

# How Switzerland's FDFA Trains Smarter with Filigran's OpenBAS

The Crisis Management Center of the Swiss FDFA ensures the preparedness of its global network of representations through regular crisis exercises. To streamline simulations and reduce workload, it chose OpenBAS by Filigran, enhancing operational readiness across 170 global sites, including embassies and consulates.

**-80%**

Crisis preparation time cut

**+100%**

Growth in crisis training exercises in 6 months

**90%**

satisfaction rate among participants

## OVERVIEW



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

### INDUSTRY

Government agency

### PRODUCT USED



OpenBAS

### USE CASE

- Incident Response (IR) Optimization
- Automation & Scalability
- Threat Awareness
- Risk Analysis

## About FDFA

The Federal Department of Foreign Affairs (FDFA) manages Switzerland's foreign policy and diplomatic network, with over 170 embassies, consulates, and cooperation offices worldwide.

Its Crisis Management Center supports the prevention and coordination of responses to crises that may impact Swiss citizens, personnel, and infrastructures abroad.

**"Some teams came back to us saying, 'That was so easy! We'd like to run another one.' That showed us they were not just complying with the mandate, but really embracing the tool."**



Margaux Messerli, Crisis Manager at Swiss FDFA.

# Context

The FDFA's Crisis Management Center was facing growing operational pressure in an increasingly volatile global environment. The rising frequency of natural disasters, prolonged armed conflicts, and unpredictable security threats demanded **faster, more scalable training methods to conduct annual crisis exercises in the 170 Swiss representations.**

To maintain preparedness, each mission is expected to run annual crisis simulations. These exercises are tailored to local risk factors and can include, for example, scenarios of civil unrest ahead of presidential elections or severe weather events. The Swiss embassy in Paris, for instance, simulated a train accident and an incident on Olympic infrastructure in the lead-up to the 2024 Games, while Tokyo conducted a flood response exercise in preparation for Expo 2025 in Osaka.

As global threats become more frequent and complex, the FDFA must ensure both agility and consistency in its crisis response approach across all embassies and consulates. And for this reason, they were on a lookout for a crisis management tool to conduct situational awareness and table-top exercises.

## Challenges

### HIGH RESOURCE CONSUMPTION FOR EACH CRISIS EXERCISE

The preparation and implementation of a single crisis simulation could require up to **40 hours of work** for role-playing exercises. While responsibility for crisis management lies with each representation, the Crisis Management Center provides direct assistance to them. Manual scenario design, injection management, and logistics left little room for coaching and strategic guidance.

By providing a tool that facilitates access to crisis exercises and reduces the resources required, the Crisis Management Center fully fulfills its mandate and frees up time for other tasks within its mandate.

*"We were losing focus on our real added value because we were spending so much time organizing the exercise itself,"* explains Margaux Messerli, Crisis Manager at Swiss FDFA.

### UNEVEN PREPAREDNESS ACROSS REPRESENTATIONS

While all Swiss representations are required to organize a crisis management exercise once a year, their level of maturity in crisis management varies considerably. **Some had very little experience in crisis management** and needed direct support to plan or carry out a simulation. **Others were more confronted with real cases due to the context.** This disparity complicated the task of the FDFA, which had to ensure that all locations were equally prepared to respond effectively.

### NEED FOR GREATER REALISM AND SCALABILITY

Paper-based scenarios and manual injections limited the operational intensity of the training exercises. As threats evolved and crises became more frequent, **the FDFA needed a scalable solution that could simulate urgency** while being easy to deploy.

*"We wanted exercises that really felt like a crisis, where staff received emails and text messages just like in real life," says Margaux Messerli. "That realism was essential for us."*

### INCREASED EXPECTATIONS FOR COMMUNICATION IN A REAL-TIME WORLD

*"Twenty years ago, there wasn't the same urgency to communicate instantly. Today, the community expects updates right away, even when verified facts are scarce," explains Margaux Messerli. In the age of social media, **this demand for immediacy** adds to the challenge of crisis response, which must be both responsive and coordinated.*

### BUDGET CONSTRAINTS AND PRESSURE TO OPTIMIZE RESOURCES

As global crises multiply, **the FDFA must do more with less, without compromising quality**. Supporting the representations of the external network, particularly in their preparation for crisis management, remains a priority of the Crisis Management Center's mandate.

*"We're being asked to reduce the resources we invest, not only at headquarters but also in the field. If one person spends 40 hours on an exercise instead of two, that's 38 hours lost for other essential tasks," says Margaux Messerli.*

## Why did FDFA choose Filigran's OpenBAS?

OpenBAS is Filigran's Adversarial Exposure Validation (AEV) platform that enables organizations to simulate real-life attack scenarios based on technical, physical, and business risks. By leveraging prioritized threat intelligence, MITRE ATT&CK frameworks, and risk-based employee profiling, OpenBAS uncovers the most probable attack paths before they materialize. This proactive approach helps security teams strengthen defenses on both the technical and human fronts, ensuring continuous adaptation and resilience against evolving threats.

### SEAMLESS INTEGRATION INTO EXISTING WORKFLOWS

OpenBAS manages crisis exercises by sending injects via Outlook and SMS, channels already used in the FDFA's daily operations. **This avoids the need to introduce a new interface or train teams on an external platform**. The familiar format enhanced realism and helped staff respond instinctively, just as they would during a real event.

### FLEXIBLE LICENSING AND UNLIMITED USE

To scale crisis training across its entire diplomatic network, the FDFA needed a solution without licensing bottlenecks, at no additional cost. **OpenBAS offered unlimited users**, messages, and scenarios, enabling both local autonomy and centralized coordination. *"We needed complete freedom to create and duplicate exercises, with no restriction on participants,"* Margaux Messerli confirms.

## FAST ONBOARDING AND AUTONOMOUS SCENARIO MANAGEMENT

Thanks to its **intuitive design**, new facilitators were able to grasp the basics of OpenBAS in no time. The FDFA quickly moved from basic testing to full-scale use, including autonomous deployments by local teams. *“After only 30 minutes of explanation, most people understood how to use the platform,”* Margaux Messerli appreciates.

## A RESPONSIVE AND RELIABLE PARTNER

The FDFA has also found a strategic partner in Filigran. **The approachability of the support team**, always open to feedback, convinced the Crisis Management Center of the platform’s long-term relevance. Filigran’s European roots also aligned with public sector cybersecurity and sovereignty standards. *“We appreciated Filigran’s responsiveness and the fact that the platform continues to evolve. The flexibility offered by OpenBAS, which allows us to grow with the tool, has been a significant advantage for us,”* concludes Margaux Messerli.

# Adoption

The FDFA began testing OpenBAS in early 2023 as part of a one-year pilot. Implementation was quick and the platform’s intuitive interface required **minimal training**. The first exercise took place in February 2024, followed by a high-stakes simulation with the Swiss embassy in Paris ahead of the 2024 Olympic Games.

During the pilot, access to OpenBAS was limited to selected representations, which enabled the Crisis Management Center to closely monitor usage and iterate. **Filigran provided responsive support throughout.** *“We always got fast, clear answers from the Filigran team, even when our needs were a bit outside the usual scope,”* Margaux Messerli notes.

While a few bugs affected email injections early on, Filigran resolved them quickly, including one critical fix just hours before an exercise, as Margaux recalls: *“On the morning of the simulation, injects weren’t going through. Filigran’s team reconfigured everything by 6:30 a.m. and the exercise ran on time.”*

By mid-year, the FDFA allowed autonomous deployments. From July onward, teams began using OpenBAS with limited oversight. **The platform officially entered full deployment in April 2025.**

# How Filigran helps the FDFA

## BY DELIVERING MEASURABLE TIME SAVINGS

OpenBAS enabled the FDFA to **cut crisis exercise preparation time by 80%**. What used to require up to 40 hours now takes just 1 to 2 hours per representation, freeing up resources at both local and central levels. *“With OpenBAS, even inexperienced teams can prepare an exercise in a matter of hours instead of several days,”* says Margaux Messerli.

## BY MULTIPLYING TRAINING OPPORTUNITIES WORLDWIDE

**The FDFA doubled the number of crisis exercises** conducted over six months, allowing more teams to test their response plans and develop reflexes under pressure, without increasing the workload.



**“After only 30 minutes of explanation, most people understood how to use the platform”**

Margaux Messerli, Crisis Manager at Swiss FDFA.

## BY IMPROVING THE QUALITY AND DEPTH OF CRISIS COACHING

OpenBAS freed crisis managers from manually executing scenarios, and they can now focus on **supporting teams in decision-making, coordination, and communication** under pressure. This hands-on support during simulations helped reinforce best practices and improve the learning experience.

## BY FOSTERING A PROACTIVE SECURITY CULTURE

Using OpenBAS has truly changed mindsets within the FDFA. Representations that had completed their annual exercise began **requesting additional simulations on their own initiative**. This shift from obligation to commitment showed that the platform made training both accessible and relevant. *“Some teams came back to us saying, ‘That was so easy! We’d like to run another one.’ That showed us they were not just complying with the mandate, but really embracing the tool,”* explains Margaux Messerli.

## BY MODERNIZING OPERATIONS WITH A SCALABLE, TRUSTED PLATFORM

OpenBAS helped the FDFA align crisis training with its overall digital transformation strategy, which includes cybersecurity, sovereign technology, and agile public services. The platform’s open architecture and European-compliant workflows made it an ideal fit. Today, OpenBAS enables secure, decentralized coordination across 170+ missions without adding complexity.

# The Road Ahead

With the official rollout of OpenBAS across its entire global network, the FDFA is entering a new phase in its crisis readiness strategy. *“Representations can now simply fill out a form and receive their exercise configuration. There’s no need for direct coordination unless something goes wrong,”* explains Margaux Messerli.

Thus, the Crisis Management Center can scale its efforts efficiently while maintaining oversight.

Thanks to the valuable time saved, the team is also expanding its catalog of scenarios from two to eight autonomous templates by the end of the year, covering a broader range of risk levels and contexts. New exercises are being designed to involve several representations at the same time, which will promote inter-embassy collaboration during complex situations.

Looking ahead, the FDFA is exploring synergies with other federal departments, testing different scenario variables, and closely following Filigran’s roadmap on AI-powered injects and advanced dashboards.

## ABOUT FILIGRAN

Filigran, a cybertech company founded in 2022, offers open-source cybersecurity solutions covering end-to-end threat intelligence management, attack simulations, and security posture validation for organizations.

