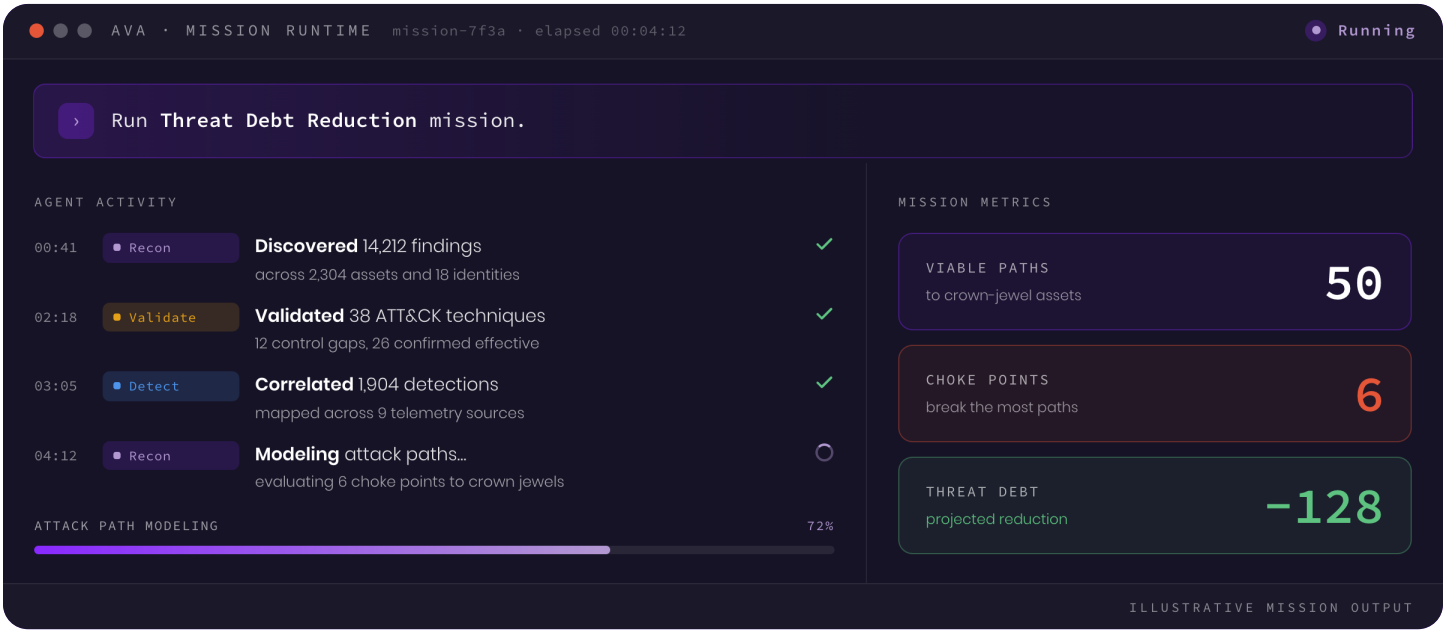
AttackIQ Professional Services

Forward Deployed Engineering

Forward Deployed Engineering embeds AttackIQ engineers directly inside your organization to turn a specific mission problem into a working, validated solution—built in your environment, against your real data and constraints, on the AVA Agentic OS. The Forward Deployed Engineer (FDE) Service pairs our engineers with your team until the outcome exists and runs on its own.

Engagements focus on a small number of high-value workflows, so working solutions land in weeks rather than months.



Build a Working Solution, Not Just a Deployment

We partner with you to solve a specific mission problem inside your own environment. Through the engagement, you will:

- Start from your organization's actual mission need, not a generic deployment checklist
- Build and validate a solution inside your environment, against your real data, systems, and constraints
- Prove the solution against the specific problem it was built to solve
- Take ownership of what was built, with your team able to operate and extend it independently

Program success requires a specific mission problem to solve, close collaboration between your team and ours, and a commitment to building, not just licensing, the solution.

Your Data, Your Controls

Forward Deployed Engineers work inside your environment, under your controls, governance, and data-handling requirements. Your mission data, detection logic, and threat intelligence remain yours — what we learn in your environment is never used in ways that erode your advantage.

Service Components

The Forward Deployed Engineer Service embeds AttackIQ engineers with your team to design, build, and validate a solution to a specific mission problem—from problem definition through handoff.

Where Engagements Focus

FDE engagements build on AVA Agentic OS's core missions, shaped to your priorities:

- **CTI-Driven Validation:** transform threat intelligence into validated defensive readiness.
- **Detection Coverage Analysis:** continuously discover what adversaries can do that your detections cannot.
- **Control & Defense Optimization:** continuously optimize security controls against real-world attack techniques.
- **Threat Debt Reduction:** pay down adversary opportunity by breaking attack paths.
- **AI Security Validation:** continuously discover AI risks and validate AI defenses.

Your mission challenge may sit squarely in one of these or cut across several.

Understand: Define the Mission Problem

Every engagement starts with your organization's actual mission need. Our engineers work with mission owners and technical leads to translate that need into clear requirements and success criteria for a working solution, prioritizing a small number of high-value workflows rather than trying to solve everything at once.

Build: Deliver Inside Your Environment

They design and build the solution on AVA Agentic OS directly inside your environment, against your real data, systems, and constraints, not in a lab or sandbox. Your team works alongside ours, so knowledge transfers as the solution takes shape.

Enable: Prove It, Then Hand It Off

Before the engagement ends, the solution is validated against the problem it was built to solve. Full capability is transferred to your team, who are left able to operate and extend it, without depending on AttackIQ to keep it running.

Customer Outcomes

Upon completion, you have:

1. A working, validated solution to a specific mission problem, running in your own environment
2. A solution built on AVA Agentic OS, using your real data, systems, and constraints
3. A team capable of operating and extending the solution without depending on AttackIQ
4. A build-alongside relationship that goes deeper than product licensing or traditional consulting

Throughout the engagement, you are paired with experienced engineers who build with you until the outcome exists and runs on its own.

Professional Services Expertise

Our engineers bring experience from government, intelligence, defense, and commercial cybersecurity environments, paired with deep platform fluency. AttackIQ is a founding Research Partner of MITRE's Center for Threat-Informed Defense, and our engineers apply that same threat-informed rigor to every engagement. Rather than deploying a generic playbook, our engineers build directly against your mission problem, applying proven delivery patterns while adapting to the data, systems, and constraints of your environment.

This is the same operator-led approach AttackIQ Professional Services brings to organizations advancing their security operations, focused here on one goal: a working solution that outlives the engagement.

Getting Started

To begin a Forward Deployed Engineering engagement, contact your AttackIQ account team.

ATTACKIQ

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ is the leader in threat-informed Continuous Threat Exposure Management (CTEM), helping organizations continuously validate defenses, break attack paths, and reduce threat debt through evidence-based security operations.

Through AVA Agentic OS, AttackIQ introduces the industry's first agentic operating system for CTEM, enabling organizations to execute it autonomously at scale. By orchestrating specialized AI agents across threat intelligence, security validation, detection engineering, control optimization, threat debt reduction, and AI security validation, AttackIQ transforms fragmented security activities into continuous cyber resilience.

Trusted by the world's largest enterprises, government agencies, and managed security providers, AttackIQ empowers organizations to continuously discover, validate, and reduce cyber risk with confidence.

CTEM Runs on AVA.