AVIATION MRO SECURITY · PRIVILEGED IDENTITY MONITORING · M/XDR (Managed Extended Detection & Response)

From Disconnected Silos to Airworthiness Governance:

Securing Privileged Access in Aircraft Maintenance Operations Software (AMOS) Environments

How Banyax transforms fragmented AMOS access monitoring into a board-ready security governance program with measurable Key Risk Indicator (KRI) reduction, automated audit trails, and structural retention in aviation clients.

INDUSTRY Aviation / Maintenance, Repair & Overhaul (MRO)

01 · WHAT CLIENTS ACHIEVE

Four measurable outcomes before reviewing any technical architecture.

Detection Speed	False Positives	AMOS Coverage	Audit Trail
<20 min	**–80%**	**100%**	**Auto**
vs. no defined baseline — not previously in security scope	*via next-gen User and Entity Behavior Analytics (UEBA) + AI correlation*	*all modules monitored, 24×7×365*	*forensic evidence, zero manual effort*

Before Banyax, detecting unauthorized access, user creation, or rights modifications in AMOS required coordinating across three disconnected departments — Infrastructure, Account Administration, and the Chief Information Security Officer (CISO) office. Correlation was manual and slow. There was no behavioral baseline, no consolidated visibility, and no board-level governance over internal access risk in maintenance operations.

After Banyax, the CISO accesses a single consolidated view of 12 critical event types — from failed logins and disabled accounts to Privileged Access Management (PAM) bypass and unauthorized user creation — as KRI trends reported quarterly to the Operations Director and Audit Committee. Forensic evidence is generated automatically for any regulatory inspection. The organization doesn't just detect faster. It governs.

02 · THE PROBLEM NO ONE WAS SOLVING

AMOS is the operational core of any MRO organization. A single unauthorized modification to a work order, user role, or airworthiness record can trigger regulatory action — yet most airlines treat AMOS as outside the security perimeter.

Three silos, zero correlation

User permission changes, login patterns, and master data modifications in AMOS live across Infrastructure, Account Administration, and the CISO office. No control correlates them. A coordinated unauthorized access spanning all three stays invisible inside each one.

The authorized user gap

The highest-risk vector is the user with legitimate credentials acting outside their normal pattern. Static controls cannot distinguish a routine modification from premeditated internal collusion in work orders, user creation, or access rights changes inside AMOS.

No evidence when regulators ask

When an incident surfaces weeks later the CISO has no consolidated, tamper-proof record of what changed in AMOS, who approved it, and what the operational context was. Forensic reconstruction is manual and incomplete when the General Directorate of Civil Aviation (DGAC), the European Union Aviation Safety Agency (EASA), or the Federal Aviation Administration (FAA) request it.

Consequences: Air Operator Certificate (AOC) suspension, regulatory fines, and loss of MRO contracts.

03 · THREE CORRELATED USE CASES — ONE GOVERNANCE PROGRAM

Detection with real MRO operational context, not static rules. Banyax's Security Operations Center (SOC) operates all three use cases in a correlated fashion through Banyax Quest, our proprietary platform. AI-led: AI processes the volume, human analysts validate every escalation.

UC1 Privileged User Activity & Access Rights Monitoring

Banyax establishes a behavioral baseline for user creation, role assignment, and rights modifications across AMOS. Any user created with elevated permissions, any access rights change outside standard operational hours, or any modification executed by a non-administrator generates an anomaly score — not a static alert. Banyax Quest cross-references the executor's role, the affected user's change history, and whether a formal ticket exists in the helpdesk system.

AI-led role: *Continuous anomaly scoring across all user and rights events in AMOS at speed and coverage no manual audit cadence can match. Reduces incident rate by up to 90% within the first 90 days of baseline deployment.*

U C 2 Failed Authentication & Anomalous Login Pattern Detection

All failed authentication events — wrong password, user not found, disabled account — are correlated against the user's historical pattern, originating host, time of day, and frequency. The use case distinguishes human error from brute-force attacks and automated access attempts using stale credentials, generating a consolidated case per user — not one alert per event.

AI-led role: *Real-time correlation across authentication events that individually appear routine but together signal a coordinated access attempt. Target Key Performance Indicator (KPI): 90% reduction in undetected authentication anomalies, with immediate visibility when any login attempt occurs.*

U C 3 PAM Bypass Detection — Direct Privileged Access Outside Authorized Channel

The engine monitors whether privileged users access AMOS directly rather than through the authorized PAM channel. It detects both deliberate control evasion and misconfigured access paths, and correlates direct access events with any subsequent master data modifications or rights changes. Each cluster of suspicious access activity is presented as a single consolidated risk case.

AI-led role: *100% visibility into privileged direct access events. PAM channel evasion rate detected in real time — the only use case with zero tolerance threshold, given the regulatory implications of uncontrolled privileged access in an MRO environment.*

0 4 · H O W T H E S E R V I C E O P E R A T E S

From capture to audit-ready evidence package in five steps, all orchestrated through Banyax Quest.

1	**Capture** Application Programming Interface (API) connector / log extraction from AMOS platform.
2	**Ingest** 12 normalized behaviors ingested: logins, passwords, users, permissions, PAM access, emails, reactivations.
3	**UEBA Correlation** Behavioral baseline × role × schedule × history — correlated through Banyax Quest.
4	**Alert** Risk scoring → prioritized queue → KRIs reported to CISO and Audit Committee.
5	**Response** Forensic evidence package → Incident Responder → Containment → DGAC / EASA / FAA ready.

0 5 · W H Y B A N Y A X — T H E S T R U C T U R A L M O A T

Four differentiators that create governance dependency, not contract dependency.

■ Behavioral baseline advantage.

The value is not in the ruleset — it's in 90+ days of accumulated normal behavior per user, per role, and per AMOS module. During the ramp-up window without an active behavioral layer, organizations operate blind — the same period when 68% of undetected internal access incidents historically occur.

■ Managed governance service, not a compliance checklist.

The client buys outcomes: qualified alerts, contained access exposure, quarterly KRI reports for the Audit Committee, and evidence packages ready for DGAC, EASA, or FAA inspection. No internal team required to operate the detection layer.

■ Aviation-context detection, not a generic access rules engine.

Most access controls in AMOS are threshold-based and role-agnostic. Banyax correlates identity, approval history, maintenance schedule, and event sequence through Banyax Quest. The signal reflects the real operational context of an MRO — shift changes, AOC-critical windows, and third-party technician access patterns.

■ Structural retention through regulatory dependency.

Quarterly reporting to the Operations Director and Audit Committee integrates Banyax into the organization's governance structure. The relationship shifts from vendor-to-IT to program-to-board. Regulatory pressure from DGAC, EASA, and FAA makes this dependency structural, not contractual.

08 · LEARN MORE & CONTACT

Learn more about Banyax M/XDR (Managed Extended Detection & Response)

Discover how Banyax's Managed Extended Detection & Response (M/XDR) service continuously reduces cyber exposure with AI-led detection and board-ready KRI governance.

Visit: banyax.com

Want to learn more?

Reach out to explore how Banyax can help reduce cyber exposure in your organization.

Email: marketing@banyax.com

Website: banyax.com