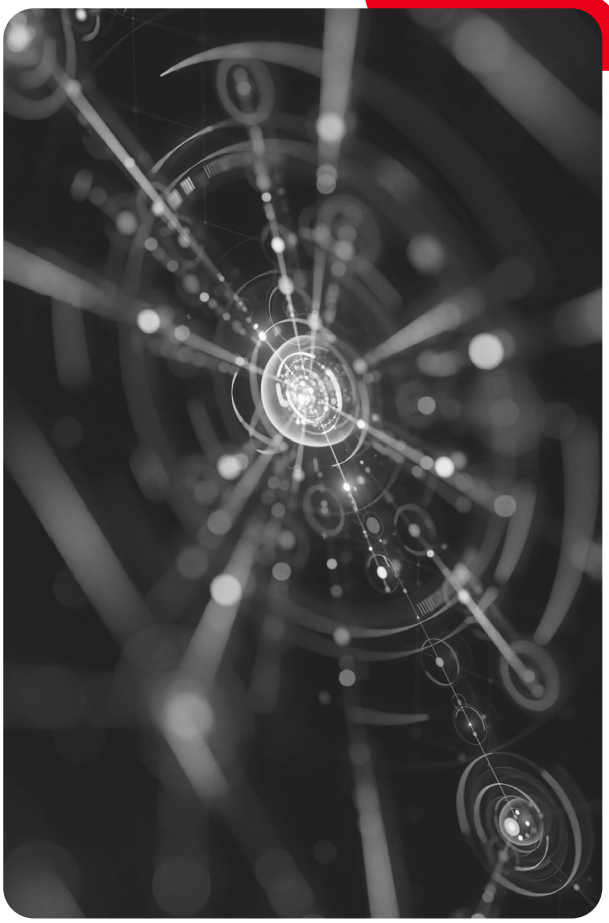
Autonomous Threat Operations

Services included with your Recorded Future subscription



Overview

Autonomous Threat Operations can transform how security teams operationalize threat intelligence. This shift requires a degree of collaboration from your team to establish integrations and connectors, ingest diverse sources, automate intelligence detections, and unlock the full potential of these capabilities.

To ensure your team's success, we're including expert services with your purchase of Autonomous Threat Operations. The primary goal of engaging with our team is to facilitate initial setup, identify and automate manual processes, consolidate your sources, and structure impactful reporting to showcase threat intelligence outcomes.

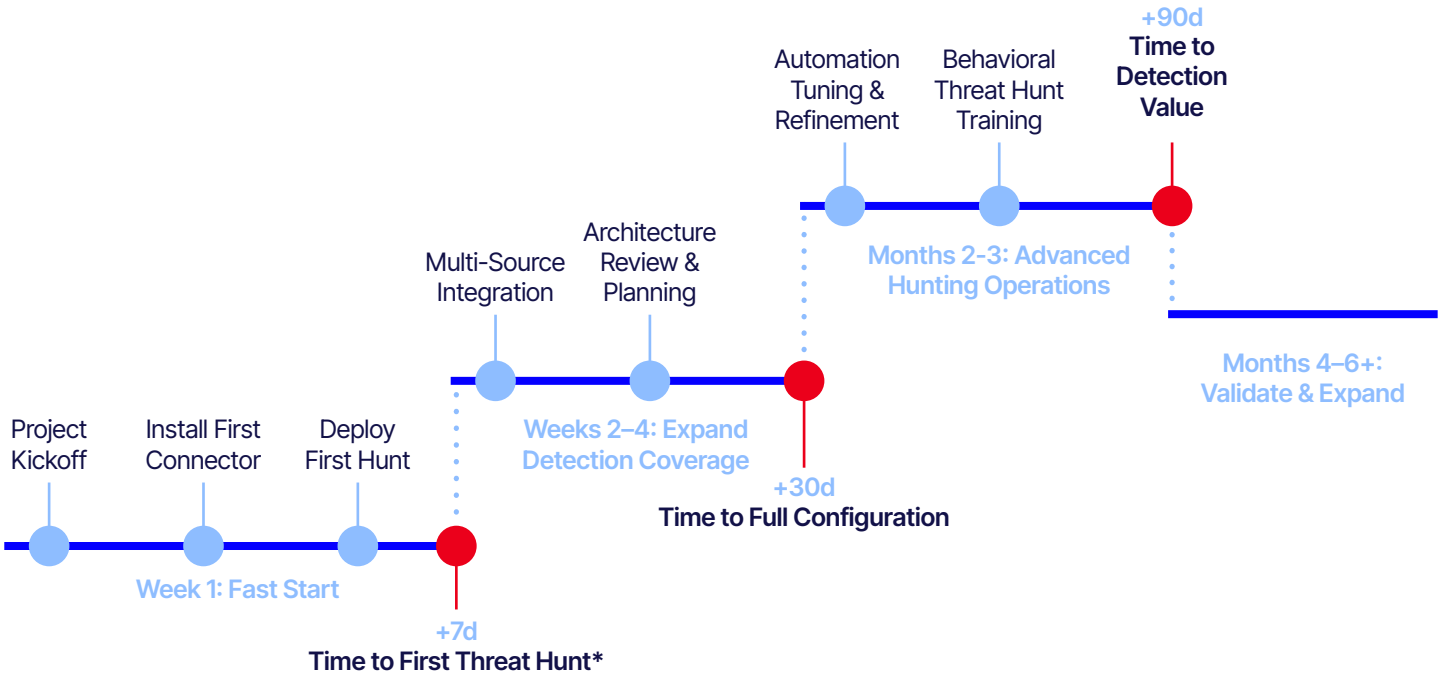
How Services Help You Achieve Autonomous Threat Operations

Achieve faster time to value.
No figuring it out on your own. We'll help you configure your first connector, set up threat hunts, and deploy automations in the first week.

Navigate integration complexity.
Your team works across a number of different tools, including EDR, SIEM, third-party, and internal feeds. We help you navigate the technical details of getting your tools connected and working correctly.

Save your team time.
Your analysts shouldn't spend weeks learning new tools. We can get them up to speed quickly with integration support and hands-on workshops.

We've designed a prescriptive services program. This path ensures that you're not just buying software—you're implementing lasting organizational change.



Week 1: Fast Start

Project Kickoff & Planning → Get a clear roadmap for which integrations to prioritize, and define success criteria.
Install First Connector → Get Professional Services support to ensure that connectors are properly configured.
Deploy First Hunt → Get your first autonomous/automatic threat hunt running.

Weeks 2–4: Expand Detection Coverage

Multi-Source Integration & Detect Deployment → Third-party feeds are ingested and automatically blocking threats in at least one security tool.
Architecture Review & Planning → Get a documented plan for how intelligence will flow between tools throughout your security stack.

Months 2–3: Advanced Hunting Operations

Automation Tuning & Refinement → Automation rules are tuned to reduce false positives and manual correlation time is essentially eliminated.
Behavioral Threat Hunt Training → Your analysts are trained on advanced hunting techniques, and they get templates optimized for your threat landscape.

Months 4–6+: Validate & Expand

Executive Reporting Workshop → Implement best practices for reporting value to leadership, regulators, and board-level executives.
Integration & Connector Review → Your environment is reviewed and updated to take advantage of new platform features and integration opportunities.
Threat-Led Penetration Testing Workshop → Your program is evolved beyond detection to proactive validation of your defenses against priority threats.

Flexible and tailored: While we recommend this path to success, we'll customize the program to meet your specific needs and priorities within the scope of the services included with your Autonomous Threat Operations subscription.

**** Approximate timeline based on customer availability***