ANOMALI

Competitive Intelligence
Threat Intelligence Platforms

Recorded Future

CrowdStrike Falcon Adversary Intelligence

PREPARED BY:
ERIN KENNEDY
MARCH 16, 2026

Executive Summary

Who This Is For

Account Executives, CSMs and SEs competing in TIP and CTI deals — especially against **Recorded Future** and **CrowdStrike Falcon Adversary Intelligence**.

How It Helps You Win

Know exactly where each competitor falls short, how to respond to common objections, and talking points to help you win.

The Bottom Line

Anomali is the only platform where TI, SIEM, SOAR, and XDR are built from one data lake — not disparate, piece-milled point products.

Market Context

Feed to Platform

TI has evolved from feeds to contextual, automated intelligence that integrates with SIEM, SOAR & EDR.

Consolidation Pressure

*Majority of enterprise security teams plan to and budget for consolidation of TI vendors. Buyers want fewer tools, not more.

Speed is the KPI

Dwell time and MTTR are board-level metrics. Buyers need platforms that reduce time-to-respond and a report to show the proof.

AI Hype vs. AI Value

Every vendor claims AI. Our buyers don't care about AI, they need automation that increases productivity and reduces risk, not wrappers on legacy products.

Security teams used to collect threat intelligence, but today they need to operationalize it. Instantly, at scale and across every tool in their stack.

*81% of enterprise security teams plan to consolidate TI vendors *(Recorded Future 2025 State of Threat Intelligence)*

Competitive Snapshot

Recorded Future	CrowdStrike Falcon Adversary Intelligence
Market leader by mindshare. Pure-play TI. Now part of Mastercard.	Endpoint-first platform. TI is a module inside the Falcon ecosystem.
✔ Strengths	✔ Strengths
• Strong brand recognition; Forrester leader, referenced by analysts • Broad coverage: identity, brand, 3rd party • Large TI dataset: +1M sources	• Intel driven by telemetry • Tight EDR-TI loop • Strong brand recognition from the EDR market leadership
✘ Where They Fall Short	✘ Where They Fall Short
• Lots of data, no action; no native SIEM, SOAR or detection • High cost per user/per module • Alert noise, info overload, complex	• TI is an upsell, not the core product • Complex licensing, expensive due to amount of SKUs required • Weak coverage; only using their endpoint data

Comparison Matrix

Value Buyers Care About	Anomali	Recorded Future	CrowdStrike Falcon Adversary Intelligence
Time to Value	Fast; cloud-native, fully integrated	Moderate; tuning required	Fast for EDR users, slow others
Operational Complexity	Low; one platform + one data lake	High; point solution, lots of integrations	High; multi-SKU platform required
Intelligence + SIEM	Native; built-in, same data	None - requires 3rd party	Limited; Falcon Next Gen only
Productivity Increase	Agentic AI automates triage and response	Strong intel with manual operationalization	EDR-focus; limited for SOC analysts
Scalability	15 years of historical intel, Petabyte-scale	Cloud-native, but increase cost with volume	Cloud-native but endpoint-focused
Deployment	Cloud, VM, on-prem	SaaS only	Cloud only

3 Messages That Win Deals

ANOMALI

1 vs. Recorded Future

ONE PLATFORM.
Recorded Future gives you intelligence, but you still need a SIEM, SOAR, and EDR to act on it. Anomali TI, SIEM, XDR, and SOAR are all built on the same data lake; **no disparate piece-milling, no maintenance, no data latency between tools.**

Proof point: Anomali customers reduce security costs by 50%+ by eliminating the need for separate TI feeds and the compute costs of legacy SIEMs

2 vs. CrowdStrike

INTEL YOU OWN.
CrowdStrike threat intelligence is powered by their endpoint telemetry, which means you need to be a Falcon customer to get value. **Anomali aggregates hundreds of intelligence sources and works with your existing stack.**

Proof point: 15 years of historical intel, flexible deployment; cloud, on-prem, or air-gapped

3 vs. Both

ACTION, NOT JUST ALERTS.
Both competitors generate intelligence. Anomali Agentic AI closes the loop by identifying threats, diagnosing root causes, and acting autonomously.

Proof point: Global airline compressed 3 hours of manual IOC collection into 3 hours, with clear next steps

ANOMALI

Common Objections

> "The time it takes to analyze a threat has gone down from 30 minutes to just a few minutes... There has been a substantial decrease in terms of meantime-to-know."
>
> — **Arindam Bose, SVP & Security Officer, Bank of Hope** (Gartner Peer Insights)

"We're a CrowdStrike shop. The intel is already in Falcon."

- Falcon's intel is great for endpoint context, but limited to Falcon telemetry
- *Our customers say Falcon can be 'overwhelming' and hard to 'take action' on
- Anomali aggregates 200+ sources
- **Works alongside Falcon, not against it**

"We already use Recorded Future. Why would we switch?"

- Intelligence alone doesn't close incidents
- Anomali can operationalize intelligence inside your SIEM and SOAR
- **Anomali can ingest Recorded Future feeds to augment, not replace**

"Everyone claims AI. What's actually different?"

- Anomali Copilot uses 70+ AI models and agentic capabilities
- **Not just a chat bot or generative AI, actually agentic and diagnosing root causes and initiating remediation**

*from actual Anomali customer quotes

Recommendations

Lean Into the Built-In House Narrative

No competitor can claim what Anomali can: a unified data lake built from the ground up, not assembled through acquisitions or integrations. Give sellers one line they can repeat in any deal: **'Every other platform is integrated. Ours is native.'** Reinforce it at every stage of the funnel.

Don’t Fuel the Competition’s Fire

Lead with buyer outcomes, not competitor comparisons. Sellers who open with 'we're better than Recorded Future' hand competitors a free mention and invite a feature war Anomali doesn't need to fight. The stronger play is to lead with the pain points (alert fatigue, integration overhead, cost) and how Anomali is the obvious answer.

More Customer Proof

Recorded Future and CrowdStrike both have deep case study libraries. Anomali proof points need to be equally specific and vertical-focused. A financial services CISO won't move on a generic 'enterprise customer' story. Prioritize 2-3 case studies with quantified outcomes (cost reduction %, MTTR improvement, analyst hours saved) in finance, public sector, and healthcare.

ANOMALI

Thank You!

PREPARED BY:
ERIN KENNEDY
MARCH 16, 2026