

# Delivering Effective Programs & Tools For Addressing Cyber Threats



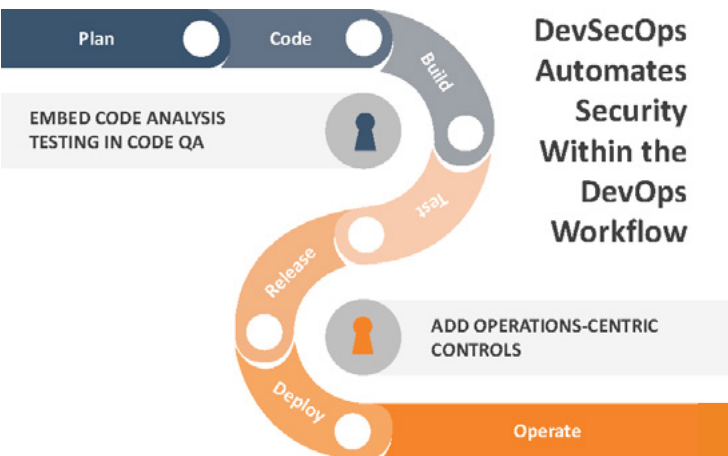
Organizations are making significant investments in cybersecurity, but threats continue to increase at a mind-boggling rate. No business is immune from attack. Furthermore, the shift to remote and hybrid work models, along with the adoption of new technologies, has expanded the attack surface that organizations must protect.

However, most organizations lack the resources to advance their security levels due to the persistent, industry-wide shortage of cybersecurity professionals. There aren't enough skilled and experienced people to fill open positions.

Technologent's **Security** program covers seven key areas encompassing the people, processes and technologies needed to reduce risk. Built on our proven methodologies, it is designed to enable efficiency and automation through repeatable systems. It is also flexible enough to be customized to meet each customer's business and IT objectives.

Our team of experienced professionals ensures the effective delivery of a comprehensive suite of security services. The program includes security assessment and advisory consulting, remediation planning and roadmap execution, high- and low-level architecture design, solutions implementation, operational management, and continuous monitoring and measurement.

## TECHNOLOGENT CYBERSECURITY FRAMEWORK



# Cybersecurity Solutions

## Security Program Management (Virtual CISO)

Cybersecurity should be managed as a program with dedicated resources and accountability. Security program management covers a wide range of activities: assessing risks, selecting and implementing controls that effectively address those risks, and ensuring effective long-term operation. Generally, program responsibility is vested in the CISO.

Technologent's virtual CISO services allow organizations to tap the expertise of an executive-level consultant who can help implement a security strategy that reduces risk while supporting operations. Our consultants have both business and IT experience, enabling them to work with business leaders to prioritize cybersecurity.

## Security Training & Awareness

Humans are the weakest link in the cybersecurity chain — 90 percent of security breaches involve user error, according to a Stanford University study. Few users don't know how to recognize threats or what to do when they encounter them. They fail to follow company policies and best practices and routinely engage in risky behavior.

Technologent helps organizations develop security training programs that help to promote awareness and effect long-term cultural change. Regular, engaging training is proven to help users retain what they've learned and apply it to their jobs.

## Security Policy Management

Organizations need effective policies that govern the basis for granting access to IT resources and the rules and procedures users must follow. These, in turn, help drive the development and implementation of system- and device-level policies that automate many administrative tasks and enable consistent enforcement of security controls.

Security policy management is the process of defining, deploying and maintaining policies throughout the IT environment. Technologent can assist organizations in developing these processes to ensure that security policies reduce risks without hampering operations.

## Third-Party Risk Management

The interconnected nature of today's supply chains creates one of the biggest threats. Business partners often need access to an organization's applications but may not have robust security controls or follow best practices. Hackers may find their way into an organization's systems by stealing third-party credentials or attacking a business partner's network.

The Technologent team can help evaluate the cybersecurity practices of your business partners and vendors against standard frameworks. We can recommend policies and procedures and identify vulnerabilities that put sensitive data at risk.

## Security Incident Management

Organizations must have an incident response that details the process of addressing a cyberattack in order to minimize downtime, damage and costs. Incident management is an overarching framework for evaluating, prioritizing and managing incidents.

Technologent helps organizations develop an incident management strategy and establish a cross-functional team that implements the incident response plan. Well-defined roles and responsibilities as well as policies and procedures will help ensure that security events are handled swiftly to reduce the risk of business disruption and data loss.

# Cybersecurity Solutions (Cont.)

## Security Architecture

All too often, organizations implement security tools to address specific threats without a unified design. The resulting “tool sprawl” makes it difficult for IT teams to manage the security environment and respond effectively to events and alerts.

The Technologist team has extensive experience in developing security architectures that identify needed controls, specify when and where to apply them, and create a structure for connecting the various components. Organizations gain an integrated environment capable of identifying and responding to complex threats.

## Vulnerability Management

Security is not a “set and forget” operation. As cyberattack methods evolve and new threats emerge, organizations must reassess their environments to identify gaps that could put critical systems and data at risk.

Technologist’s vulnerability management services focus on establishing processes for continuously identifying, prioritizing and remediating vulnerabilities across systems, applications and endpoints. Our in-depth understanding of business and IT operations and access to threat intelligence enable us to develop strong programs for quickly addressing high-priority vulnerabilities.

