Mantis Adaptive Security Risk Assessment and Mitigation Methodology

Overview

Mantis Security consultants test the effectiveness of an organization's infrastructure and application security program against real world threats. Our methodology assesses security effectiveness beyond just regulatory compliance in order to improve operational security through a remediation and mitigation strategy that aligns with business objectives and risk tolerance.

Using the Mantis Adaptive Security Risk Assessment and Mitigation Methodology, an organization's infrastructure and application security architectures will be evaluated for effectiveness using leading security principles and practices. This approach provides measurable security benefits beyond those of a traditional security compliance assessment by completing a prioritized, detailed security evaluation of areas of greatest concern.

Methodology Benefits

- Tailored towards business objectives, risk tolerance, and security concerns
- Identifies and prioritizes the security areas that require an in-depth technical security review
- Evaluates the effectiveness of the most important applied security controls (management, operational, and technical)
- Provides a remediation and mitigation strategy based on leading security principles and practices

Mantis Security Approach

We assess our customer's security program's effectiveness. Our approach is a standards-based, lightweight and adaptive methodology, requiring minimal organizational involvement, expertise, and other limited resources. It allows us to perform an overall security risk assessment in **three phases**:

1. Lightweight, tailored risk assessment
2. Detailed technical security review
3. Remediation & mitigation roadmap

Phase I – Lightweight, Tailored Security Risk Assessment

Our security assessment team follows a blend of risk assessment methodologies that provide a comprehensive risk analysis. This allows us to evaluate security from a threat-centric and information asset-centric perspective, while tailoring towards an organization's security concerns.

Mantis Adaptive Security Risk Assessment Methodology

Approach	Benefits
1. Establish risk tolerance and measurement criteria	• Evaluates areas most significant to its mission and business objectives • Ensures mitigation decision consistency across multiple information assets and operating or departmental units
2. Identify threat agents, motivations, and methods (threat-centric perspective)	• Identifies threat agents that pose the greatest risk, including their objectives and methods for exploitation • Cross-referenced with existing vulnerabilities and controls libraries to identify areas of greatest exposure
3. Identify the critical information assets (information asset-centric perspective)	• Provides a comprehensive profile of critical information assets and their containers (e.g., internal hosted databases, external laptops, file cabinets, etc.) that identify the asset's boundaries and security requirements • Serves as the basis for the identification of threats and risks for critical information assets
4. Identify organizational security concerns	• Represents real-world areas of concern, and will represent threats and their corresponding undesirable outcomes.
5. Identify threat scenarios overlapping threat-centric and information-asset centric perspectives	• Provides an opportunity to consider probability of threat scenarios (useful in later steps to prioritize risk mitigation activities)
6. Identify greatest threat-risks and compare to vulnerabilities and controls and determine exposure	• Assists in profiling potential cyber threats as they relate to information assets protected by security features
7. Identify and prioritize risks and remediation opportunities, aligning with risk measurement criteria and security concerns	• Evaluates consequences if a threat is realized, completing the risk picture
8. Determine and prioritize the detailed security evaluation areas based on criticality, likelihood, risk tolerance, and security concerns	• Provides a strategy that considers the value of the information assets and baseline security requirements

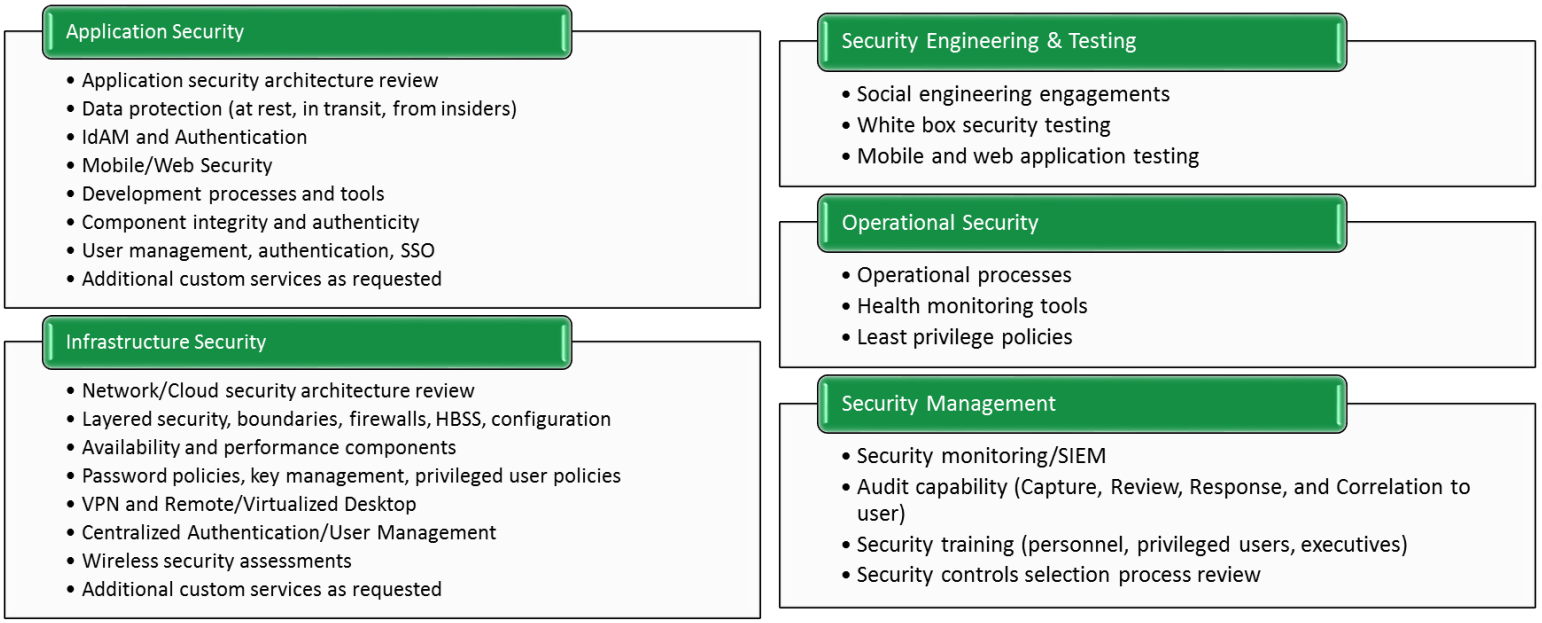
Phase II – Detailed Technical Security Review

Our security architects and engineers perform detailed technical reviews of the infrastructure and application components that revealed the highest risk (as determined by business priority, exposure, and probability). After each security evaluation area has been determined (through Phase I analysis), a

detailed security review is performed for each area (which may be a management, operational, or technical security concern).

Detailed security effectiveness evaluation activities are generally comprised of five focus areas:

1. Application Security
2. Infrastructure Security
3. Security Engineering & Testing
4. Operational Security
5. Security Management



Phase III - Remediation & Mitigation Roadmap

Security findings from each detailed technical security review (through Phase II) are used to produce a detailed remediation strategy. Recommendations may target improvements to management, operational, or technical security areas, including security architectures, continuous monitoring, component modernization, system and network configurations, system health and event monitoring, SDLC CM, and security awareness training.

- A detailed roadmap is provided for each recommendation based on organizational inputs such as criticality, schedules, cost, and other factors.
- Periodic (or automated) assessment may be recommended for security areas of high concern
- Report and presentation