



Tactical Remediation & Advanced eXecution by K logix

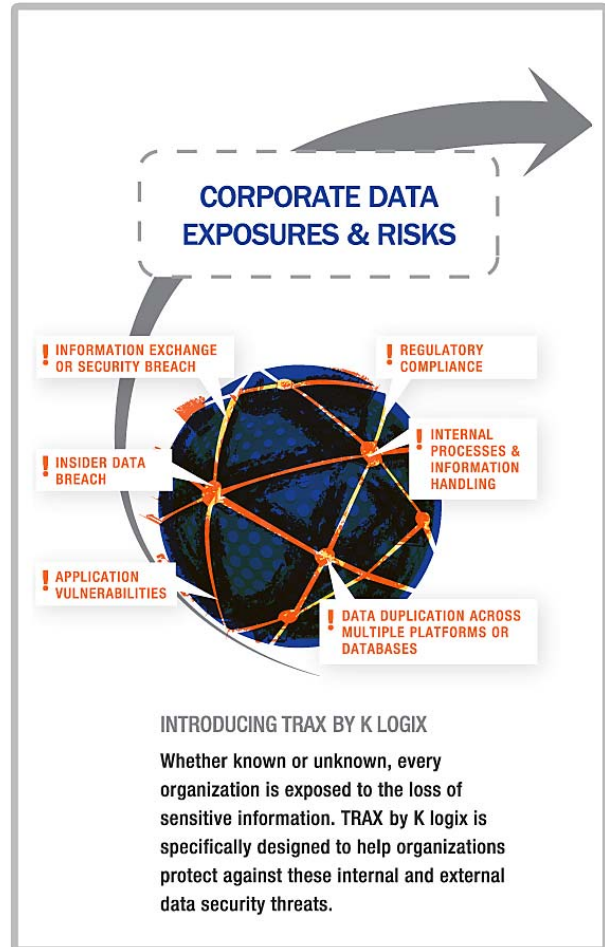
In this early part of the 21st century, our collective ability to generate, store, move, and manipulate information has nearly eclipsed our ability to fully understand and control it. As a result, internal and external data breaches have reached all-time highs. In coming years, organizations will have to get smarter about the way they optimize, manage, and protect critical information. Engaging with K logix **TRAX**, a service-based information security solution, is how many will do it.

K logix TRAX uses a three-phased approach, beginning with a **Vital Security Assessment**—an analysis of a firm’s critical information and its interactions with users, applications, and distribution points. The second phase is a comprehensive report and detailed **Game Plan for Remediation**. The last phase involves the **Execution of Strategy** set forth in the Game Plan, which includes heavy focus on mitigation of security risks to critical information.

Governments and other entities are doing their slow and methodical best to establish and mandate compliance with rules and regulations designed to mitigate security lapses, but those actions are largely reactionary.

In the end, businesses themselves are responsible for their own information and solely accountable for how its security affects their customers, employees, shareholders, and partners. Consequently, all businesses must look within and understand where their critical data resides, identify weaknesses, anticipate possible routes of attack, and take proactive measures to prevent them.

K logix **TRAX** information security methodology empowers firms of every size to do just that.



TRAX quantifies and remediates disclosure risk associated with critical information by providing the capability to discover and classify critical data, analyze the access and distribution of that data, and measure and test the security of applications that interact with the data.

The **TRAX** information security methodology is fueled by The K logix team of security specialists with niche focus areas in data discovery, network protocol security, forensics, cryptography, and application penetration testing. Our team honed their skills at places like @Stake and QinetiQ Trusted, and all have otherwise strong backgrounds in information security. Over the past decade, we've built a reputation for being able to secure the most critical applications and data for the largest companies in the world.

K LOGIX TRAX METHODOLOGY

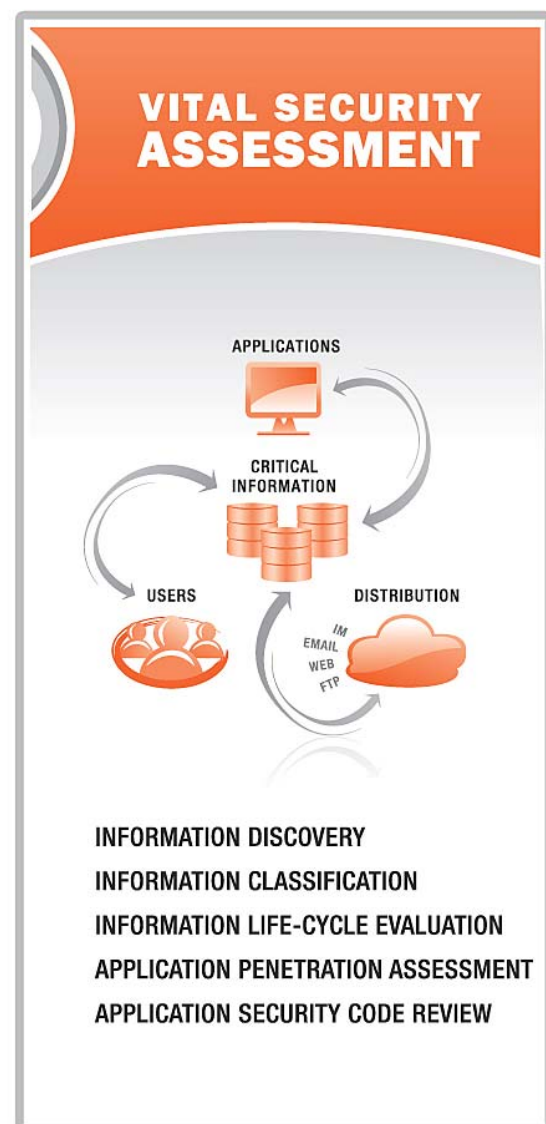
Vital Security Assessment

Information Discovery

K logix TRAX was developed to help our customers that required assistance performing security assessments on particular databases or applications, where some or all of their confidential information resided. What we quickly realized was that many firms do not know what information is critical, nor do they know where that information is located.

During Information Discovery, K logix works with the client:

- To understand existing technical safeguards, which may help limit exposure to sensitive data
- To understand existing business processes
- To understand technical system components
- To understand data flow and information lifecycle
- To understand types of data stored, processed, or transmitted by the systems within the scope of the project



Information Classification

Adhering to a formal Data Classification Program is just one of the many keys to proper information security practice.

During this phase of the assessment, K logix works with the client:

- To identify existing data classifications
- To identify security controls
- To assist in the classification of information identified during Information Discovery
- To verify the information lifecycle of critical data within an organization and determine whether controls are adequate to safeguard a company's most valued information

In organizations where information classification standards haven't been defined, K logix works with the client:

- To define information classification categories
- To design protective controls necessary to safeguard data based on these classifications
- To identify and understand business risks and any relevant industry or regulatory drivers
- To understand the overall importance and classifications of the data and policies
- To identify any existing protective controls used to enforce access to or safeguard the data
- To verify the information lifecycle of critical data within an organization and determine whether controls are adequate to safeguard a company's most valued information

Information Lifecycle Evaluation

Reviewing an organization's Information Lifecycle is a critical step to ensure that information is adequately safeguarded from malicious or inadvertent disclosure.

By using the data gathered during the Information Discovery Assessment and Information Classification, **TRAX** will:

- Validate a firm's information handling policies and practices throughout their actual lifecycle
- Perform point-in-time validation of the location of critical data
- Identify components that store, transmit, or process this data
- Seeks understanding of the controls used to safeguard the data within the existing lifecycle

Upon performing this evaluation, **TRAX** will determine whether gaps exist between the expected information lifecycle and associated security controls in contrast to those identified during the assessment.

Further, **TRAX** will evaluate the relevance of existing policies and controls as compared with best practices and provide a roadmap to achieve more rigorous protection.

Application Penetration Assessment

The purpose of the Application Penetration Assessment within **TRAX** is to evaluate a production-like deployment of the application components, review its security architecture, enumerate potential threats, and validate those threats during the penetration assessment. During the application penetration phase of a project, the application security team evaluates the likelihood or potential impact on confidentiality, integrity, and availability of the application.

The **TRAX** Application Penetration Assessment serves as a cost-effective mechanism to perform a baseline assessment of potential exposures within an application or system. It's intended to simulate real-world attack scenarios on systems, networks, or data.

The following outcomes are key objectives of this exercise:

- Review relevant documentation to identify potential vulnerabilities
- Review the application's core functionality
- Assess detailed design documentation and conduct interviews with key stakeholders (application architects & developers)
- Analyze the interaction between the application and integrated components or products
- Identify security vulnerabilities and the impact associated with exploitation scenarios
- Analyze application in production
- Perform informed vulnerability tests against authentication, authorization, session management, and use of cryptography

Application Security Code Review

The **TRAX** Security Source Code Review identifies instances of insecure coding practices and other language-specific security vulnerabilities. The results from this review provides clients with a detailed list of implementation-level security findings and general guidance regarding how to adjust the Software Development Lifecycle (SDL) to reduce the occurrence of often repeated coding mistakes.

The following areas are commonly assessed:

- Implementation of authentication, authorization, and session management

- User input validation, including the handling of user input data intended to execute additional functions or spawn external programs
- Proper use of cryptography
- Existence of hard-coded information
- Proper handling of security-critical data, including authentication credentials and cryptographic keys
- Proper use of security-critical APIs
- Secure interaction with the operating system, web server, file system, etc.
- Appropriate error handling
- Existence of test or debug code not intended for production deployment
- Logging of errors and informational messages
- Information leakage
- Adherence to any additional secure code standards required by the client
- Code maintenance and code complexity

Remediation Game Plan

Standards and Procedures

While planning remediation, K logix compares the **TRAX** findings with the client's organizational standards and procedures. This comparison is done to reduce the likelihood of future threats with proven standards and processes that mitigate and safeguard client systems and information. K logix can help define standards and processes based on industry standard frameworks, such as ISO 27002.

Detailed Vulnerability Report

The **TRAX** Detailed Vulnerability Reports provide both key business and technical staff the information necessary to prioritize and implement remediation recommendations quickly and effectively.

Some areas of focus include:

- Prioritization of vulnerabilities based on difficulty of exploit, remediation effort required and impact of exploit on business
- Additional research to support analysis and proof of vulnerabilities



- Delivery of reports, which includes findings, analysis, and recommendations
- Transfer of knowledge

For a client's business staff, **TRAX** provides an executive summary that outlines key risks identified during the assessment and areas in which an organization performed well. **TRAX** prioritizes remediation recommendations based, ranging from easy-to-implement, short-term tactical fixes and longer-term strategic recommendations.

For a client's technical staff, **TRAX** outlines each vulnerability, explaining the vulnerability in detail, outlining the potential business impact, the difficulty of exploit (where applicable), steps necessary to reproduce or verify existence of the vulnerability, and the recommendations needed to eliminate or mitigate each identified risk. **TRAX** summarizes the assessment into areas of analysis, comparing major themes of the assessment against industry best practices and outlining recommendations to better align with those best practices.

Outlined Data Protection Game Plan & Recommendations

K logix analyzes information gathered during the Vital Security Assessment stage of **TRAX** and prioritizes vulnerabilities based on risk. The end result is a gap analysis between existing standards and procedures vs. identified vulnerabilities. In addition to risk prioritization, K logix provides clients with a recommended action plan for remediation and reviews these with the appropriate client-side team. K logix will then work with that team to develop information-handling policies that ensure adequate protection of high-risk data.

A detailed plan will be put in place to address the following:

- Implementation and adherence to data classification categories
- Recommendation of protective controls for safeguarding data
- Developing long-term recommendations for information security enhancements
- Identify and make recommendations for addressing security issues of immediate consequence
- Developing long-term recommendations and strategic initiatives to enhance security by leveraging industry best practices

Business Impact Evaluation

The **TRAX** Business Impact Evaluation provides an executive summary, detailing the set of exposures within the organization that could adversely impact business.

Some areas of focus:

- Impact associated with most likely and worst case exploitation scenarios
- Impact of security breach
- Impact of data loss
- Impact of inadequate data handling procedures

- Consequential impact on customers, partners, etc.

Execution of Strategy

Security Training Awareness

TRAX Security Training Awareness will provide a detailed understanding of these topics:

- The importance of data classification
- Employee behavior for handling critical data sets
- Managing exposure through policy
- Incident response & forensics
- Foundations of application security (classes charged separately)

Best Practices for Information Protection

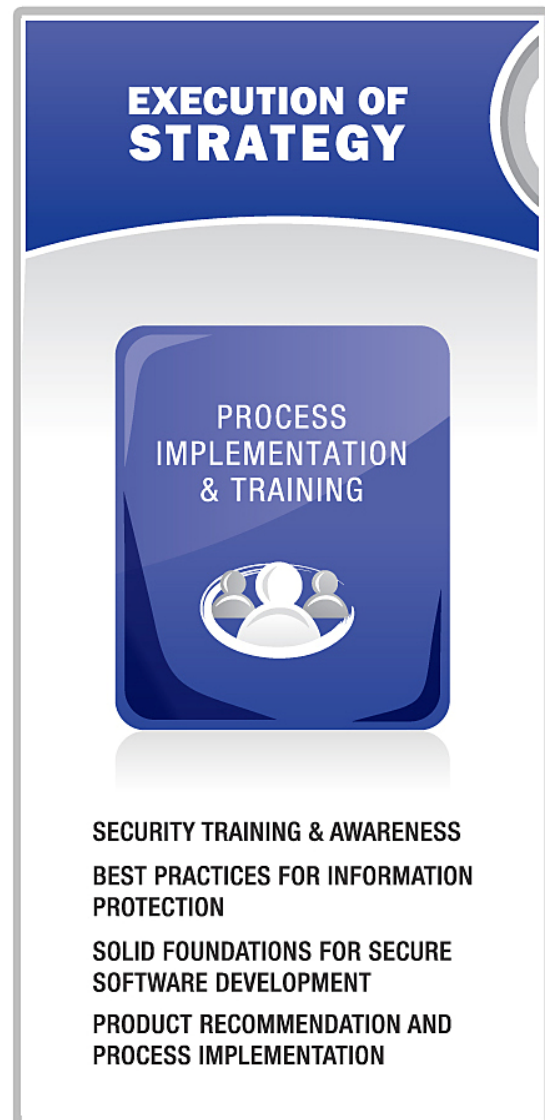
K logix **TRAX** has a discipline-driven set of Best Practices for Information Protection. These guidelines take into account industry, regulation, and compliance:

- Industry specific regulatory compliance
- Emphasis on internal data handling policies
- Employee education in data loss prevention best practices
- Best practices to become “TRAX Certified”

Solid foundations for secure software development

TRAX will provide the client with a detailed list of guidelines on how to adjust the development process to reduce the occurrence of application vulnerabilities. Some of the topics covered will include:

- Detailed framework, set of principals, and disciplined methods for development of secure code
- Process for lifecycle code review analysis for development team



Product recommendation and process implementation

Technology is needed to help enforce security policies and procedures. K logix will make technology recommendations to create a layered security approach that enforces the client's information security polices. This automation enables the client to quickly adjust and defend against changing regulations and security threats.

As an additional service, K logix will architect and deploy these solutions in a timely fashion based on budget and business impact.

