Synechron cyber ai

Synechron CyberAI

Enhancing Cybersecurity with AI: Proactive threat detection and secure AI governance

AI for Security

- Develop AI models for rapid detection of complex cyber threats.
- Create GenAI frameworks for dynamic incident response and mitigation.
- Enhance cybersecurity capabilities with AI-enabled security posture.

Security for AI

- Identify threats and model vulnerabilities in the GenAI lifecycle.
- Implement measures to safeguard sensitive data and prevent breaches.
- Establish robust AI governance and adopt a secure-by-design approach.

Synechron

Accelerator Overview

AI-Powered innovation across risk management, application security, incident resolution, and the GenAI lifecycle

RiskControl.AI

Empowering risk management with AI automation

- A cutting-edge IT risk platform that ensures compliance, detects deviations, and identifies control deficiencies.
- Leverages AI for threat modelling, security control mapping, and advanced risk simulations to automate risk management

AppSec.AI

Transforming application security with integrated insights

- A comprehensive application security solution that integrates multiple tools for a unified view of vulnerabilities.
- Leveraging AI, it reduces false positives, deduplicates vulnerabilities, and creates a prioritized vulnerability overview with financial risk scores.

Resolve.AI

Optimizing incident response with AI intelligence

- Advanced incident analysis and proactive resolution through incident categorization and tracking mechanisms.
- Utilizing AI, it enhances system reliability and provides predictive insights including change impact analysis, anomaly resolution, and capacity planning.

Validate.AI

Securing & monitoring Gen AI across the lifecycle

- Integrates security controls, model monitoring, and governance across the AI model and application lifecycle.
- Offers AI guardrails including detecting prompt injection, data and privacy leakage, and insecure output handling with real-time AI moderation.

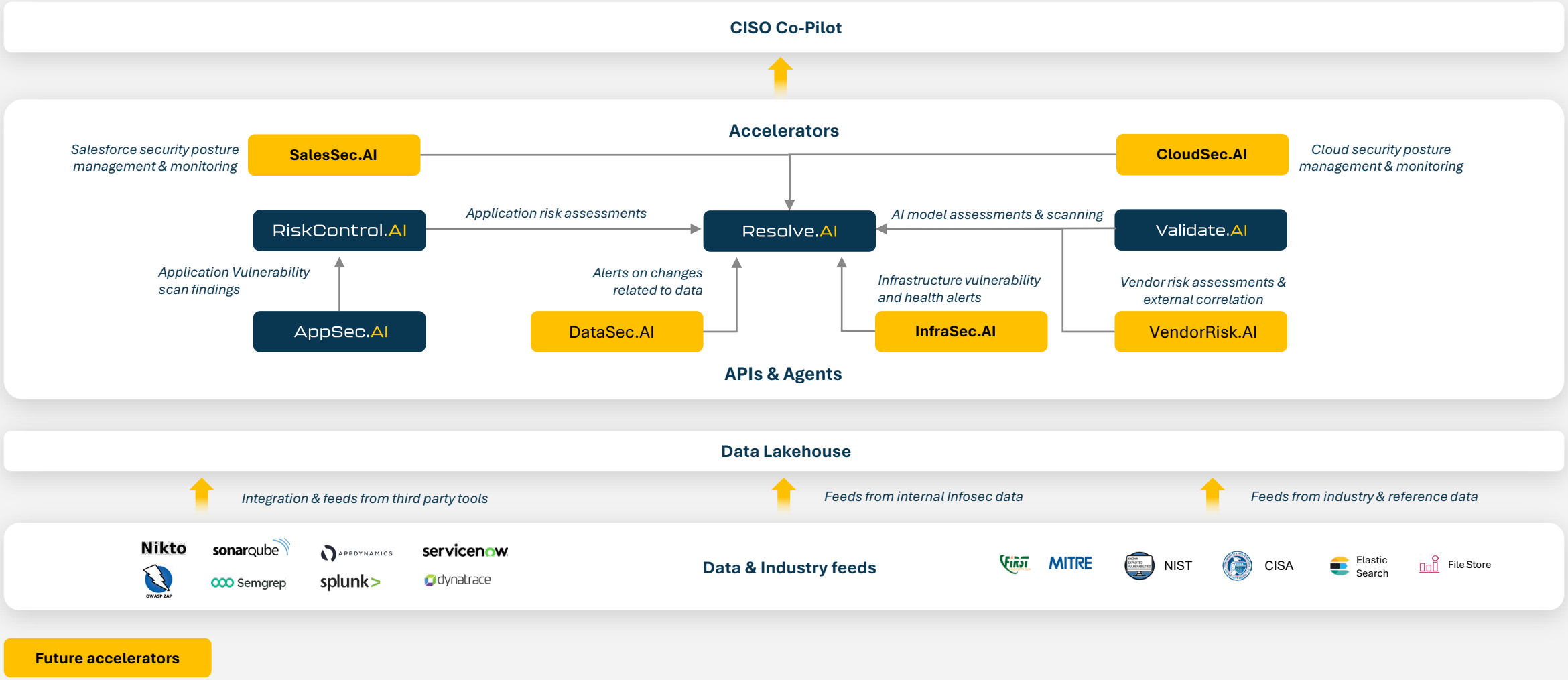
AI FOR SECURITY

SECURITY FOR AI

Synechron

Cyber^{AI} Platform

Our unified security platform vision: Enhancing risk Management and operational resilience



RiskControl.AI

Transforming cybersecurity through integrated AI-driven risk management

Synechron

Challenge

Enterprises struggle with vulnerability management due to a fragmented landscape of tools, leading to operational inefficiencies and increased risks.

Inefficient data management and manual processes hinder effective risk assessment, creating blind spots and complicating cybersecurity strategies.

The overwhelming complexity results in high signal-to-noise ratios, making informed investment decisions for remediation increasingly challenging.

Solution

The solution features an integrated IT Control and Risk Platform that ensures compliance with control frameworks while identifying deviations and non-compliance.

It supports custom risk calculation algorithms, prioritizing risks based on key controls like identity and third-party assessments for automated reporting.

GenAI enhances threat modelling, facilitating continuous control testing, and enabling risk simulations to conduct "what-if" scenarios.

Benefits

The platform improves IT risk management by integrating multi-source data, enabling continuous control monitoring, automated assessments, and actionable insights.

An improved second line of defence focuses on better vulnerability prioritization and compliance with regulatory frameworks.

GenAI strengthens threat modelling and scenario testing, providing flexible risk simulations that enhance compliance and resilience against evolving cyber threats.

AppSec.AI

Transforming application security through intelligent AI-powered vulnerability management

Synechron

Challenge

Organizations struggle to identify and manage vulnerabilities across their application landscape due to escalating cybersecurity threats.

Traditional DAST and SAST tools generate overlapping results and false positives, causing inefficiencies and increased manual workload for security teams.

This complexity hinders timely remediation of critical vulnerabilities, elevates the risk of security breaches and can lead to financial and reputational damage.

Solution

The solution integrates vulnerability data from multiple DAST and SAST tools, offering a comprehensive scanning mechanism for applications.

By normalizing scanning outputs, it creates a unified and prioritized vulnerability management dashboard, enhancing efficiency.

AI deduplicates vulnerabilities, minimizes false positives, and generates insights with financial risk scores, streamlining the reporting process.

Benefits

The solution drives improved efficiency through automated deduplication and false positive reduction, significantly reducing manual effort.

The integrated visualization and prioritization of vulnerability findings fosters quicker decision-making enhancing overall security management.

Integration with GRC tools ensures collaboration across security teams, leading to stronger application security and compliance with industry standards.

Resolve.AI

Synechron

Revolutionizing incident management through predictive analytics and proactive maintenance

Challenge

Modern enterprises face challenges in error analysis, prolonged downtime, and increased security risks due to an expanding application landscape.

There's a critical need for efficient production support to manage application errors and security incidents in real time.

Identifying issues for incidents complicates root cause analysis, hindering system health maintenance and timely incident resolution.

Solution

The solution analyses change requests and incidents to categorize issues and offer predictive analytics for proactive incident management.

Key features include error analysis insights, health index dashboard, change impact analysis, and anomaly detection for predictive maintenance.

Leveraging historical data and real-time insights, the accelerator enhances decision-making and incident response with conversational AI support.

Benefits

Improved efficiency in incident management, reduced downtime and application risk, and enhanced decision-making capabilities.

Categorizing errors based on frequency and providing actionable insights enables faster issue resolution for organizations.

The AI assistant streamlines support, while health index assessments optimizes resource allocation and enhances system reliability.

Validate.AI

Synechron

Fortifying Generative AI through comprehensive security integration and resilient applications

Challenge

The use of GenAI models and applications can lead to potential risks and vulnerabilities, complicating deployment of models into production.

Risks include prompt injection, training data poisoning, and disclosure sensitive data, potentially causing breaches, IP theft, and reputational damage.

Lack of robust AI security measures to address these vulnerabilities effectively exposes organizations to cyberattacks and operational disruptions.

Solution

The solution integrates advanced security controls and protocols directly into GenAI models and applications across the development lifecycle.

It includes implementing AI safeguards against prompt injection, ensuring secure output handling, and protecting against data and privacy leakage.

Combining open-source frameworks, custom models, and advanced monitoring techniques, our solution embeds security for AI measures to identify vulnerabilities.

Benefits

Implementing GenAI guardrails enhances data protection, reduces the likelihood of breaches, and fosters user trust.

Organizations can safeguard sensitive information while maintaining compliance with data privacy and AI usage regulations and policies.

A proactive security approach minimizes the risk of reputational damage and financial loss, leading to more resilient AI applications and increased adoption

Synechron

Thank You