Capgemini

Security Operations Center (SOC)

Cybersecurity tailored to your unique needs

The challenge

Almost all organizations will experience a data security breach this year. Do you have the resources to counter the threat; and how quickly will you respond?

As cyber attacks become increasingly sophisticated, research suggests that it takes an average 78 days* for a malicious attack to be identified. The good news is that this is down from 101 days in 2017. The bad news is that it is still a long time during which a cybercriminal, competitor, aggressive nation state, or even a disgruntled employee has unauthorized access to your business systems and critical information assets.

Safeguarding data

Data privacy and protection are also core to today's security strategies. Data fuels business success. If it is clean, safe, organized, and accessible, people will have more trust in your organization. Far from putting a halt to the way you monetize data or build digital strategies around its value, securing your data can help you become more competitive and productive. Effective data security equips you to pursue wider digital possibilities.

Supply and demand

The battle for talent is another critical cybersecurity challenge. As the growing demand for cybersecurity expertise far outpaces supply, many enterprises lack the in-house resources to direct, execute and hone cybersecurity strategy. In a 2017 Capgemini research project conducted with LinkedIn, more than half (55%) of companies surveyed said that the digital talent gap between demand and supply was widening, with cybersecurity skills ranking first in both demand and talent gap.

Monitor, detect, respond

Even if you are well protected with the right tools and the right processes in place, you still leave yourself open to attack if you are not monitoring systems; detecting potential security incidents; and able to make changes to your operations quickly to counter any threat detected. Add to this the reputational damage of a security breach, and it is evident that a new generation of cybersecurity is needed.

The average size of data breaches is growing, increasing 1.8% from 2016 to more than 24,000 records in 2017. The financial cost alone explains why cybersecurity is, more than ever, a strategic imperative: the global average cost of a data is $3.62 million, and the average cost for each lost or stolen record containing sensitive and confidential information is to $141.

Ponemon Institute, 2017 Cost of Data Breach Study

Almost 2 billion records were lost or stolen worldwide during the first half of 2017, up 164% from the last half of 2016.

* *Mandiant (a FireEye company), M-Trends 2019 report*

Cybersecurity tailored to your needs

Every enterprise has its own, unique security requirements. That's why our consulting-led starting point is always to help our clients understand and quantify their risk profiles, identify critical data assets, and assess their current security strategies and levels of protection.

This wholly customer-centric, end-to-end approach enables us to prioritize and manage threats to the business. It ensures that the solutions we build fit each client's individual strategic priorities and security challenges, enabling them to put protection where it's needed most.

What remains constant for all organizations, is the growing threat posed by increasingly audacious cyber attackers, whether financial criminals or state-sponsored hackers. Many enterprises have already implemented SIEM (Security Information and Event Management), yet they have failed to see the expected benefits due to the rapidly evolving complexity of today's security threats. The lesson is clear: enterprise cybersecurity must also evolve. But this evolution should be individual to each organization's business risks and priorities.

With services tailored to our clients' specific context and business ambitions, we meet this need. They are services that are flexible enough to adapt to the enterprise, while able to evolve with emerging threats, so that we identify and pre-empt sophisticated attacks.

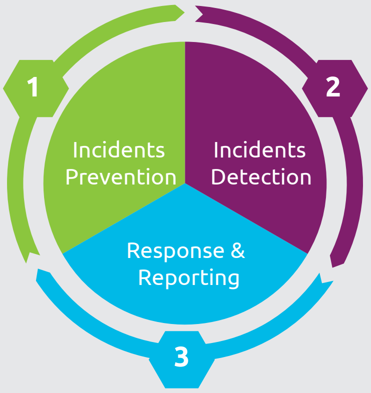
This progressive range of end-to-end services is delivered through our proven Security Operations Center (SOC) model. With a worldwide presence, our global SOCs adapt their service delivery mode according to each customer's needs, as described in the following pages.

The Security Operations Center

Capgemini's Security Operations Centers (SOCs) orchestrate the multiple roles, processes and technology needed to enable efficient incident detection, analysis and response. Comprising a set of processes, technologies, and a team of trusted security analysts and R&D specialists, each SOC provides complete visibility of both an enterprise's IT and its security system.

Whether dedicated wholly to your individual enterprise, or provided as a multi-tenant managed service, a Capgemini SOC will equip you with the tools and resources you need to: prevent; detect; and respond.

A Security Operations Center is the centralized incident-response team reporting through an organization's Chief Security Officer/ Chief Information Security Officer (CSO/CISO).



Incidents Prevention

- Threat Intelligence
- Vulnerability Management

Incidents Detection

- Security Monitoring
- Security Analytics
- GRC

Response & Reporting

- Security Response

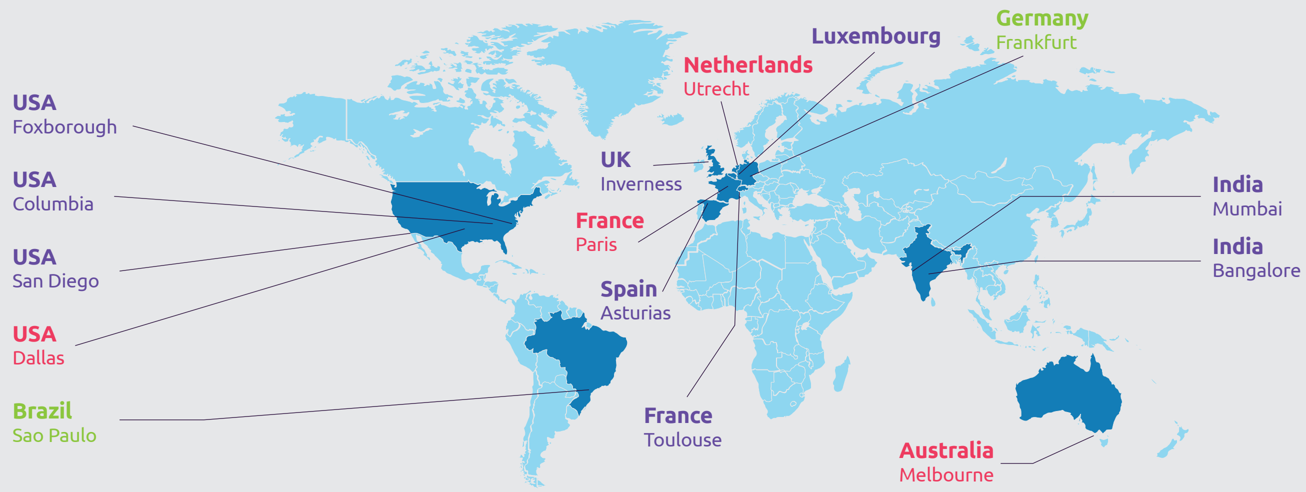
A global presence

Our network of global Security Operations Centers (SOCs) stretches stretches across the world, with SOCs in India, Europe and North America complemented by satellite SOCs. They collaborate, share expertise and best practices, and communicate success stories in their relentless pursuit of robust cybersecurity. Clients benefit from comprehensive intelligence, better preparedness, swifter response and improved resilience.

Flex it, scale it—your way

The flexible tiered scale of Managed SOC services offers enterprises the opportunity to swiftly establish a highly effective Security Operations Center, out of the box, and at low TCO (total cost of ownership).

A Connected Network of SOCs Constantly Monitoring Threats, wherever you are.



🟪 SOC 🟥 Satellite 🟩 Opening shortly

Your security; your choice of delivery model

We know that there is no one-size-fits all approach to cybersecurity. So, our services are offered through several delivery models:

- **Dedicated SOC:** Depending on your individual risk profile, regulatory requirements, or competitor landscape, you may opt for a dedicated SOC that is fully customized to your business. This enables you to benefit from Capgemini's security expertise and skills, which is of huge value if your organization lacks internal cybersecurity resources. You will save time and cut the cost of team training, management, and supplier management, which is all provided by Capgemini with services wholly tailored to you.
- **Managed SOC:** Our industrialized service delivery model uses unified and standardized SOC processes that can be repeated to enable a low cost of entry (with reduced CapEx) and swift deployment. Choose the service level that best suits your business need, from standard services that cover the basics across monitoring, detection, prevention and response, and reporting, to enriched service levels that combine the basics with customized services, analytics-based threat intelligence and advanced SOC automation.
- **Hybrid SOC:** We use both offshore and local resources in a single seamless SOC after determining the best balance between your resources and our own. We identify the ideal combination of onshore, nearshore and offshore talent to deliver the optimum solution for your business. Using this model, you'll be able to improve your productivity, predictability and responsiveness, while reducing costs, risks and workload for your teams.

Three Levels of Services for our Managed SOC (SOCaaS)

COMPREHENSIVE services that extend advanced SOC services to automate SOC activities

Counter advanced threats with THREAT INTELLIGENCE

Bronze Services

Services providing MODERATE customization and extended SOC solutions

INTRODUCES threat intelligence backed by analytics

Silver Services

Includes STANDARD, yet critical elements of the SOC: Monitor, detect, prevent, respond & report

REDUCES overall operational overhead & infrastructure costs to maintain and sustain SOC services

Gold Services

Threat Intelligence and Analytics

Data is a crucial element of our SOC success story. We use it to turn our customers from the hunted into the threat hunters.

Our advanced data analysis capabilities bring together SIEM, network security monitoring, endpoints monitoring, payload analysis and offline big data analytics in an intelligence-driven approach.

We also improve the capacity to detect the most sophisticated advanced persistent threats with:

- Focused detection rules aligned with a client's IT environment, and the threat landscape
- A deep understanding of the context (threat intelligence; knowledge of applications within the attack perimeter);
- An efficient response through the creation of a strong link to the IT Service Management, as well as a security team;
- Security analytics focused on the user (behavior and external attacks), applications, and DNS malware to identify malware infected hosts.
- Predictive attack discovery through IT vulnerabilities management (patch recommendation, network of honey pots)

Responding to regulations

Capgemini's SOCs help clients comply with regulatory changes relating to security, including Europe's NIS Directive, the EU's GDPR, New York State Department of Financial Services regulations in the US and other industry specific guidelines such as PDIS and PFS.

Together with the increase in the frequency, scope and sophistication of cyberattacks, these regulations are forcing enterprises to go beyond their conventional network protection to focus on securing data, as well as on the detection and anticipation of threats in their systems.

Capgemini's SOCs bring a deep understanding of this regulatory landscape, the associated business concerns and opportunities, and relevant technology solutions and cybersecurity approaches.

Industry-leading analytics

Capgemini uses a broad range of threat intelligence sources, allied with industry-leading analytics capabilities. Our award winning* Cognitive Security Operations Center solution brings advanced data analysis to enterprise security, and enables security threatsof all types to be identified early and counteracted swiftly, decreasing cost and disruption to the business.

**2018 IBM Beacon Award for Outstanding Security Solution*

Taking an industry perspective

We deploy our Security Operations Center model in enterprises across all sectors. Each client has unique needs, many of which are only applicable to the industry in which they operate. The following examples demonstrate three industry-specific use cases:

Automotive

Security in the automotive industry has risen high on the strategic agenda in recent years. The car is now an intelligent, communicating device, with hundreds of intelligent, communicating parts adding up to a large attack surface. According to one survey, 62% of customers fear cars will be easily hacked. And it's not just the vehicles themselves that are open to cyber-attack: there are threats at every stage of the plan-build-run lifecycle, with one report citing automotive manufacturers as the top targeted manufacturing sub-industry.

Capgemini's end-to-end approach in this sector brings together previously disparate areas of cybersecurity focus in a single, consistent strategy. This extends from manufacturing plants to the connected vehicle and into broader enterprise IT operations. Our automotive-centric SOC acts as mission control, looking for anomalous behavior in any aspect of the operation, and tracking events, incidents, and responses.

Energy & Utilities

Critical infrastructures, such as energy grids and water supply systems, have always demanded a high-level of security. Now, with digital advances, a new security risk has arisen: that of smart meter security. While smart meters offer the potential for greater accuracy of usage information, the challenge is to ensure that this information is protected against cyber-attack. The threat is very real, with concerns about the potential for malicious code to cut power to homes, or for a hacker to access data on power or water usage to spot when a homeowner is away from the premises.

Capgemini's SOCs have the data science expertise to help companies in this industry identify incidents and respond rapidly and appropriately. We have been at the forefront of the smart metering evolution for many years and combine this expertise with our deep cybersecurity knowhow. Capgemini SOCs offer real-time monitoring that allows organizations to rapidly identify and fix any security issues on the smart meter network.

Financial Services

Consumer trust is essential in the financial services industry. Customers expect their personal and financial data to be protected from security breaches. Yet in a 2016 survey, less than a third of participating financial services organizations said they offered both strong data privacy and a sound security strategy. This has potentially damaging ramifications, with 74% of the consumers surveyed saying they would switch their bank or insurer in the event of a data breach. With the EU's GDPR enforcing the reporting of any data breach within 72 hours after an incident, consumers will become even more aware of security issues.

There is thus a clear incentive for investing time and resources in safeguarding customer data. A Capgemini SOC can help. As well as improving breach and attack detection, our SOCs can mitigate the impact and help prevent future attacks, for example with threat intelligence services.

Capgemini Security Operations Centers – keeping your systems, applications and data protected, day and night.

Capgemini

About Capgemini and Sogeti

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE., listed on the Paris Stock Exchange.

For more information please visit

www.sogeti.com

This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

For further information please contact:

infra.global@capgemini.com