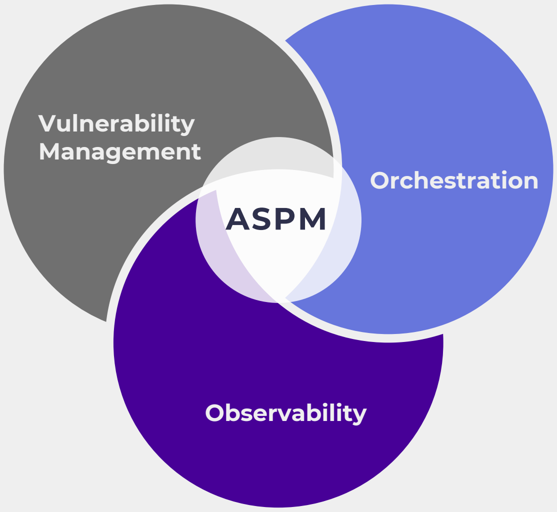
UNDERSTANDING ASPM

OVERVIEW

The importance of Application Security has grown, compounding the complexity of maintaining the complete application security lifecycle. To fully manage an organization's application security posture, it requires a fully integrated platform combining vulnerability management, orchestration, & observability so that organizations can transform application and security data into actionable information.



VULNERABILITY MANAGEMENT

Vulnerability Management is a cornerstone of any effective application security program. Here's why it's critical and what you need to consider:

- Core Functionality: Aggregates, prioritizes, and tracks remediation of vulnerabilities.
- Limitations: Only addresses a part of the full application security lifecycle.
- Contextual Importance: Must be integrated into a broader security program to be truly effective.
- Unified Defense: Combining vulnerability management with other security components builds a more adaptive and unified defense against threats.
- Beyond List Management: Standalone solutions are limited; dynamic workflows and risk-based prioritization are essential for significant improvements.
- Integration: Essential for responding to changes in application and security requirements within the SDLC.

1. CONSOLIDATION
2. RISK-BASED PRIORITIZATION
3. BACKLOG MANAGEMENT
4. SLA MANAGEMENT

ORCHESTRATION

Orchestration in application security goes beyond automation by coordinating entire workflows and ensuring processes are executed correctly. Here's why it matters:

- Process Focus: Manages entire workflows involving multiple automated tasks, ensuring end-to-end administration.
- Vendor Integration: While single-vendor solutions may work, most organizations need a universal platform that supports various tools.
- Tool Agnostic: Allows plug-and-play integration from different vendors, evolving with the security program.
- Scalability: Essential for managing the ratio of developers to security managers, preventing security bottlenecks.
- Contextual Awareness: Must be integrated with SDLC awareness and risk-management metrics to effectively contextualize security components.

1. POLICY DEPLOYMENT
2. SECURE GATEKEEPING
3. EXCEPTION MANAGEMENT
4. SCHEDULED SCANS

UNDERSTANDING ASPM

WABBI

OBSERVABILITY

Observability provides a holistic view of system health and performance, crucial for understanding the 'why' behind system behaviors. Here’s why it’s essential:

- Single Pane of Glass: Offers a comprehensive view by collecting and correlating diverse data sets.
- Distinction from Monitoring: While monitoring focuses on predefined metrics and alerts, observability aims to infer internal system states.
- Proactive Insights: Enables a deeper understanding of system issues, allowing for more proactive problem-solving.
- Contextual Understanding: Emphasizes data correlation to provide context and deeper insights.
- Limitations: On its own, observability tools may provide insights but fall short in managing the complete application security lifecycle within the SDLC.

1. GUIDED ACTIONS
2. ACTIONABLE INSIGHTS
3. SIGNAL WORKFLOWS
4. DYNAMIC MANAGEMENT

APPLICATION SECURITY POSTURE MANAGEMENT (ASPM)

An ASPM solution must combine vulnerability management, orchestration, and observability because these elements together enable risk-based security management, from policy deployment and enforcement to coordinating responses and prioritizing risks. Without this integrated approach, organizations lack the context and responsiveness required to manage application security in the SDLC.

- Management Focus: Ensures control and consistency in managing application security.
- Comprehensive Approach: Combines vulnerability management, orchestration, and observability into a unified platform.
- Actionable Insights: Transforms data into actionable information for better decision-making.
- Industry Recognition: Named one of Gartner’s transformational technologies in cybersecurity.
- Holistic Security: Offers a comprehensive view and control of security across applications and infrastructure, aligning security with business objectives.

Organizations need an end-to-end ASPM platform to effectively advance their application security programs and integrate security into development. Relying on point solutions leads to a fragmented, incomplete approach. Remember, the key components are:

- **Vulnerability Management**: Organizes data
- **Orchestration**: Puts data into workflows
- **Observability**: Makes data insightful

Only by integrating all three can organizations manage cyber risk in line with business objectives.