Microsoft | Capgemini

Cyber Defense Center (CDC)

Powered by Microsoft Azure Sentinel

Cybersecurity tailored to your unique needs

The challenge

The arms race against cybersecurity attacks is continuous. New threats, new attackers, and new targets emerge every day, and cyber criminals are constantly evolving to breach your defenses. Do you have the resources to counter the threat; and how quickly will you respond?

As cyber-attacks become increasingly sophisticated, research findings published in 2020 suggest that it takes an average 56 days* for a malicious attack to be identified. The good news is that this is down from 78 days in 2018. 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 the cybersecurity strategy.

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 (due to a permanently evolving threat landscape) 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 global average cost of a data breach is $3.86 million, while the average cost for each lost or stolen record containing sensitive and confidential information is $146, rising to $150 for those containing personally identifiable information (PII). Figures like this clearly demonstrate why cybersecurity is a strategic imperative.

Ponemon Institute, 2020 Cost of Data Breach Study

* Mandiant (a FireEye company), M-Trends 2020 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 Cyber Defense Center (CDC) model. With a worldwide presence, our global CDCs adapt their service delivery mode according to each customer's needs.

The Cyber Defense Center Powered by Microsoft Azure Sentinel

Capgemini's Cyber Defense Centers (CDCs) orchestrate the multiple roles, processes and technology needed to enable efficient incident detection, analysis and response.

We continuously adapt and improve our Operating Model (People, Process and Technology) to move to a more proactive posture, as opposed to being purely defensive.

Comprising a set of processes, technologies, and a team of trusted security analysts and R&D specialists, each CDC provides complete visibility of both an enterprise's IT and its security system.

Deploy the optimal solutions to safeguard your enterprise

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

We know that cyber criminals don't wait, so the quicker we can implement and scale, the better equipped our clients are to protect their businesses against hackers and malicious threats. Microsoft Azure Sentinel is the foundation in our arsenal. It enables us to quickly implement a full CDC platform in just days or weeks, as opposed to the traditional months or even years.

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

Next generation Cyber Defense Centers and Azure Sentinel

Azure Sentinel is Microsoft's cloud-native security SIEM product, providing intelligent security analytics at scale. It complements our next generation CDC platform incorporating: cloud-native elasticity; embedded machine learning; cloud native storage; and advanced hunting and investigating capabilities to maximize analyst efficiency, reduce mean time to recover (MTTR), and economically scale to address ever increasing demands.

With a cloud-oriented pay-as-you-go pricing model, pre-built content, and improved functionality, we ensure our clients tap into the power of cloud automation for a cost effective and scalable CDC environment.

Your security; your choice of delivery model

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

Better together: Capgemini and Microsoft

As a Microsoft Azure expert and Managed Gold Certified Provider, Capgemini brings a wealth of experience to deploying and running the Azure Sentinel tool in our global CDCs.

We continually enhance and strengthen our 22+ year partnership with Microsoft, driving cloud transformation with joint enterprise customers worldwide.

Our clients benefit from set of unique advantages, including our presence in over 25 countries, on 5 continents, and supported by 45,000 Microsoft skilled professionals with Accelerated Delivery Centers and Rightshore® Delivery options.

Our flexible delivery approach supports our clients' individual security approaches, whether in cloud based, local datacenter, hybrid cloud/ on-premise, or multi-cloud model.

With a complete portfolio of Microsoft cloud solutions, we support our customers, from cloud strategy development, to managing secured hybrid environments that deliver a cloud-first way of working.

Mutualized

- Industrialized CDC services capability through the Global network of CDCs.
- Security operations support in local language with a local presence.
- Best ROI, still result and KPI driven.

Dedicated

- Tailored CDC to suit a client's security needs & risk profile.
- Managed in-house or in a Capgemini location.

Hybrid

- A single seamless CDC that balances a client's resources with Capgemini's.
- Improves productivity and responsiveness while reducing costs, risks and workloads.

Responding to regulations

Capgemini's CDCs 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.

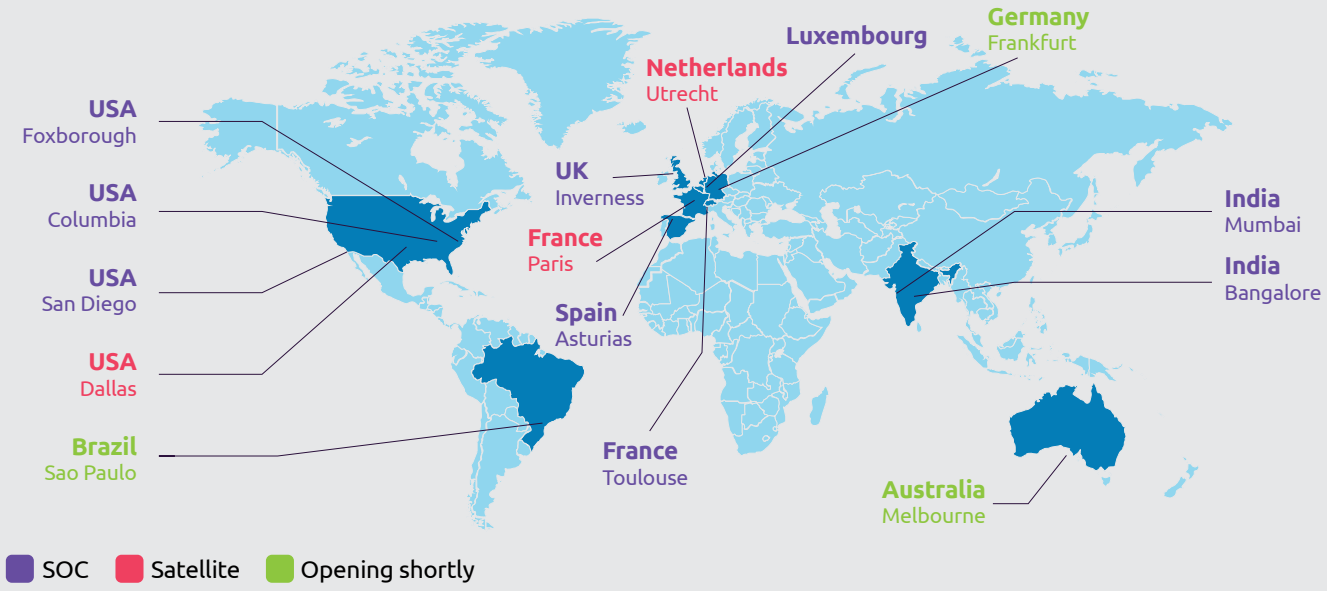
Together with the increase in the frequency, scope and sophistication of cyberattacks, these regulations are forcing enterprises to go beyond their conventional network protection to focus both on securing data and on the detection and anticipation of threats in their systems.

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

A global presence

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

Connected Network of 15 CDCs Constantly Monitoring Threats, wherever you are.



Flex it, scale it—your way

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

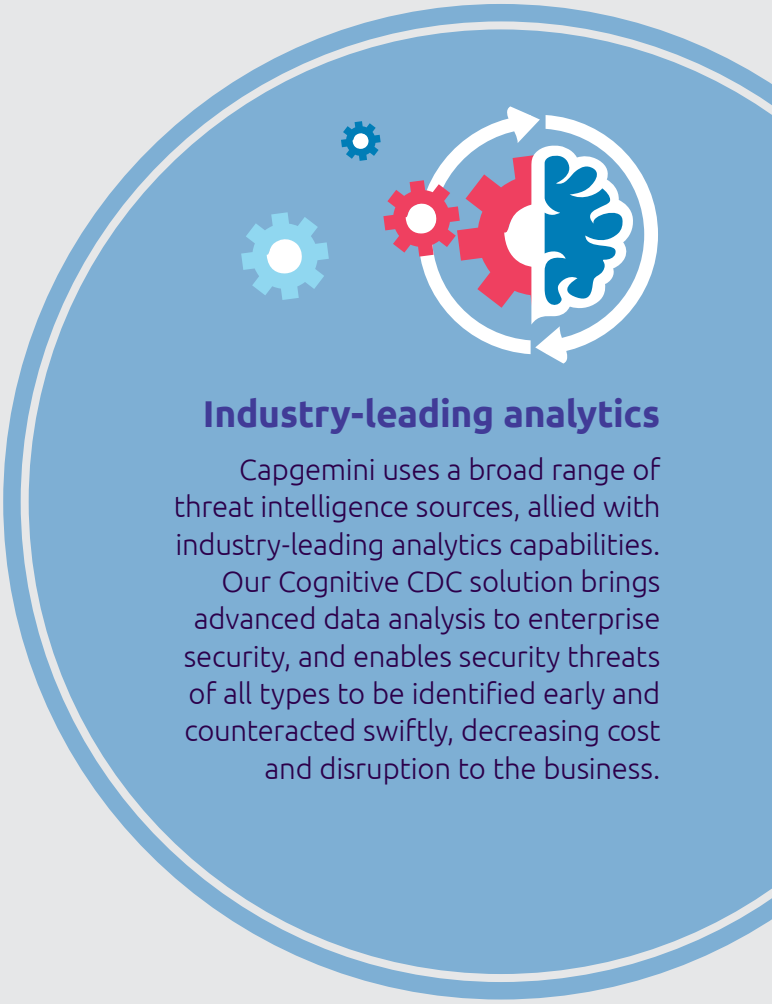
Threat Intelligence and Analytics

Data is a crucial element of our CDC 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:

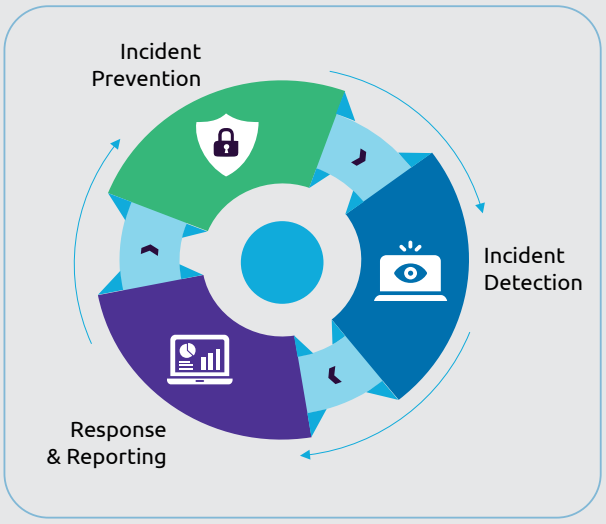
- Focused detection rules aligned with a client's IT environment and the threat landscape.
- A deep understanding of the context (threat intelligence; knowledge of applications within the attack perimeter).
- An efficient response through the creation of a strong link to the IT Service Management, as 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).

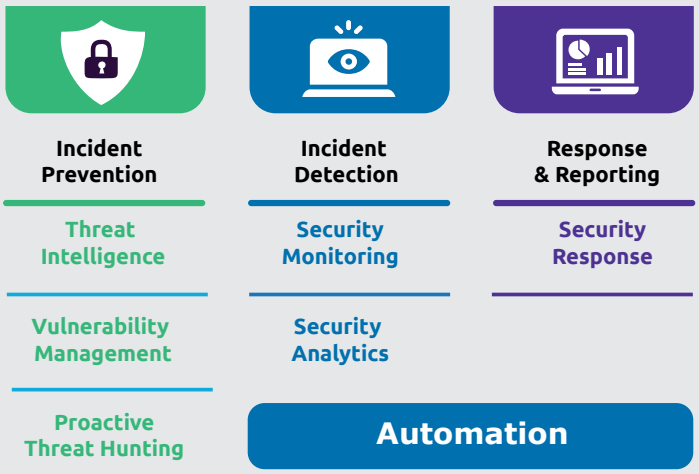


Industry-leading analytics

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

Advanced Analysis to Minimize Incidents





Taking an industry perspective

We deploy our Cyber Defense 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 CDC 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 CDCs 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 CDCs 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. With the EU's GDPR enforcing the reporting of any data breach within 72 hours after an incident, consumers are more aware of security issues than ever before.

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

Capgemini Cyber Defense Center, powered by Microsoft Azure Sentinel – keeping your systems, applications and data protected, day and night.

Take control. Contact Capgemini

The strength of your security posture, and your ability to exploit transformational business opportunities all depend on cybersecurity. Grab the reins and regain control. Contact Capgemini today for additional details and case studies about our unique—and uniquely effective—CDCs.

About Capgemini

Capgemini is a global leader in consulting, digital transformation, technology, and engineering services. The Group 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. A responsible and multicultural company of 265,000 people in nearly 50 countries, Capgemini's purpose is to unleash human energy through technology for an inclusive and sustainable future. With Altran, the Group reported 2019 combined global revenues of €17 billion.

Visit us at

www.capgemini.com

For further information please contact:

cybersecurity.in@capgemini.com