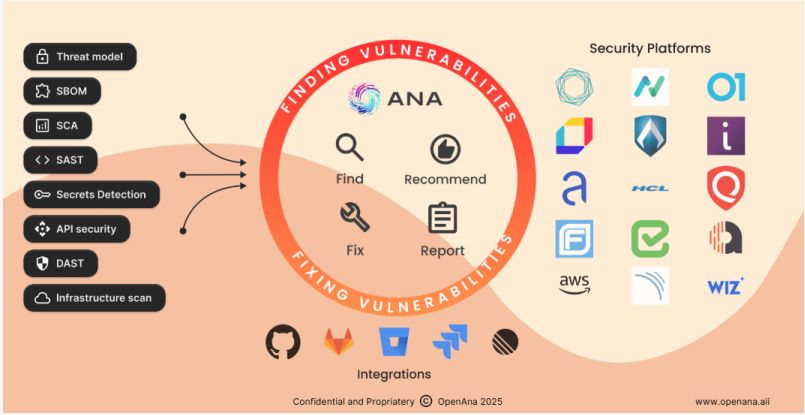
OpenAna Launches Autonomous Security Engineers to Transform Enterprise Vulnerability Remediation

OpenAna automates security fixes, eliminating backlogs & cutting remediation time by 80%. Enterprises go live in days & see ROI in weeks.



Ana, Autonomous Security Engineer Overview for Code, API and Infrastructure

NEW YORK, NY, UNITED STATES, April 29, 2025 /EINPresswire.com/ -- Cybercrime is projected to inflict $9.5 trillion in global damages in 2024, with the average cost of a data breach in the U.S. reaching $9.36 million. Despite significant investments in security technologies, enterprises remain vulnerable due to an overreliance on detection tools that fail to close the remediation gap.

Security teams are identifying more vulnerabilities than ever before—but attackers are moving faster. According to industry reports, 82% of cyberattacks exploit known vulnerabilities that organizations failed to patch in time. Manual remediation often takes weeks or months, while threat actors operate in hours.

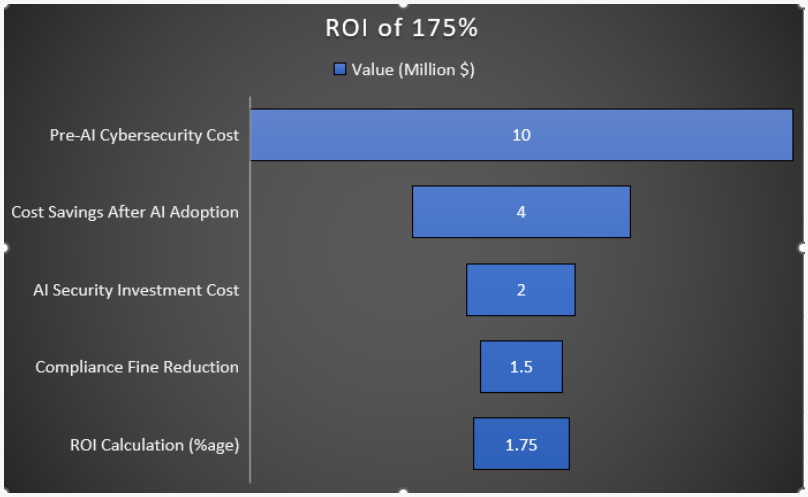
> Ana, an Autonomous Security Engineer focuses on remediating vulnerabilities helping enterprises implement a scalable remediation solution and advance shift left implementation by empowering engineers."
>
> *Arsh Anwar, CTO, OpenAna*

As security alerts pile up and developer productivity slows, organizations face mounting operational and compliance risks.

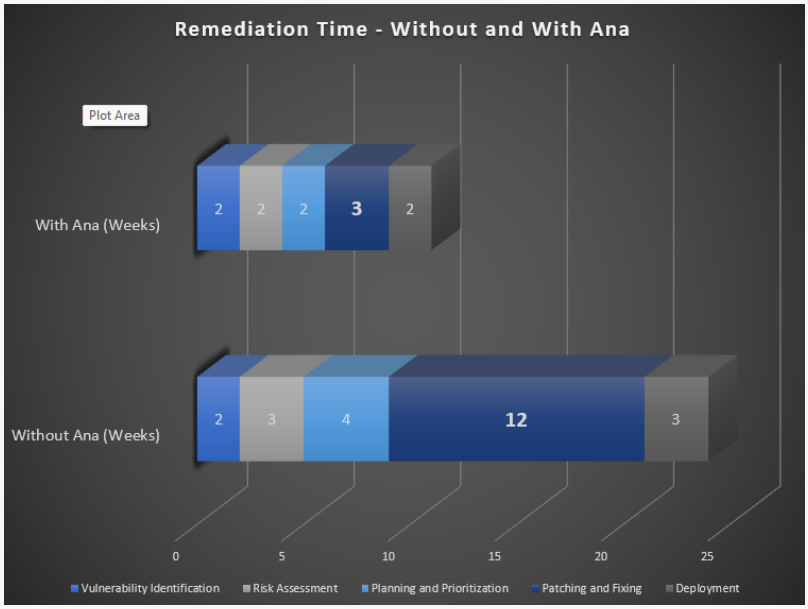
Addressing the Growing Remediation Gap with Ana AI
To address this challenge, OpenAna today announced the launch of Ana AI Autonomous Security Engineer (ASE) a breakthrough in enterprise security operations. Unlike traditional tools that only detect vulnerabilities, Ana autonomously fixes security issues, generating, validating, and applying secure patches in real time.

Key capabilities of Ana AI Autonomous Security Engineer include:

1. Automated Remediation – Generates and applies secure patches autonomously.
2. 80% Faster Remediation – Reduces vulnerability closure times from weeks to minutes.
3. 50% Fewer Breaches – Fixes vulnerabilities before they can be exploited.
4. 40–60% Developer Time Saved – Eliminates security-related bottlenecks in the development cycle.
5. Shift-Left Enablement – Embeds security early into development workflows without burdening developers.
6. Seamless Enterprise Integration – Supports integration with more than 30 leading security and development platforms.



ROI of 175% with AI powered Vulnerability Remediation



Reduce Security Vulnerability Remediation time by 70%

"Security has traditionally been at odds with developer velocity either slowing down releases or allowing vulnerabilities to slip through," said Arsh Anwar, Chief Technology Officer at OpenAna. "Ana AI changes that dynamic by automating security fixes without impeding development speed."

How Ana Works: Fully Autonomous Security Remediation
Ana AI integrates seamlessly with an enterprise's security stack to remediate risks across code, infrastructure, and cloud environments without manual intervention.

1. Seamless Integration with Security Platforms – Works across SAST, DAST, API security, infrastructure security, SBOM, and SCA solutions.
2. Intelligent Prioritization – Focuses remediation efforts based on exploitability, business impact, and compliance risks.
3. Automated Pull Requests and Patches – Autonomously generates validated code fixes and security pull requests.

4. Cloud Infrastructure Protection – Detects and fixes misconfigurations in AWS, Azure, and GCP environments.
5. Compliance-Ready Reporting – Supports compliance frameworks such as NIST, ISO 27001, SOC 2, and software supply chain security standards.

Importantly, Ana's autonomous security remediation is powered by the interplay of three specialized Autonomous Engineers:

Code Security Engineer – Focuses on remediating vulnerabilities in application codebases.
API Security Engineer – Detects and fixes vulnerabilities in APIs and service interfaces.
Infrastructure Security Engineer – Secures cloud and infrastructure environments by remediating misconfigurations and hardening deployments.

This multi-engineer collaboration enables a comprehensive and coordinated security remediation strategy across the modern enterprise attack surface.

"Ana ASE has a forward-looking and innovative roadmap that redefines how Agentic AI can transform enterprise cybersecurity and data privacy," said Rajiv Sondhi, CEO and Co-Founder of OpenAna.

Found by Your Existing Tools, Fixed by Ana
Ana AI enhances and extends the value of enterprises' existing security investments. Rather than replacing current security platforms, Ana integrates with and fixes vulnerabilities found by them.

OpenAna recently announced integrations with over 20 leading cybersecurity platforms, including Checkmarx, Invicti, and Tenable. These partnerships allow vulnerabilities identified by established tools such as static and dynamic code analyzers, vulnerability scanners, and cloud security platforms to be automatically fixed by Ana, closing the last critical gap in enterprise security operations.

Key supported integrations include:

SAST & DAST – Static and dynamic security testing.
SBOM & SCA – End-to-end software supply chain security.
API Security – Automated detection and remediation of API vulnerabilities.
Infrastructure Scanning – Fixes misconfigurations across cloud and on-premise environments.
Cloud Security – Automated hardening of AWS, Azure, and GCP deployments.
Enterprises can go live with Ana in days and realize ROI within weeks—an essential advantage in today's fast-moving threat environment.

The Future of Security: Autonomous, AI-Driven, and Always-On
The cyber threat landscape is evolving rapidly, and traditional manual remediation methods are

no longer sustainable. Enterprises adopting AI-driven, autonomous security remediation can achieve:

Faster Risk Reduction – Fixing vulnerabilities before attackers can exploit them.
Improved Compliance – Streamlined adherence to regulatory and security standards.
Operational Efficiency – Allowing security teams to focus on strategic priorities instead of manual patching.
Proactive Threat Defense – Transitioning from reactive response to proactive protection.

Ana AI Autonomous Security Engineer represents a critical shift towards a future where enterprises can defend their entire attack surface, from code to cloud, at machine speed.

About OpenAna
OpenAna is a U.S.-based pioneer in Agentic AI Platform of Autonomous Engineers for software development, cybersecurity, and DevOps/SRE. Through its breakthrough platform of Autonomous Engineers, OpenAna enables enterprises to adopt self-healing, autonomous systems that accelerate innovation, strengthen cybersecurity resilience, and drive operational excellence.

For media inquiries, please contact:
 hello@openana.ai
 www.openana.ai

Ana
OpenAna
hello@openana.ai
Visit us on social media:
LinkedIn
YouTube
Other
