Capgemini

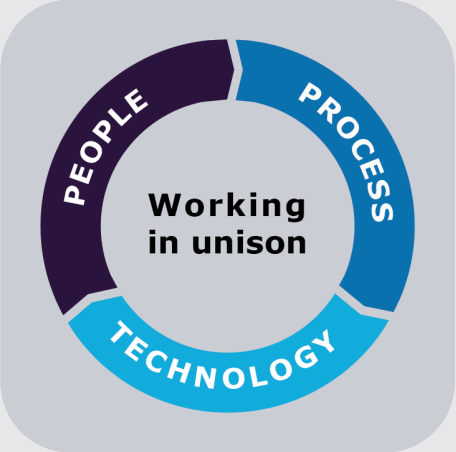
Achieving cybersecurity resilience is the mission

Conquer the challenge by leveraging a recognized leader

Strengthen your organization's cybersecurity today

Partnering to protect

Cybersecurity is a complex task and cyber teams can be stretched thin defending against the ever-changing threat landscape. Success depends on how well people, process, and technology work in unison. Achieving this critical goal can require leveraging the resources of a strong, flexible partner to execute a proven strategy designed to safeguard your enterprise, your business, and your customers.



When you partner with Capgemini, you gain access to more than a decade of enterprise defense experience refined through hundreds of large-scale cyber engagements within the Fortune 500. Our team of highly trained cybersecurity practitioners have the skillset and mindset required to meet today's challenges and ensure a strong, mature cybersecurity posture.

Our solutions and services deliver a more advanced security posture, sustainable threat protection, and an adaptive long-term cybersecurity strategy. Leveraging Capgemini cyber capabilities ensures your organization will have the necessary resources to defend your enterprise and secure your business.

Unified Enterprise Defense strategy

Our applied framework defines the components of an effective cybersecurity program, establishes an integration strategy, and provides a roadmap to create a strong cybersecurity foundation that supports the evolution to a mature adaptive posture.

The Unified Enterprise Defense (UED) structure was developed by Capgemini to outline and characterize all the important elements that an organization must develop and integrate cohesively to have an effective plan for protecting and defending an enterprise from cybersecurity threats.

Key foundations for an adaptive defense

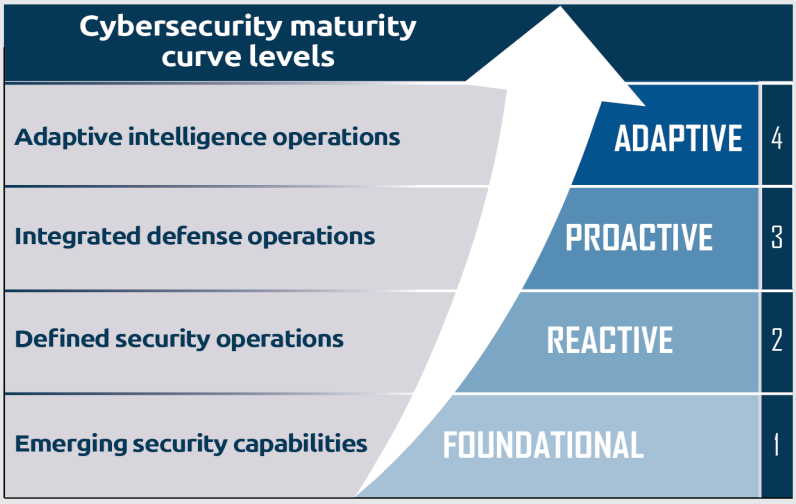
Core to good cybersecurity planning is an underlining strategy, one that defends, protects, and evolves with your organization. Capgemini's UED framework establishes a strong security foundation and implements a suite of adaptive capabilities to provide sustainable threat protection.

Unified Enterprise Defense framework	
Culture and organization	• Defined mission, vision, and strategy • Effective concept of operations
Governance	• Compliance and regulations mapped and satisfied • Risks identified and measured
Visibility and controls	• Visibility across enterprise and applications • Foundational controls deployed
Focused defense	• Specialized platforms optimized for effectiveness • Tailored detections and strategic mitigations
Intelligence operations	• Intelligence-enabled mindset • Skilled and adaptive resources

In order to build a truly effective cybersecurity program, these five pillars and their components must be implemented and operated in an integrated and cohesive fashion. Capgemini leverages the UED framework to apply the right balance of people, process, and technology in a coordinated and strategic manner.

Transform to achieve cybersecurity maturity

All enterprise organizations can be evaluated, measured, and improved. The cybersecurity maturity curve has the following clear organizational levels: foundational, reactive, proactive, and adaptive. Organizations are analyzed to determine their level. Applying our UED framework defines the current level of cyber resiliency and provides a clear path forward to achieve adaptive intelligence operations.



Strengthen your cyber defense program

Capgemini's team of cybersecurity practitioners can help you implement a Unified Enterprise Defense strategy to protect your organization and create a resilient enterprise. Our team of experienced cyber analysts will partner with you to transform your cybersecurity capabilities into an effective, efficient, and adaptive program securing your business now and into the future.

We work with your team step by step to evolve your cybersecurity posture.

Cybersecurity solutions and services

DEFINE:

Create a baseline, validate where you are today, understand tomorrows goal, plan and transform forward.

- Unified Enterprise Defense Assessments
- Application security
- Pen testing, red teaming and threat simulation
- Governance, risk and compliance

PROTECT:

Execute a transformative plan, programs and projects to secure your environment.

- Security transformation and operations
- Engineering and architecture
- Identity and access management
- Network segmentation
- Device management
- Insider threat

DEFEND:

Leverage personnel, help develop programs, and platforms to actively detect, and mitigate threats.

- Managed Security Services (MSS)
- Managed Detection & Response (MDR)
- Outsourced / hybrid / embedded

Define

Assess, test, and validate the effectiveness of your cybersecurity capabilities

SOLUTIONS AND BENEFITS

Unified Enterprise Defense (UED) assessments	▪ Cyber Defense Maturity Evaluation (CDME) identifies and measures an organization's cybersecurity maturity. It provides a full evaluation of how well people, process, and technology work in unison. ▪ Scores against defined UED principles and a baseline against industry peers ▪ Additional industry frameworks, such as NIST, ISO, FFIEC, and CMMI can be incorporated into the assessment and report process.
Application security testing	▪ The tests provide a full spectrum review of the security of applications, including static, dynamic, and penetration testing, to identify vulnerabilities in your source code, application processes, and production environments.
Penetration testing, red teaming, and threat simulation	▪ This evaluates your network security, systems, personnel, and processes against a wide array of known adversary tactics, identifying an organization's strengths and weaknesses and providing actionable, prioritized remediation recommendations to improve security of the environment.
Governance regulatory and compliance (GRC)	▪ Our GRC services: cybersecurity risk modeling, regulatory compliance, and cybersecurity governance frameworks. ▪ Understand risk posture and build a governance model that supports the rest of your cybersecurity program. ▪ Develop processes to strengthen compliance through regular audit and controls.

Protect

Through **design, deployment, and optimization** of key cybersecurity solutions

SOLUTIONS AND BENEFITS

Security operations	▪ Our practitioners partner with you to evolve your security operations from reactive to adaptive by adopting an intelligence-based mindset and increasing organizational maturity. ▪ Our transformative approach aligns and maximizes the effectiveness of people, process, and technology via: – High-level organization concept of operations – Workflows that define roles and responsibility – Process and procedures and playbooks. – Intelligence-based mindset – End-to-end analyst skillset
Security engineering and architecture	▪ Align platforms and technology to support and provide maximum leverage to your security operations teams ▪ Helps to design, deploy, optimize, integrate, and tune your tools ▪ Partner with leading security vendors to ensure that our clients benefit from the latest tools and technologies to safeguard their enterprise assets
Identity and Access Management (IAM)	▪ Define your IAM strategy, build an integration roadmap, and implement a solution to manage and secure user registration, authentication, and rights and permissions.

(Protect continued on next page)

Protect

Through **design, deployment, and optimization** of key cybersecurity solutions

SOLUTIONS AND BENEFITS

Network segmentation	▪ Assess and evaluate both IT and OT/IoT network defense architectures to measure access and network controls within each environment and identify improvement opportunities to enhance overall control-system segmentation and security.
Device management	▪ Provides a comprehensive solution including design, implementation, and end-to-end operations and optional monitoring support of your security controls. A strategic partner with leading security vendors.
Cloud security	▪ Assess, advise, implement, and monitor to secure your cloud architecture ▪ Delivered from our global network of ISO27001-certified SOCs, accessible either via our wider Capgemini Cloud Platform (CCP) or as standalone services
Insider risk and threat services	▪ Evaluates and measures an organization's capabilities to prevent, detect, and respond to insider threats by following a structured insider risk assessment. It is aligned with NIST, ISO, NISPOM, and other industry-leading standards. ▪ Design, implement, and operate platforms that detect and help mitigate insider threats.

Defend

Custom **managed enterprise defense** via embedded, hybrid, and remote services

SOLUTIONS AND BENEFITS

Managed Security Services (MSS)	▪ Remote continuous monitoring of network security platforms. Delivery of all applications and tools necessary to provide security for our customers 24/7/365 ▪ Tier-1 operations, SIEM, endpoint, and other security tools ▪ Monitoring, execution of moves, adds, and changes to core cybersecurity platforms
Managed Enterprise Defense	▪ A new-breed solution that delivers advanced monitoring, detection, and response capabilities via three flexible models to meet your organization's demands
Managed Detection and Response (MDR)	▪ Full-scope enterprise defense capability delivered remotely. Highly experienced security analysts, incident responders, and threat hunters proactively monitor and detect threats early, analyze them completely, and deliver a response customized to your environment.
Hybrid defense	▪ Combine the efficiency and global visibility of our remote MDR capability plus dedicated embedded analysts to provide the right combination when teamed with your internal staff.
Embedded operations	▪ Dedicated enterprise defense practitioners sitting shoulder-to-shoulder with you to bring our experience, mindset, and skillset to support your security operation objectives.

Additional cybersecurity capabilities

Our experts maintain a broad set of skills and capabilities beyond those mentioned above including:

Compliance frameworks and standards, GDPR readiness, cyber risk quantification, cloud security architecture, threat hunting, incident response, etc.

Cyber services – remote capabilities

Our remote capabilities are here to ensure your organization's cyber resiliency. We have established a set of remote services in these areas: application and infrastructure protection, incident response, managed detection and response, device management, threat hunting, and training. These services can be implemented remotely and support your workforce's transformation from premises-focused to remote-focused cybersecurity.

How can we help? We have capacity and technical resources that can be applied remotely. If you need additional support to run cyber operations, additional eyes to help your analysts, need always-on support, or platform management and monitoring expertise, resources are available.

Scalable deployments

Capgemini has deep experience in large-scale cybersecurity transformations. We help organizations develop and implement transformation plans, including roadmaps generated from baseline assessments, delivering fully functional cybersecurity programs at a global scale. Our team of skilled professionals are accessible at scale and backed by a global network of extremely sophisticated SOCs.

Deployment services

- IAM
- SIEM
- Device management
- Managed security
- Endpoint security
- Network security
- GDPR controls

End-to-end solutions

Our cybersecurity approach provides end-to-end cybersecurity that starts by assessing, testing, and validating a client's security, partners to evolve a transformative plan, protects while this evolution occurs and, alongside our clients, defends the enterprise throughout the process.

Global visibility with local expertise

- One globally linked team, supported by 12 connected SOCs and labs
- Resident cybersecurity expertise in 13+ countries across five continents
- 2,500+ cybersecurity defense analysts, engineers, architects, and integrators

Achieving cybersecurity resiliency is the number one concern

Capgemini is a partner committed to your evolution, helping you build a strong foundation and mature capabilities to meet the challenges of an ever-evolving cyber threat landscape. We ensure you have the right cybersecurity practitioners, processes, and technology to keep you ahead of adversaries. Through our end-to-end solution set, from trusted advisors to skilled analysts, to Security-as-a-Service solutions, and more – we can assist you anywhere along your cyber journey.

Our cyber practitioners certifications

Industry-standard certifications including CISSP, CISM, CISA, CCSP, including ITIL, CEH, CCIE, GSTRT, Global Industrial Cyber Security Professional (GICSP) certified consultants, and other technology certifications.

Contact our Capgemini sales team:

cyber.security.nar@capgemini.com

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. Capgemini is driven by the conviction that the business value of technology comes from and through people. Today, it is a multicultural company of 270,000 team members in almost 50 countries. With Altran, the Group reported 2019 combined revenues of $18.5 billion.

Learn more about us at

www.capgemini.com

CSNA.20.05.20.L042.R18