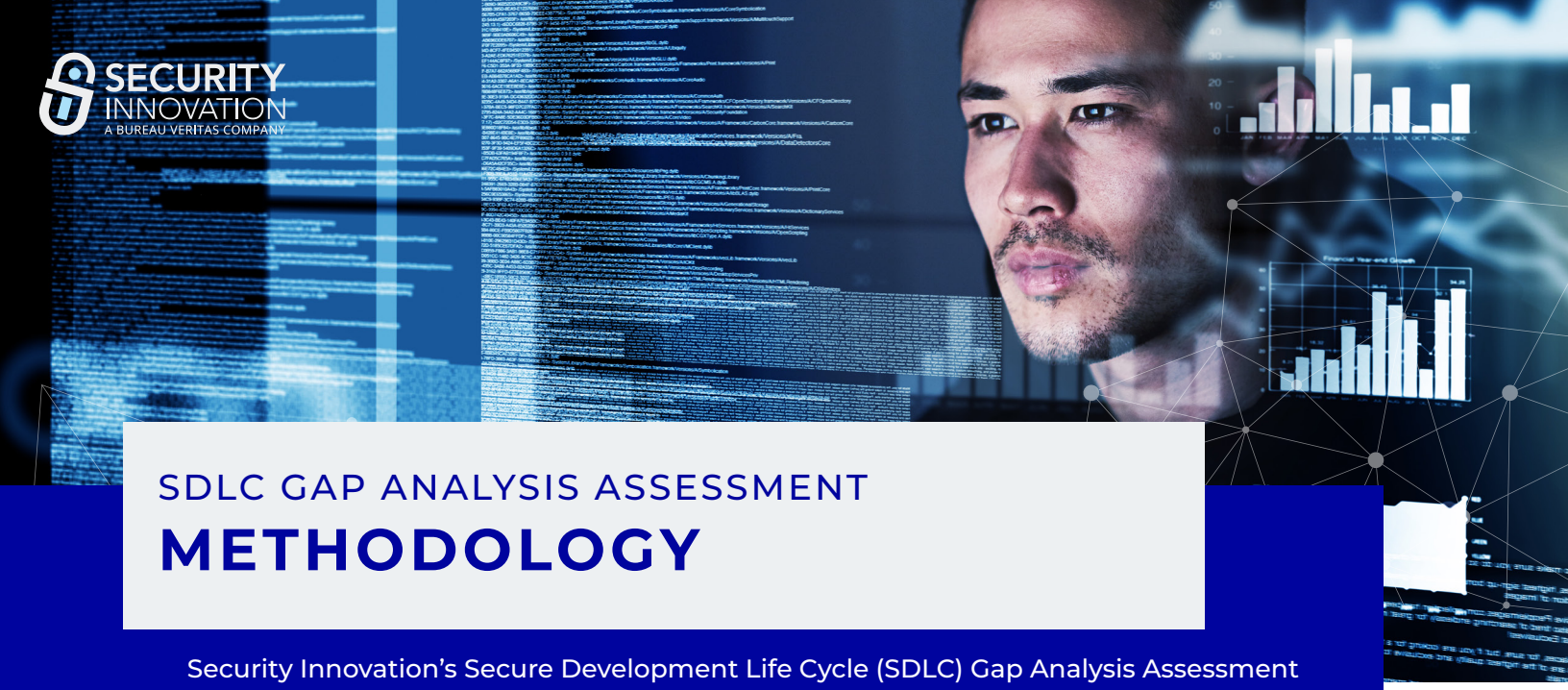

SECURITY INNOVATION
A BUREAU VERITAS COMPANY

SDLC GAP ANALYSIS ASSESSMENT

METHODOLOGY

Security Innovation's Secure Development Life Cycle (SDLC) Gap Analysis Assessment service offering is built upon the widely accepted five phases of a software development life cycle and can be applied to any development methodology or framework, e.g., Agile, RUP, Waterfall, etc.:

- Requirements
- Design
- Implementation
- Test
- Deployment

OUR PROGRAM ASSESSMENT METHODOLOGY CONSISTS OF FOUR PHASES:

Assess existing efforts

Identify security goals, objectives, and requirements

Evaluate gaps

Deliver a remediation roadmap

ASSESS EXISTING EFFORTS

In this phase, our goal is to understand the software development standards and processes, including everything that is currently being done with respect to software security. Our assessments are based on security industry best practices drawn from a number of industry sources, including the NIST Secure Software Development Framework (SSDF), OWASP SAMM, PCI Secure Software Lifecycle (Secure SLC), ISO 12207, ISO 15288, ISO 27002, ISO 27034, NIST SP 800-160, NIST SP 800-53, ITIL frameworks, the Microsoft SDL1, as well as our own extensive database of customer secure development lifecycle engagements.

Specifically, we will review your:

- Application security training program
- Application security policies and governance controls
- Security automation and tooling in place at each phase of the SDLC
- Organizational capabilities related to application security
- Requirements and design phase security activities including security requirements objectives, threat modeling, design practices and security design reviews
- Implementation phase security activities including secure coding practices and security code review documentation

SISALES@SECURITYINNOVATION.COM +1 877 839 7598 WWW.SECURITYINNOVATION.COM

- Test phase security activities including abuse case definition, threat modeling for penetration testing, and penetration testing
- Deployment and response phase security activities and preparedness including deployment practices, security deployment review processes, and attack response and patching processes

In each area reviewed, we will understand the state of your development security controls, activities, practices, processes, and policies and determine the gap between what is currently being done and industry current best practices in each area

IDENTIFY SECURITY GOALS, OBJECTIVES, AND REQUIREMENTS

This is a goal setting exercise in which we work with you to set appropriate goals to bring your application security development processes to the next level. In each area, we will help you set goals that will maximize your ROI, while

- Security Innovation is an approved Microsoft SDL Pro Network Partner minimizing your risk.
- Importantly, we also review customer requirements (legal, compliance, and other) to determine product/platform-specific risks. This will enable the prioritization of changes in the remediation roadmap.
- The result of this phase is a customized set of goals that we map against current practices and an ideal state to create a remediation plan for improving your security development practices and activities.

EVALUATE GAPS

We use your goals, requirements, and key risks to analyze gaps and prioritize the areas that are most in need of remediation based on practical and proven IT risk and cost/benefit considerations. The final step of this phase is the creation of a software risk remediation roadmap, which becomes the basis of specific security improvement initiatives.

The SDLC assessment process reviews the following kinds of application lifecycle security controls, activities, practices, and processes:

- Software security requirements gathering
- System architecture and design reviews
- Threat and attack modeling
- Secure coding guidance and practices
- Secure code reviews
- Application security testing
- Security and Quality defect management processes
- Release management practices
- Secure application deployment practices
- Secure software maintenance practices
- Application security incident response
- Security tool chain review
- Application security training program review

DELIVER AND EXPLAIN REMEDIATION ROADMAP

The development team will receive a prioritized listing of the remediation recommendations. During the Executive Briefing, we discuss the remediation recommendation highlights and answer questions about the recommendations.