TCG POSITIVELY DISTINCT®

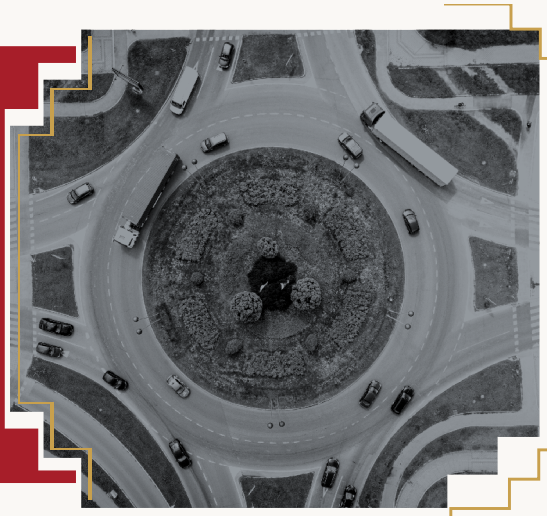
TCG CAPABILITIES

DevSecOps

SECURE SOFTWARE DELIVERY

Unifying teams for efficient, secure delivery.

In complex environments with distributed responsibilities, we build unified teams that share responsibility to consistently deliver and maintain secure applications and tools.



The TCG Approach

TCG uses an iterative approach across four dimensions to ensure that an agency's DevSecOps practice is perfectly tailored to their environment. Every engagement follows formal CMMI Level 3 and ISO processes, giving agencies auditable delivery and low execution risk.

Technologies

Identifying the nearest neighbor technologies to what's currently in use, so organizations don't need to upend their whole infrastructure.

Practices

Adopting and integrating practices in an order that will most positively impact the team at every step.

Zero-Trust

Planning and executing multiple iterations of Zero-Trust architecture based on the premises of elimination of implicit trust, continuous verification, and the assumption of a breach.

Team Building

Embracing collaboration, a core principle of DevSecOps, to work across the multiple vendors that perform development, security, and O&M.

Why Our Approach Works

ONLY PAY FOR FEATURES THAT AN ORGANIZATION NEEDS

A complete shift in an underlying platform, code repository, build process, and test process requires a large investment. Many times such a dramatic shift is unnecessary and wasteful. We help agencies assess their environment, find and implement the right tools, and, if a big change is needed, provide a solid foundation for making changes at the right pace.

MINIMIZE RISKS

Use of neighboring technologies and iterative transition helps avoid errors that are difficult to diagnose and system outages that often accompany new tools and processes.

MAINTAIN INSTITUTIONAL KNOWLEDGE

There is valuable institutional knowledge at agencies in the current architecture and maintenance. Reconstructing this knowledge for a new infrastructure is costly and time consuming.

3 KEY STRATEGIC TENETS

01

Agile Collaboration and Transparency

The DevSecOps approach works hand in hand with Agile methodologies to foster collaboration and transparency between development, operations, and other stakeholders. Agile practices such as Scrum or Kanban enable cross-functional teams to work closely together, promoting open communication and sharing of responsibilities.

02

Identifying Near Neighbor Technologies

“Near neighbor technologies” refer to tools, technologies, or practices that can integrate with or easily replace those already in use by a customer to enhance the development and delivery process. Examples include version control systems, continuous integration servers, automated testing frameworks, and containerization platforms.

03

Iterative Implementation

The DevSecOps approach follows an iterative implementation process to right-size the DevSecOps practices for the customer’s specific needs. They start with a small-scale pilot project or a single application and gradually expand DevSecOps practices based on feedback and lessons learned.

CONTINUOUS DELIVERY PIPELINE

SHARED RESPONSIBILITY

CONTINUOUS DEVELOPMENT

Release products quickly in small increments for continual improvement after deployment.

CONTINUOUS INTEGRATION

Automate integration of code changes to eliminate bugs and establish sustainable development pace.

CONTINUOUS TESTING

Develop tests before writing the code or feature to build in quality from the beginning.

CONTINUOUS DELIVERY

Deploy integrated changes with the press of a button to save time and ensure consistent delivery of reliable products to end users. Built with Terraform, Ansible, Docker, and Kubernetes.

SECURITY

Scan, test, and review code for security issues from the beginning of the development cycle using SonarQube, OWASP tools, and Tenable.

SECURE DELIVERY

SUCCESS STORIES

US INTERNATIONAL TRADE COMMISSION

TCG’s DevSecOps/Kanban pipeline deploys Congressionally mandated Harmonized Tariff Schedule updates within 15 days of enactment while exceeding unit test SLAs. Our Power BI-based Security Vulnerability Dashboard structures daily Tenable scan data so responsible teams can act quickly, with no per-user license required.

100%
On-time deployment of mandated HTS updates

50%
Reduction in open security vulnerabilities

SECURITY VULNERABILITY DASHBOARD

- Real-time automated updating and syncing
- Full history of vulnerabilities and remediation
- Filtering by responsible division, mapped to host names and applications
- Clear visualizations to track trends and recurring issues