Air France-KLM Stakeholder Outreach

Microsoft Security Engagement | Email Sequences for Key Decision Makers

RECOMMENDED OUTREACH SEQUENCE

Multi-threaded engagement targeting both Paris and Amsterdam decision-makers simultaneously.

1	2	3	4
DAY 1	DAY 1	DAY 3	DAY 5
Chucky Tam	Barbara Duinker	Muriel Lavodrama	Pierre-Olivier Bandet

EMAIL 1: SECURITY OPERATIONS LEAD

Chucky Tam
Director, Security Operations • Netherlands

HIGH PRIORITY

To: chucky.tam@airfranceklm.com
Subject: NIS2 Compliance & Unified Security Operations for Air France-KLM

Hi Chucky,

I lead Microsoft Security partnerships with European aviation leaders navigating **NIS2 compliance and security modernization**. Given Air France-KLM's critical infrastructure designation and the evolving threat landscape facing global carriers, I wanted to reach out directly.

We've been helping airlines address three challenges I suspect are on your radar:

- **NIS2's 24-hour incident reporting** — automated detection-to-notification workflows that meet Article 23 requirements
- **Unified visibility across subsidiaries** — single SOC view across Air France, KLM, and Transavia operations
- **M365 security consolidation** — leveraging your existing Microsoft investment for integrated threat protection

Given your role leading security operations, I'd value 20 minutes to share how **Lufthansa Group and IAG** have approached these same challenges with Microsoft Sentinel and Defender XDR.

Would Thursday or Friday this week work for a brief call?

Best regards,
[Your Name]
Microsoft Security | Aviation & Transportation

STRATEGY NOTES

Approach: Lead with NIS2 compliance (operational urgency) rather than breach reference. Position as peer conversation with aviation security expertise. Reference competitor airlines to create social proof. **Goal:** Technical discovery call to understand current security posture and SIEM/EDR gaps.

EMAIL 2: CIO OFFICE (NETHERLANDS)

Barbara Duinker
VP CIO Office • The Hague, Netherlands

HIGH PRIORITY

To: barbara.duinker@airfranceklm.com
Subject: Security Consolidation Opportunity for Air France-KLM's Microsoft Environment

Dear Barbara,

I'm reaching out regarding **security portfolio optimization** for Air France-KLM's Microsoft 365 environment. Our teams have identified significant consolidation opportunities for organizations with mature M365 deployments like yours.

Specifically, we're seeing European enterprises achieve **25-35% security TCO reduction** by integrating Microsoft Security capabilities they're already entitled to through existing licensing, including:

- **Identity consolidation** — Entra ID Premium replacing fragmented IAM tools
- **Native endpoint protection** — Defender for Endpoint integrated with M365
- **Cloud-native SIEM** — Sentinel with pre-built M365 connectors

Given the CIO Office's role in technology strategy and vendor evaluation, I'd welcome the opportunity to present a **complimentary Microsoft Secure Score assessment** that maps your current security posture against industry benchmarks.

Would you be open to a 30-minute briefing on the consolidation potential?

Kind regards,
[Your Name]
Microsoft Security | Enterprise Accounts

STRATEGY NOTES

Approach: Lead with cost optimization and licensing value — speaks to CIO Office priorities. Position as strategic vendor conversation, not tactical security sale. **Goal:** Secure executive briefing to present consolidation business case and establish Microsoft as strategic security partner.

EMAIL 3: CIO CHIEF OF STAFF (PARIS)

Muriel Lavodrama
Chief of Staff to Group CIO • Paris, France

MEDIUM PRIORITY

To: muriel.lavodrama@airfranceklm.com
Subject: Microsoft Executive Briefing Request — Air France-KLM Security Partnership

Dear Muriel,

I'm reaching out to request your guidance on the appropriate channel to discuss **Microsoft's security partnership** with Air France-KLM at the executive level.

We've been working with aviation leaders across Europe on **NIS2-compliant security architectures**, and given your group's digital transformation initiatives, I believe there's strategic alignment worth exploring.

Specifically, we'd like to offer:

- **Executive Security Briefing** — Microsoft's aviation security reference architecture and NIS2 compliance framework
- **Secure Score Assessment** — Complimentary analysis of Air France-KLM's security posture with peer benchmarking
- **Strategic Roadmap Session** — Alignment between your security priorities and Microsoft's innovation roadmap

I understand you support Pierre-Olivier Bandet's office on IT transformation initiatives. Could you advise on the best path to arrange an executive discussion?

With appreciation,
[Your Name]
Microsoft Security | Aviation & Transportation

STRATEGY NOTES

Approach: Respect the gatekeeper role — ask for guidance rather than demanding CIO access. Position as relationship-building, not transactional. Reference transformation initiatives to show awareness of strategic context. **Goal:** Secure warm introduction to CIO or confirmation of appropriate engagement path.

EMAIL 4: GROUP CIO (EXECUTIVE SPONSOR)

Pierre-Olivier Bandet
Group EVP & CIO • Paris, France

EXECUTIVE OUTREACH

To: pierre-olivier.bandet@airfranceklm.com
Subject: Microsoft + Air France-KLM: Multi-Cloud Security Partnership

Dear Pierre-Olivier,

Congratulations on the strategic cloud transformation partnership announced in December — it's an ambitious vision for Air France-KLM's data infrastructure.

As you execute this multi-cloud strategy, I wanted to introduce **Microsoft Security's role as the unified security layer** that protects workloads across Azure, AWS, and Google Cloud environments. We've designed our security portfolio specifically for organizations like yours that operate across multiple cloud platforms.

European aviation leaders are prioritizing three security imperatives:

- **NIS2 compliance** — Automated incident detection and 24-hour reporting capabilities
- **Multi-cloud security posture** — Unified visibility regardless of cloud provider
- **AI-powered security operations** — Security Copilot for accelerated threat response

I'd welcome the opportunity to arrange an **executive briefing with our Aviation Industry team** to discuss how Microsoft Security can complement your cloud transformation while addressing regulatory requirements.

Would your office have availability for a strategic discussion in the coming weeks?

Respectfully,
[Your Name]
Microsoft Security | Aviation & Transportation

CC: [Microsoft Account Executive], [Microsoft Aviation Industry Lead]

STRATEGY NOTES

Approach: Lead with acknowledgment of Google Cloud partnership — shows awareness and positions Microsoft Security as complementary, not competitive to cloud choice. Focus on multi-cloud positioning. **Goal:** Executive-level sponsorship for security evaluation. CC Microsoft aviation industry leadership for credibility. **Timing:** Send after Barbara/Muriel engagement to create bottom-up momentum.

FOLLOW-UP CADENCE

Day 4 — No Response

LinkedIn connection request with personalized note referencing email. Keep it brief: "Hi [Name], sent a note about Microsoft Security for AF-KLM. Would welcome connecting."

Day 7 — Follow-Up Email

Brief follow-up with value-add: "Wanted to share this [NIS2 aviation brief / Sentinel case study] that may be relevant. Still happy to discuss when timing works."

Day 14 — Final Touch

Breakup email: "I'll assume the timing isn't right. If security priorities shift, I'm here. In the meantime, happy to stay connected for industry insights."