opentext™

OpenText Aviator

Use case scenarios: Security/SOC

Security/SOC scenarios

Intuitive threat detection

I’m a cybersecurity analyst detecting threats before they do major damage. AI spots threat signals that we humans miss. I can now expose threats faster and act with confidence using AI-powered detection and analysis.

Let’s go

Software compliance checks

I’m a compliance officer spotting real risks in new software before they cause real trouble. With AI in my corner, I can catch sneaky vulnerabilities, squash compliance issues, and keep development moving—without playing guess-the-guideline.

Let’s go

Team collaboration for secure fixes

I’m a compliance officer spotting risks and helping Devs fix them fast. With AI bringing everyone to the same page—literally—we cut the drama, share what matters, and turn vulnerability fixes into a team win.

Let’s go

Security/ SOC made simple

Why it's hard today

- SOC teams are overwhelmed by false positives and alert fatigue
- Hard to detect subtle internal threats before damage is done across siloed systems
- Developers miss critical issues that surface late in the SDLC
- Manual and reactive compliance efforts instead of proactive continuous assurance
- Difficult to enforce DLP without disrupting productivity

Powered by OpenText

- **OpenText™ Application Security Aviator™**
- **OpenText™ Core Threat Detection and Response**

Wins for everyone

- **Security/SOC teams:** Spot risks early and potential threats faster with AI insights.
- **Developers:** Deliver secure code faster with AI-driven testing and fixes.

The big payoffs

Detect threats early

Uncover subtle and emerging risks with AI-powered insight that sees what rules-based tools miss.

Respond before damage is done

Cut response times from days to minutes—to shut down threats fast and stay ahead of impact.

Streamline compliance reviews

Make audits faster and cleaner with explainable AI that tracks, logs, and justifies every decision.

Let's get started...

Threat detection and response
Uncovers real threats faster and automate incident triage.

Insider threat monitoring
Identifies unusual behaviors, access patterns, or data exfiltration indicators in real time.

Code security and vulnerability management
Proactively scans and ranks code vulnerabilities by business impact.

Compliance and audit readiness
Automates evidence gathering and reporting to maintain compliance with security frameworks (e.g., NIST, ISO, SOC 2).

Data loss prevention (DLP)
Lags suspicious file access, transfers, and sharing behavior before data leaves the enterprise.

Spot threat signals that humans miss

I'm a cybersecurity analyst detecting threats before they do damage.

1 Spot stealthy threats

A user or system behaves unusually—maybe slow, subtle, or insider-driven.

Action: OpenText flags the behavior, integrated with Microsoft Defender or Entra ID.

Impact: AI uncovers hidden risk patterns too subtle for rules-based tools.

2 Summarize risk, instantly

AI pulls context-rich summaries tied to high-risk entities.

Action: OpenText generates a plain-language breakdown of risky actions mapped to MITRE ATT&CK.

Impact: Threat hunters know what happened—and why—at a glance.

4 Drill into what matters

Cybersecurity teams select specific events to understand risk drivers.

Action: OpenText adds insight around key moments, helping prioritize the right response.

Impact: Reduce time to understand the threat. No wasted cycles.

5 Shut it down fast

With context in hand, the team acts decisively.

Impact: What used to take days now takes hours, maybe minutes. Contain the threat before damage is done.

See it in action!

Expose threats faster and act with confidence using AI detection and analysis

Unlock the possibilities:

- **Spot suspicious behavior** and stop attacks before they spread.
- **Decrease mean time to detect** and shut it down faster than ever.
- **Decrease false positives**—fewer distractions means better focus on true threats.

Identify vulnerabilities in public-facing apps

I’m a compliance officer surfacing and remediating real vulnerabilities.

1 Spot a red flag

A routine application scan uncovers a critical SQL injection vulnerability in an online shopping app.

Action: OpenText sends a results summary and flags the issue as “Critical with Remediation Required.”

Impact: I get alerted to high-risk issues without digging through reports.

2 Zero in on what matters

I review the results and see dozens of issues. OpenText highlights the most urgent and suppresses the rest.

Action: OpenText categorizes 32 critical, 20 high, and 1 low-severity issue and auto-suppresses known non-issues.

Impact: I’m not overwhelmed by noise—I can prioritize and assign quickly.

3 Follow the thread

I click into a flagged issue to learn more. OpenText Aviator shows history, AI analysis, and risk status.

Action: OpenText provides a detailed rationale for marking an issue as “Not an Issue.”

Impact: I have full visibility and can verify audit trails with confidence.

4 Validate the finding

After review, I confirm the finding is a false positive. Aviator updates the status automatically.

Action: OpenText changes status and logs the reason with a complete explanation.

Impact: One less issue to chase. One more step toward a clean audit.

5 Close the loop confidently

Security and dev teams resolve real issues while I track audit status in real time.

Impact: Risk is reduced; compliance is maintained, and I stay ahead of the next review.

6 Audit like a pro

OpenText helps compliance officers identify real vulnerabilities, cut false positives, and reduce risk—without slowing down audits or development.

See it in action!

Confidently manage risk and compliance with explainable AI at your side

Unlock the possibilities:

- **Higher audit pass rates** thanks to cleaner reports and fewer false alarms.
- **Fewer post-deployment patches** by catching risks before they reach production.
- **Shorter audit time** with faster validations and AI-supported documentation.

Fix security flaws with compliance and dev in sync

I’m a compliance officer flagging risks and guiding developers to remediation.

1 Flag the issue

A routine scan reveals a critical SQL injection vulnerability in an online shopping app. The compliance officer alerts the dev team.

Action: OpenText Aviator sends an issue summary and recommends immediate review.

Impact: Risk is identified and routed fast—no delay, no confusion.

2 Let’s dig in

The developer opens “My Open Issues” to find the flagged vulnerability and dives into the code.

Action: Aviator helps analyze the source code and identify the root cause of the issue.

Impact: Developers don’t waste time guessing—go straight to the problem.

3 Call in backup

The developer checks the history tab for Aviator’s summary and fix guidance.

Action: Aviator automatically provides recommendations and code- level changes needed.

Impact: Compliance gets clarity, developers get direction.

4 Patch it up

Using Aviator’s guidance, the developer fixes the code. The next scan will verify resolution.

Impact: The issue gets resolved quickly, with AI as a shared guide between security, dev, and compliance.

5 Drive proactive response

The collaboration between dev and compliance—with help from Aviator—keeps the app secure and audit-ready.

Impact: Faster fixes, fewer compliance gaps, and a stronger security posture.

See it in action!

Bridge compliance and code

Unlock the possibilities:

- **Reduce friction** between dev and compliance teams with shared visibility and AI summaries.
- **Detect and fix** vulnerabilities faster
- **Address flagged issues** with clear compliance context.

opentext™

Limitless