Federal Application Security, Architecture & Engineering Services

Experience the commitment®

Each agency and department has a unique set of threats, risks, regulatory drivers and security considerations. CGI delivers individualized security engineering solutions that address architecture, application and data security needs to protect organizations from cybersecurity threats.

While applications provide users with a rich interactive experience, they also represent a window for malicious attacks against the enterprise. Attackers are shifting their focus to critical enterprise data at the application layer. This level of attack can cause considerable damage to an agency and the citizens it services. As threat sophistication increases, organizations must advance application security defenses beyond network security and endpoint protection. CGI has developed a robust set of individualized security engineering services to address these threats and protect what matters most: your agency's mission, business applications and sensitive data.

APPLICATION SECURITY CAPABILITIES

- **Static Application Security Testing (SAST)**, or white box testing, analyzes an application's code and binaries for security vulnerabilities. SAST detects highly complex vulnerabilities that are not visible without access to the source code.
- **Dynamic Application Security Testing (DAST)**, or black box testing, analyzes an application while it is running. DAST simulates attacks, evaluates the application's reactions and determines its vulnerability.
- **Mobile Application Testing** analyzes mobile applications using a combination of static and dynamic techniques to discover malicious or potentially risky behavior. Mobile Application Testing assesses the whole system including applications, web services, web controls and storage.
- **Open Source Components Assessment (OSCA)** delivers a full spectrum security analysis of open source components and their dependencies. OSCA combines dynamic runtime analysis with static code review. The analysis employs both automated vulnerability discovery tools and manual testing tailored to the environment.
- **Internet of Things (IoT) Assessment** identifies physical and logical security threats and weaknesses in embedded devices, interface applications, back-end services, APIs, cloud clusters and controllers/gateways in IoT ecosystems.
- **Database Security Services** encompass a broad range of information security control services to protect databases against compromise. Using

CGI'S APPROACH

Our approach to federal application security solutions is tightly integrated with core development teams, targeted guidance and remediation solutions specific to the client's needs.

To maximize the effectiveness of evaluations, the team relies on creative and flexible testing methodologies that proactively identify vulnerabilities.

CGI's approach involves:

- Integration with the software development lifecycle
- Understanding the root causes of security defects
- Remediation guidance
- Overall system risk reduction
- Applied experience with similar systems
- Solutions meet all federal records management and security standards

various control categories such as technical, procedural/administrative and physical, database security services utilize techniques to detect potential input points of SQL injection, data leaks and database inconsistencies.

- **Network Security Evaluation** assesses the security posture of the network infrastructure based on industry standards. Evaluation includes network layer of the OSI model and how applications, services and upper layers can potentially be exploited, specifically at the port level of public internet accessible devices or servers.
- **Penetration Testing** uses a seven-step process to find vulnerabilities in an attempt to exploit the enterprise infrastructure. At a minimum, penetration testing provides a means for prioritizing the highest risk vulnerabilities.
- **Proactive Application Intrusion Detection (PAID)** leverages security technologies to proactively detect application-layer attacks, using the application itself. PAID provides advisory services on tuning and configuration of intrusion detection systems with the goal of preventing external and insider threats to the application.
- **Web Application Firewall (WAF) Configuration and Policy Management** inspects the contents of each incoming and outgoing packet at the application layer to prevent web application attacks. This service detects and prevents new attacks by watching for unusual or unexpected traffic patterns and providing configuration and policy guidance with common best practice considerations to ensure the highest level of security.

APPLICATION SECURITY REQUIRES EXPERIENCE AND EXPERTISE

CGI application security experts bring together diverse experience in cybersecurity, networking, development / coding, cloud computing, compliance and project management. Team members are experts in the latest techniques, attack vectors and approaches to application security, with multiple members holding advanced degrees in cybersecurity and industry certifications such as CSSLP, GWAPT CEH, and CISSP. They scour applications for potential security issues and control noncompliance, using references such as the OWASP Top 10, SANS Top 25, DISA STIGs and NIST SP 800-53.

The team evaluates more than 100 systems per year, including many large-scale, cross-domain applications. CGI's approach has proven to resolve defects with minimal cost and schedule impacts.

Our clients include government and commercial customers in the healthcare, finance, defense and other sectors.

RELATED SERVICES

- Security architecture and secure coding practices training
- Controls documentation, implementation and testing
- Application hardening
- Security awareness and technical training

ABOUT CGI

Founded in 1976, CGI is one of the largest IT and business process services providers in the world. We partner with federal agencies to deliver end-to-end solutions through high-quality business and IT consulting, systems integration and outsourcing services. CGI works with clients around the world through a unique client proximity and best-fit global delivery model to accelerate their digital transformation. Within CGI's cybersecurity solutions, CGI's Application Security, Architecture and Engineering Services help clients protect their business, applications and data. Committed to client success, our average client satisfaction score consistently measures 9 out of 10.

For more information
Visit **cgi.com/us-federal**
or contact **info@cgifederal.com**