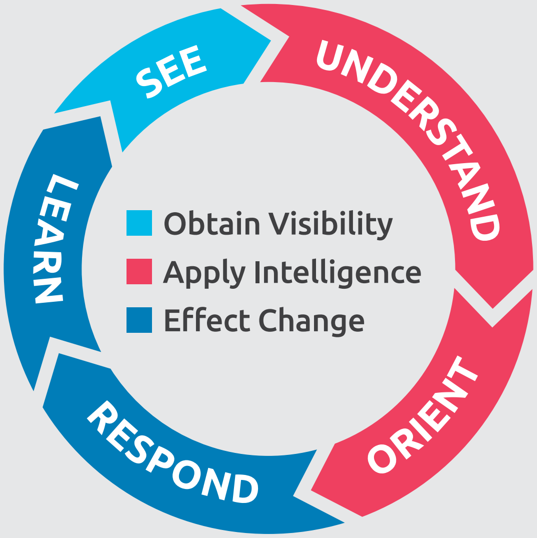
Cybersecurity Defense Maturity Evaluation

The Cybersecurity Defense Maturity Evaluation establishes a baseline of the maturity and measures how comprehensive an organization's cyber defense and resiliency are against opportunistic attacks and the most advanced cyber threats, including advanced persistent threats (APT) and identification of insider risks.

The evaluation is based on the Capgemini Unified Enterprise Defense strategy and associated lifecycle, driving a comprehensive evaluation for how an organization is both securing the enterprise as well as defending the enterprise through proper visibility and impactful leverage of threat intelligence. This evaluation is best suited for organizations that not only want to understand that they are focusing on the right cybersecurity areas across their enterprise, but also that the ways in which they are operationalizing those areas are truly being effective. The most effective cybersecurity approach necessitates that organizations stay proactively ahead of emerging threats. To do this requires a continuous collection of intelligence, an understanding of emerging threats, and the ability to adapt to an adversary's methods dynamically.



UNIFIED ENTERPRISE DEFENSE STRATEGY:

An overall theme applied to define how well an organization's defense security operations capabilities can accomplish five critical tasks and achieve a successful implementation:

1. **SEE:** Monitor cyber activity
2. **UNDERSTAND:** Identify and isolate advanced cyber threat activity from normal network or system traffic
3. **ORIENT:** Determine a course of action
4. **RESPOND:** Take action to implement defenses and execute mitigations
5. **LEARN:** Build new, actionable intelligence

Capgemini

The Cybersecurity Defense Maturity Evaluation takes an all-inclusive view across the enterprise and more specifically the components responsible for network and system defense. Results are measured against the following maturity progression to define the organization's current cybersecurity defensive posture:

Crisis Response – The enterprise does not have a defined strategy for implementing a cyber defense program. Foundational security capabilities are either not in place or lacking, presenting a high risk for potential threats or currently active compromise.

Emerging Security Capabilities – The enterprise has started to build out capabilities for foundational areas of security aligned to risk. Operations are in a distributed manner, and a standardized model and consistent approach has not been defined or focused on network defense functions.

Defined Security Operations – The enterprise has a baseline of repeatable security operations and may have a dedicated team for network defense. Workloads are primarily reactive cyber response activities, preventing effective defensive operations. Threat intelligence may be leveraged in an ad-hoc capacity.

Integrated Defensive Operations – The enterprise has aligned both aspects of securing the enterprise and defending the enterprise into a well-defined industry model. Threat intelligence is integral to daily operations and feeds detective and defensive strategies.

Adaptive Intelligence Operations – The enterprise has established a mature cyber defense program. Operations continue to mature and adapt through automation efficiencies and partnerships as the threat landscape changes. Custom capabilities are established and threat intelligence managed to the degree that historical data trending enables the security organization to stay ahead of adversaries.

This evaluation is appropriate for organizations with established foundational cybersecurity components such as NIST, IEC 62443, and ISO 27001. This evaluation is not focused on compliance to a standard but evaluates capabilities beyond the scope of best practice standards and/or industry regulations to analyze the security program from the vantage point of the defender. Organizations leverage this evaluation to compare their cybersecurity maturity posture to that of their peers and to justify investments in personnel and advanced technologies.

For further information, please contact:
infra.global@capgemini.com

What does it Evaluate?

This evaluation compares the security posture of an organization, relative to a proactive Unified Enterprise Defense organization, by investigating and measuring the strategic vision, people, processes and technologies within the existing network defense program. Specifically, the Cybersecurity Defense Maturity Evaluation measures an organization's alignment to the Unified Enterprise Defense framework across 13 specific Evaluation Domains:

1. Organization and Mission
2. Executive Support
3. Architecture and Engineering
4. Security Technology
5. Enterprise User Awareness
6. Enterprise Visibility and Monitoring
7. Response and Mitigations
8. Analysis Process and Skills
9. Defender Operations
10. Malware Analysis
11. Intelligence Management
12. Metrics and Measuring Success
13. Supporting Programs

About Capgemini

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.

Learn more about us at

www.capgemini.com/cybersecurity

People matter, results count.

|