activestate

Center of Excellence

ActiveState's Vulnerability Management as a Service uniquely combines Application Security Posture Management (ASPM) and Intelligent Remediation capabilities with expert guidance. This solution enables companies to not only identify vulnerabilities in open source packages, but also to automatically prioritize, remediate, and deploy fixes into production without breaking changes, ensuring that applications are truly secured.

Our expert guidance is delivered by the ActiveState Center of Excellence (CoE). It focuses on ensuring that your open source software is secure, compliant, and effectively integrated into your workflows. We offer tailored services to meet unique vulnerability management & remediation challenges.

Implementation Process

Discoverability and Observability: Monitor open source usage and vulnerabilities.

Continuous Open Source Integration: Detect and remediate vulnerabilities at every stage.

Secure Environment Management: Create consistent environments across the SDLC.

Governance and Policy Management: Enforce open source governance policies.

Regulatory Compliance: Meet GDPR, HIPAA, and other regulatory standards.

End-of-Life Support: Transition to new versions or alternatives as needed.

Key Use Cases

An ActiveState expert guides the implementation:

Discover and monitor:
Connect to the ActiveState platform.

Analyze:
Establish risk profile and generate reports.

Upgrade and curate:
Create an open source catalog and establish governance.

Build and deploy:
Access customizable and SLSA-compliant build infrastructure.

Training and Enablement

Set a training plan:
Align training with specific needs.

Role-based onboarding:
Provide role-specific training.

Ongoing certification:
Offer self-paced or assisted certification.

Assessment and Growth

Document ROI and business impact:
Measure KPIs and document ROI.

Prioritize additional high ROI use cases:
Focus on high priority projects.

Adopt best practices:
Share knowledge from other customers.

The ActiveState CoE team brings its nearly 30 years of experience in securing open source in the enterprise to act as an extension of a company's DevSecOps team and to ensure a successful implementation. This ensures end-to-end vulnerability management from discovery and prioritization through remediation and deployment.

A key function of the COE is to provide unmatched visibility into your entire open source software supply chain. Utilizing ActiveState's extensive database of over 40 million open source artifacts and 20+ years of build expertise, the COE helps map your application's complete dependency graph, including hidden transitive dependencies often missed by traditional SCA tools.

This deep insight enables the COE to offer best practices and support for Intelligent Remediation, complementing ActiveState's platform in identifying, prioritizing, and deploying fixes at scale, ultimately reducing the burden on development and DevOps teams.

activestate

www.activestate.com | solutions@activestate.com