

Spotlight Guide:

Leveraging Cycode AI & SAST in a Complete ASPM at Nomi Health



Alex Flowers
Application Security Lead,
Nomi Health

Introduction

Nomi Health, a leading healthcare provider, is at the forefront of integrating AI-powered Static Application Security Testing (SAST) remediation into their DevSecOps practices. This guide outlines their approach and success, offering inspiration for other organizations seeking to enhance their security and development workflows.

Why AI SAST Remediation?

- **Enhanced Efficiency:** Identifies and fixes vulnerabilities in the code before they reach production.
- **Increased Velocity:** Automates the detection and remediation process, reducing manual effort and time.
- **Improved Code Resiliency:** Provides developers with precise, personalized, context-aware fixes, leading to cleaner, more secure code.



The coolest part here is that the code is contextualized exactly for my development teams. As a security engineer I'm confident that everything that's automated and integrated directly into Cycode is personally for my developers.

- Alex Flowers

Implementation at Nomi Health

01

Integration with Development Pipelines

- **Seamless Integration:** AI SAST tools are integrated directly with our IDEs' and into CI/CD pipelines, ensuring continuous security checks.
- **Automated Scans:** Every code commit triggers an automated scan, catching vulnerabilities early in the development cycle.

02

AI-Powered Remediation

- **Contextual Fixes:** AI provides context-aware remediation suggestions, tailored to the specific codebase and development environment.
- **Developer Empowerment:** Developers receive clear, actionable insights to their code, enabling them to fix issues efficiently.

03

Collaborative Approach

- **DevSecOps Alignment:** Close collaboration between development, security, and operations teams to prioritize and address vulnerabilities.
- **Training and Support:** Continuous education and support for developers on security best practices and tool usage.



The relationship with Cyscale has been immense because AI in itself is a transformation that is changing constantly and quickly in any organization so it's essential to have a partner that I can always rely on through the process.

- Alex Flowers

Benefits Realized

Faster Time to Market

- **Reduced Bottlenecks:** Automated remediation reduces the need for extensive security reviews, accelerating the development process. It starts with being able to have the ability to have a Complete ASPM that can prioritize and separate those thousands of vulnerabilities down to groups that really matter.
- **Improved Productivity:** Developers spend less time on manual vulnerability investigation and fixes — and more on feature development.

Strengthened Security Posture

- **Proactive Security:** Early detection and remediation prevent vulnerabilities from being exploited in production.
- **Continuous Improvement:** Regular feedback loops and metrics drive ongoing improvements in security practices.

Cost Efficiency

- **Reduced Remediation Costs:** Fixing vulnerabilities early in the development cycle is significantly cheaper than addressing them post-deployment.
- **Resource Optimization:** AI-driven automation allows the security team to focus on more strategic initiatives.



With Cyscale we know that we have the workflows, controlled shift left capabilities, and AI remediation to make sure we don't only just detect, but prevent violations before they go into production for Peace of Mind. Cyscale's Executive Dashboard gives me real numbers I can report on and see actual progress made.

- Alex Flowers

Key Takeaways for Other Organizations



Start Small, Scale Gradually

Begin with pilot projects to demonstrate value and organize so that you can build confidence within the development teams.



Embrace Automation

Leverage Cymode's remediation guidelines AI capabilities to automate personalized code, allowing your team to focus on critical security challenges and for developers to focus on developing, not on fixing.



Foster Collaboration

Encourage close collaboration between development, security, and operations teams to ensure a unified approach to security.



Documentation

Document your own personalized Cymode environment so that you can share with others and any company or outside stakeholders.



Invest in Training

Provide ongoing training and support to help developers understand and embrace AI-powered security tools.



Cymode's philosophy of making application security a team sport between development and security has really engrained itself into the fabric of our culture.

- Alex Flowers

Conclusion

Nomi Health's successful integration of AI SAST remediation showcases the transformative potential of AI in DevSecOps. By adopting similar practices, organizations can enhance their security posture, improve development efficiency, and achieve faster, more secure software delivery.