In average, it takes **10 minutes to deploy 40 detection altering rules**

80%

Automation

80% of SOC analyst's tasks is automated

3

CAPGEMINI AND MICROSOFT PARTNERSHIP

CAPGEMINI PARTNERSHIP WITH MICROSOFT AT A GLANCE

Our Partnership

- More than **22 years managed partnership** driving Digital Transformation with joint enterprise customers worldwide
- **Joint business framework** in place to drive €4.5Bn Capgemini bookings across 3yrs and $1Bn ACR in the next 3yrs: (FY20/21/22) across three domains (Enterprise Portfolio Modernization, Data & AI, Digital Manufacturing and Industrial IoT)
- **Alliance governance** presence in five continents (Asia Pacific, Australia, North & South America, Western & Eastern Europe) combining more than 60 FTEs to manage it on both sides
- Involved in the **Cloud Early Adopter** programs and **Azure Advisory Councils (Cloud, DevOps, SAP, Security)**
- Dedicated Microsoft Cloud Solution Architects (**CSAs**) & access to Global Black Belts

Global Capabilities

- Heavy focus on capabilities with **70K trained FTEs globally**
- Over **7000 total certified FTEs** ramping to 10000+ within 3yrs
- Microsoft Azure specialists in Center of Excellence (CoE) with **IaaS**, **PaaS and SaaS** expertise
- **Microsoft Managed Service Provider (MSP)** Azure Expert

Gold Microsoft Partner | Azure Expert MSP

- **Cloud Solution Provider (CSP)** with global Center or Excellence

Microsoft Cloud Solution Provider (CSP)

- Access to Premier Support and Azure sandbox environments with $750k available for customers POC

Competencies

18 Microsoft Gold Competencies

Gold Microsoft Partner

- Gold Security
- Gold Cloud Platform
- Gold Cloud Productivity
- Gold Collaboration and Content
- Gold Communications
- Gold Enterprise Mobility
- Gold Datacenter
- Gold DevOps
- Gold Application Development
- Gold Application Integration
- Gold Cloud Business Applications
- Gold Data Analytics
- Gold Data Platform
- Management
- Gold Enterprise Resource Planning
- Gold Messaging
- Gold Project and Portfolio Management
- Gold Small and Midmarket Solutions
- Gold Windows and Devices

2019-2020 Focus:

- **Enterprise Portfolio Modernization Initiative** Offerings: Application Modernization, SAP/Azure, Cloud Native & Datacenter Transformation
- **Data & AI**
  Offerings: Unified Data Mgmnt, Data Estate Modernization, Industrialized AI & Analytics
- **Digital Manufacturing & Industrial IoT** with vertical solutions such as 'Factory of the Future' and 'Connected Vehicles' leveraging the Azure IoT platform (Capgemini is part of the IoT Elite Partner program).

- 2020 Data Analytics Partner of the Year award (runner-up)
- 2020 Proactive Customer Service Partner of the Year award (runner-up)
- Capgemini Spain - Partner of the Year in Management Cloud Services
- 2019 Microsoft SAP / Azure Partner of the Year
- 2019 Microsoft SAP / Azure Advanced Specialization
- 2019 Microsoft Mixed Reality Partner, France
- 2018 Microsoft Country Partner of the Year, France

Recent Microsoft Partner Award

Winner Microsoft Partner 2019 Partner of the Year SAP on Azure Award Microsoft

CAPGEMINI: MICROSOFT – CYBERSECURITY

Partnership status

•More than **20 years managed partnership** driving Digital Transformation with joint enterprise customers worldwide

•**Joint business framework** in place to drive €4.5Bn Capgemini bookings across 3yrs and $1Bn ACR in the next 3yrs: (FY20/21/22) across three domains (Enterprise Portfolio Modernization, Data & AI, Digital Manufacturing and Industrial IoT)

•Involved in the **Cloud and Security Early Adopter** programs and **Azure Advisory Councils (Security, Network, End point, SOC, DevOps, SAP,)**

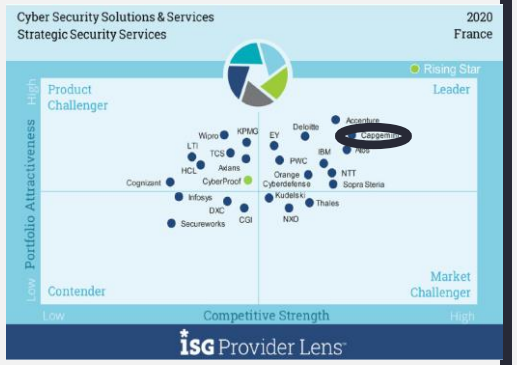
•Dedicated Microsoft Cloud and Security Solution Architects (**CSAs**) & access to Global Black Belts

Global Capabilities

- 2020 :
  Number of Cyber Skill Training: +2000
  Number of Cyber Certification : +1000
  (SC900, AZ500, MS500, SC200, SC300, SC400)

- Magic Quadran

Advisor Vision : Capgemini Cyber Services positioning



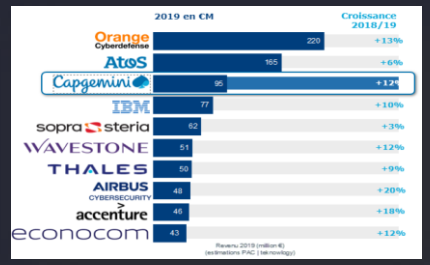
Skills

- Gold Security
- Gold Cloud Platform
- Gold Cloud Productivity
- Gold Cloud Business Application
- Gold Datacenter
- Gold Data Platform
- Gold Messaging
- Gold Windows and Devices
- Gold Collaboration and Content
- Gold Communications Gold DevOps
- Gold Enterprise Mobility Management
- Gold Application Development
- Gold Application Integration
- Gold Data Analytics
- Gold Enterprise Resource Planning
- Gold Project and Portfolio Management
- Gold Small and Midmarket Solutions

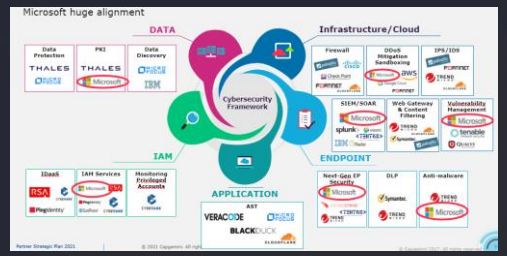
Gold Microsoft Partner — Azure Expert MSP

Our Value Proposition

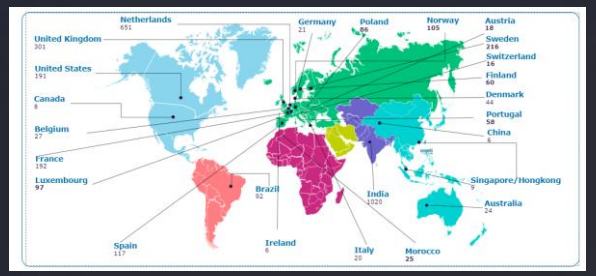
France Cyber market: 2,559 M€ in 2020 growing at 9% [PAC]



Capgemini Overview of Capgemini Security Services (Map vendors)



Microsoft Certified professionals across global regions

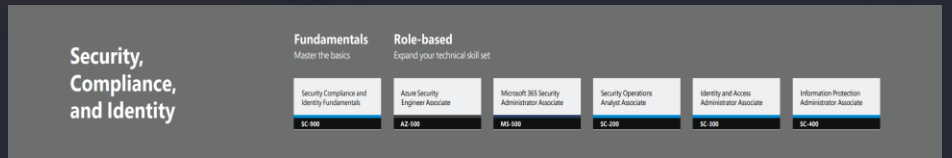


Microsoft Partner Awards

• 2020 Proactive Customer Service Partner of the Year award (runner-up)

Recent Microsoft Partner Award

Winner Microsoft Partner 2019 Partner of the Year SAP on Azure Award



4

NEXT STEP

CONTACT US

frederic.urvoy-de-portzamparc@capgemini.com	CDC-SOC Pre-sales lead
nicolas.dignoire@capgemini.com	CDC- SOC France delivery lead
christophe.dupas@capgemini.com	CAPGEMINI Security Partnership lead
christophe.menant@capgemini.com	CAPGEMINI Security offering lead

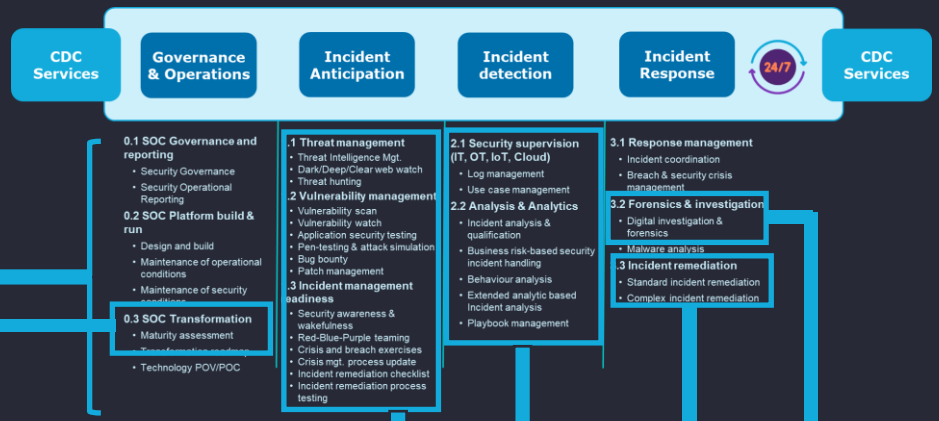
QUESTIONS?

- Do you know the maturity level of your SOC services ?
- What is the false positive ratio of your security monitoring fabric?
- Do you have a team capable of handling a serious security incident, with up-to-date expertise on the latest attacks, and available 24/7?
- Do you know how to provide your teams with the, business, tactical and technical intelligence necessary for understanding, anticipating and reacting to cyber incidents?

The customer journey

1. **The CLIENT doesn't know how efficient and relevant its SOC maturity is** → CAPGEMINI performs a SOC maturity assessment → CAPGEMINI defines the SOC strategy, gap analysis and the associated roadmap to improve the maturity
2. **CLIENT knows what to do to enhance its SOC Maturity** → CAPGEMINI designs and builds solutions to meet the Client's requirements → Optionally CAPGEMINI runs some SOC Services
3. **CLIENT has been breached** → CAPGEMINI Incident Response service is triggered (Investigation / SWAT) → CAPGEMINI Incident Response team defines the technical tactical plan → Optionally CAPGEMINI Remediation team implements the tactical plan
4. **CLIENT got INCIDENT DETECTION service from CAPGEMINI** → CAPGEMINI Incident Detection team defines the technical recommendation to handle an Incident → Optionally CAPGEMINI Remediation team implements the tactical plan
5. **CLIENT wants to be prepared for the next breach / crisis** → CAPGEMINI provides Incident Anticipation services
6. **CLIENT needs specific skillset to support his SOC security projects / run operations** → CAPGEMINI provides staff augmentation with appropriate skills → The security professionals is included into the project/operating model of the CLIENT

CAPGEMINI CDC Service Catalogue



Question?

Thank You