The Rise of AI-Powered Security Orchestration

Uday Korlimarla | Sr. Technical Success Manager

snyk

Agenda

snyk

"A Ship in a harbour is safe but that is not ship are built for.

John A. Shedd – Salt in my Attic.

Uday Korlimarla

Sr. Technical Success Manager

+   +   +   +

snyk

Traditional DevSecOps Challenges

Silos

One common theme is silos resulting into communication gaps

Manual Processes

Manual processes for tasks like provisioning, deployment, and testing

Automation

Manual configuration and management become increasingly challenging as complexity increases

Visibility

Traditional DevOps setups may lack robust monitoring and visibility into the entire application stack

Security as an afterthought

Security is often addressed as an afterthought in traditional DevOps, rather than being integrated into the development process from the beginning. This can lead to vulnerabilities and security breaches.

snyk

The promise of AI

AI allows businesses to analyze vast amounts of data quickly and accurately.

Netflix use Unsupervised ML to understand customer preferences and behavior, enabling data-driven decisions on content recommendations, personalization, and pricing strategies.

Tesla uses AI to process data from sensors and cameras, informing real-time decisions for autonomous driving.

Tesla
Safer driving!

Netflix
Recommender systems

GPT-4
Content generation

snyk

AI-Powered Orchestration

1940-50

Birth of AI

Early AI research focuses on symbolic reasoning and logical inference

1960-70

Knowledge Representation

Dendral and MYCIN, are developed to mimic human expertise in specific domains.

1980-90

Neural Networks resurgence

Neural networks experience a resurgence with the development of backpropagation and improved training algorithms.

1990-2000's

Machine Learning & Support Vector Machines

Machine learning gains prominence, with algorithms like support vector machines and decision trees.

2010-2020

Deep learning

large neural networks and massive datasets, revolutionizes AI applications.
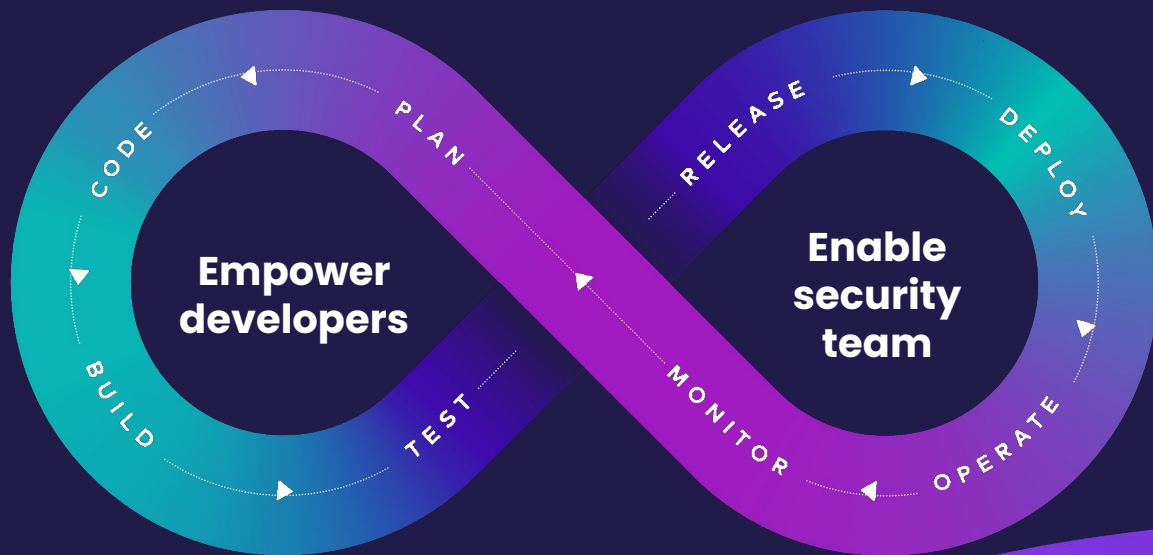
2020-xxxx

Beyond AI Advancements & Ethics

Ethical concerns related to AI bias, privacy, and job displacement gain increasing attention and ongoing advancements including quantum computing for AI

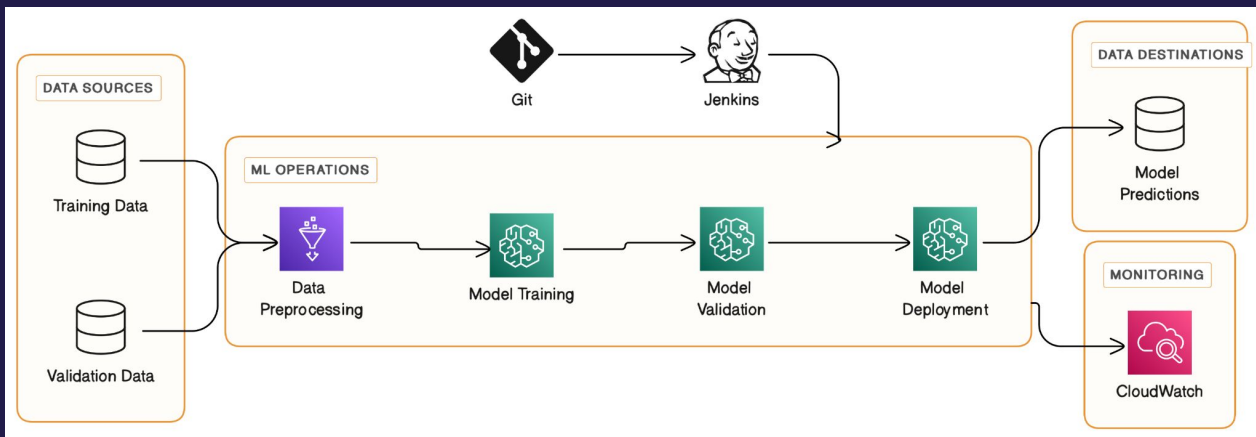Today, AI can be used to continuously monitor and analyse logs or events for threats or anomaly detection so that security can scale quickly

snyk

Traditional DevOps Process

Using AI to extend the reach of your security team with a developer-centric approach

snyk

AI-Driven Orchestration

Assist Developers

1 With remediation recommendations within the IDEs & Developer workflows.

Scale Operations

2 Enable operations to scale services

Posture management

3 Observe current posture and drive decisions based on data to enable remediation that reduces risk.
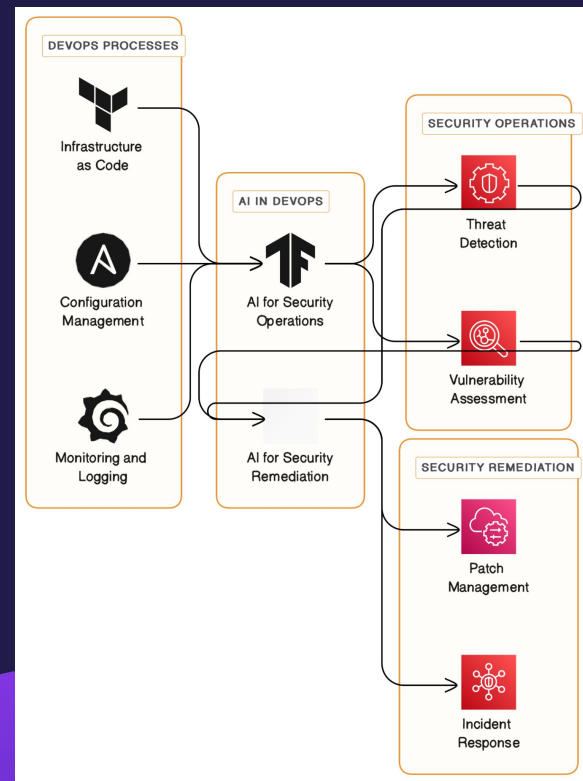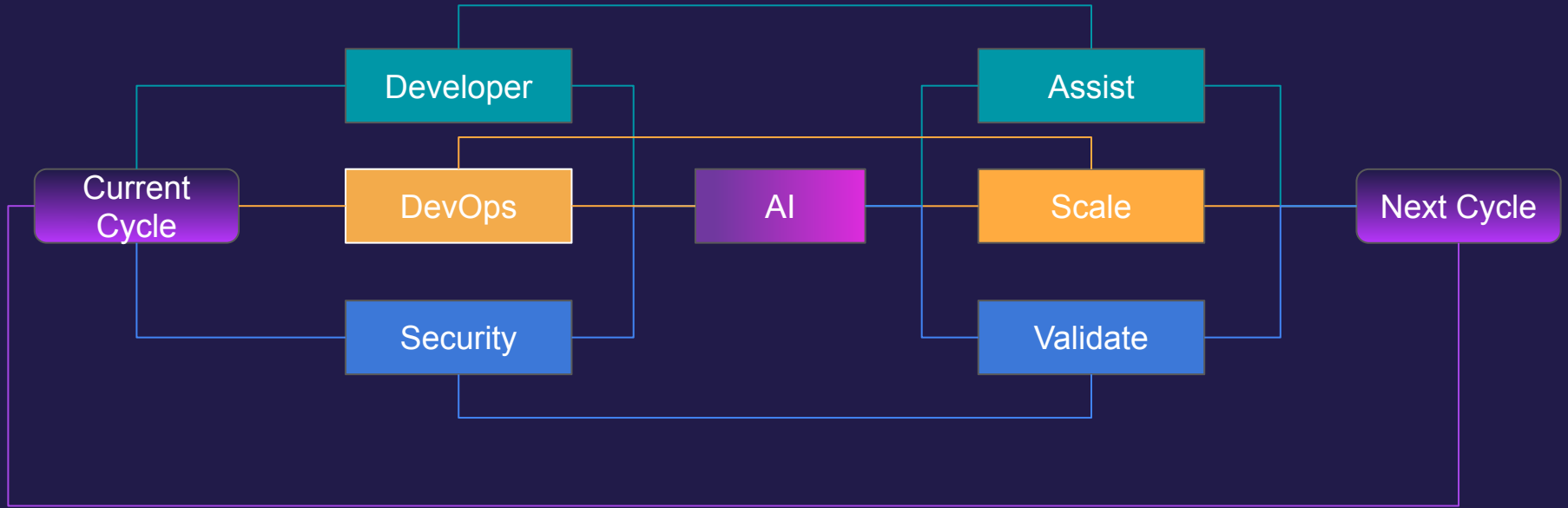
snyk

Instance: AI-Drive DevOps Process

Note:

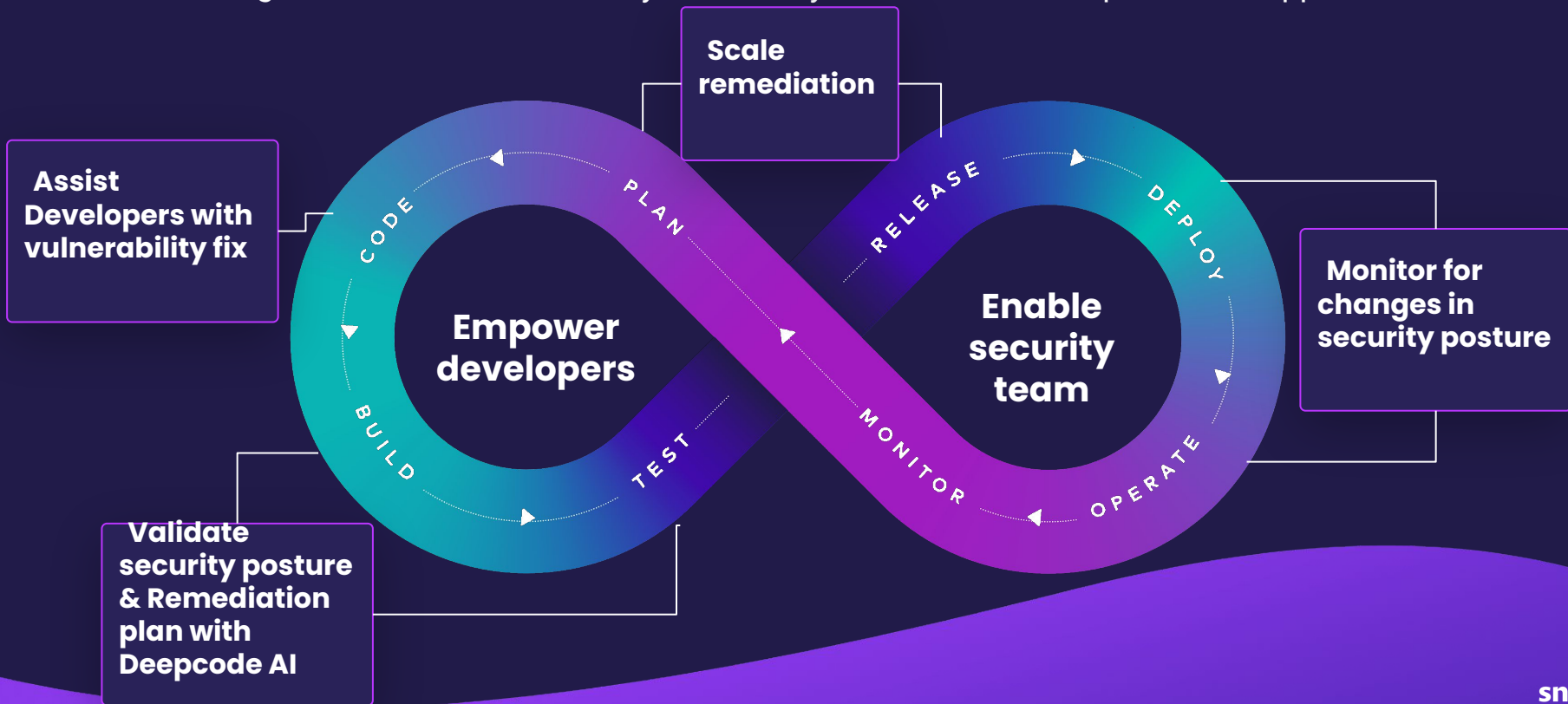This architecture diagrams here are generic depictions on how AI in DevOps processes can benefit organisations.

AI-Drive DevOps Process

Current Cycle → Developer / DevOps / Security → AI → Assist / Scale / Validate → Next Cycle

snyk

AI-Driven DevSecOps Process

Using AI to extend the reach of your security team with a developer-centric approach

Scale remediation

Assist Developers with vulnerability fix

Monitor for changes in security posture

Empower developers

Enable security team

CODE

PLAN

RELEASE

DEPLOY

BUILD

TEST

MONITOR

OPERATE

Validate security posture & Remediation plan with Deepcode AI

snyk

Closing Remarks

A Ship in a harbour is safe but that is not ships are built for.

Make use of AI best suited to meet your goals. AI is still evolving and is a double edged sword. Malicious actors can use the same technology to cause harm or naive usage results into privacy issues

TIME saved   **COSTS** reduced   **Competitive** advantage

snyk

Thank you for tuning in!

Please meet us at our booth to learn more about Snyk's journey with AI, Deep Learning & Neural networks

snyk