Avocado

Avocado Systems, Inc.

Securing the Future of Applications with AI-Driven Insight

Avocado Reveal-AI: Unleashing Proactive Security Through Automated Threat Modeling

In today's fast-paced digital landscape, applications are the lifeblood of organizations across critical industries like telecommunications, banking, and defense. However, with increasing complexity and rapid development cycles, traditional security approaches are often reactive, slow, and unable to keep pace with evolving threats. The need for a proactive, intelligent solution has never been more critical.

Avocado Systems introduces the Avocado Security Platform, an innovative suite designed to embed security throughout the entire application lifecycle. A core component of this platform is **Avocado Reveal-AI**, a revolutionary application security solution that leverages cutting-edge Artificial Intelligence (AI) to transform manual, time-consuming threat modeling into an automated, real-time, and actionable process.

What Avocado Reveal-AI Offers: Key Features and Benefits

Avocado Reveal-AI moves beyond static analysis, providing dynamic, AI-driven insight into application vulnerabilities before a breach occurs. It offers a comprehensive suite of features designed to empower security teams, developers, and compliance officers.

Automated Expertise

Advanced tool capable of swiftly identifying and assessing threats throughout the SDLC Developers without extensive security backgrounds, can benefit from an intelligent co-pilot in addressing vulnerabilities effectively

Real-Time Mitigation Guidance

- Real-time mitigation guidance, bridging the knowledge gap for developers
- Instantaneous feedback allows developers to implement security measures proactively
- Gen-AI workflow in shift-left saves time and resources

Accelerated Delivery

- Developers can focus on writing code with confidence, while Gen-AI is actively identifying and guiding the mitigation of vulnerabilities
- 90% reduction in time compared to manual pre-design threat modeling
- Effective shift-left for faster and secure delivery

Streamlined Collaboration

- Streamlined collaboration between security teams and developers
- Breaks the siloes and fosters a common language and understanding of security and best practices

1. AI-Driven Threat Modeling – Automated Expertise

Avocado Reveal-AI automates the complex and often subjective process of manual threat modeling. The platform's AI engine analyzes the application's architecture, data flows, and runtime behavior to construct an accurate, dynamic threat model.

- **Benefit:** This ensures comprehensive coverage and consistency, eliminating human error and drastically reducing the time required to understand potential attack surfaces.
- **Example (Banking/Finance):** In a complex microservices-based banking platform, Avocado Reveal-AI automatically maps every data transaction endpoint, identifying potential insider threats or data leakage points in real-time fund transfers, ensuring compliance with data privacy regulations like GDPR or CCPA.

2. Real-Time Mitigation Guidance

Security vulnerabilities are only half the battle; knowing how to fix them quickly is crucial. Avocado Reveal-AI provides specific, actionable, and context-aware mitigation steps for every identified vulnerability.

- **Benefit:** This bridges the gap between security teams and development teams, allowing developers to implement fixes rapidly without needing deep security expertise.
- **Example (Defense):** For an IoT sensor network used in field operations, Avocado Reveal-AI identifies a weak authentication mechanism and provides the exact code snippets and configuration changes required to implement FIPS-compliant multi-factor authentication, ensuring operational resilience.

3. Streamlined Collaboration

The platform is designed to break down organizational silos. By providing a single source of truth for all threat data and mitigation efforts, it fosters seamless collaboration between Security, DevOps, and Compliance teams.

- **Benefit:** Clear, shared understanding of risks and responsibilities accelerates decision-making and ensures everyone is aligned on security priorities.
- **Example (Telecommunications):** When a new 5G network function virtualization (NFV) component is deployed, cross-functional teams use Avocado Reveal-AI’s shared dashboard to track, prioritize, and remediate vulnerabilities identified in the dynamic network environment, ensuring minimal service disruption.

4. Accelerated Delivery

By shifting security left and automating the most time-consuming aspects of vulnerability identification and remediation, Avocado Reveal-AI helps organizations deliver secure applications faster.

- **Benefit:** This integration of security within the CI/CD pipeline prevents security bottlenecks, allowing organizations to maintain rapid development velocity without sacrificing security posture.

How Avocado Reveal-AI Works: A Step-by-Step Approach

Avocado Reveal-AI seamlessly integrates into existing development workflows, providing a continuous feedback loop for security posture improvement. The process is fully automated and driven by proprietary AI capabilities.

Step 1: Avocado Reveal Builds an Automated Runtime Threat Model

Upon integration into the application environment (staging or production), Avocado Reveal-AI automatically begins observing the application's behavior, architecture, data flows, and dependencies in real-time. It constructs a dynamic, living model of the application's ecosystem.

Step 2: Automatically Find and Map Application Module / Architecture / Functional Vulnerabilities

The AI engine analyzes the generated threat model against a vast knowledge base of known vulnerabilities (CVEs, OWASP Top 10) and emerging threat patterns. It systematically maps specific risks to individual application modules, architecture choices, and functional behaviors.

Step 3: Identify and Describe Most Appropriate Mitigation Steps for Each Vulnerability

For each identified vulnerability, the system's AI provides precise, context-specific remediation instructions. It details *what* needs to be fixed and *how*, often including links to documentation or best practice guides. In appropriate suggestions, it may include code snipets.

Step 4: Identify and Describe Impacts of Mitigation Including Required Compliances

A crucial differentiating feature, Avocado Reveal-AI assesses the potential impact of applying a mitigation in positive and negative manners. It describes if a fix might automatically mitigate other major issues or corner cases. It also cross-references required industry-specific compliance standards (e.g., PCI-DSS, HIPAA, FedRAMP, NIS2, etc.), ensuring all fixes meet regulatory requirements.

Step 5: Automatically Generate a Full Threat Model in Various Formats and Make it Downloadable

The final output is a comprehensive, exportable threat model documentation package. This report, available in formats like PDF, JSON, HTML or integrated directly into GRC tools, provides an audit trail for compliance and a clear strategic overview for management. Application Security teams can also get fully automated threat models for OWASP Threat Dragon, Microsoft Threat Modeling Tool, or other industry accepted threat modeling tools.

Conclusion

Avocado Reveal-AI is not just another security tool; it is an intelligent partner in application security. By automating the threat modeling process and providing actionable, AI-driven guidance, it empowers organizations in critical sectors to proactively manage risk, maintain compliance, and accelerate innovation securely. Transform your security posture today with Avocado Reveal-AI and focus on what you do best: building exceptional applications.

To learn more and schedule a demo, please visit the Avocado Systems website at www.avocadosys.ai or email us at info@avocadosys.com.