ANOMALI | PRODUCT MARKETING

Competitive Intelligence

Threat Intelligence Platforms

Recorded Future | CrowdStrike Falcon Intelligence

Prepared by: **Erin Kennedy** | Audience: Sales Team | March 2026

EXECUTIVE SUMMARY

What Sales Needs to Know

Who This Is For

Account Executives and SEs competing in TIP, CTI, and SecOps platform deals — especially against Recorded Future and CrowdStrike Falcon Intelligence.

How It Helps You Win

Know exactly where each competitor falls short, how to flip common objections, and the 3 talking points that land hardest when Anomali is in the deal.

The Bottom Line

Anomali is the only platform where TI, SIEM, SOAR, and XDR are built from the same data lake — not bolted together. That's a structural win, not a feature claim.

**Based on publicly available information — Gartner, PeerSpot, Forrester, and vendor documentation.*

MARKET CONTEXT

The TI Landscape in 30 Seconds

🎯 **Talk Track:**

"Security teams used to collect threat intelligence. Today they need to operationalize it — instantly, at scale, across every tool in their stack. Buyers are consolidating: 81% plan to reduce their number of TI vendors in the next 12 months."

From Feed to Platform

TI has evolved from raw IOC feeds to contextual, automated intelligence integrated with SIEM, SOAR & EDR.

Consolidation Pressure

81% of enterprise security teams plan to consolidate TI vendors. Buyers want fewer tools, not more.

Speed is the KPI

Dwell time and MTTR are board-level metrics. Buyers reward platforms that reduce detection-to-response time.

AI Hype ≠ AI Value

Every vendor claims AI. Buyers are demanding proof: automation that works, not wrappers on legacy pipelines.

COMPETITIVE SNAPSHOT

Know Your Competition

Recorded Future

Market leader by mindshare (~21%). Pure-play TI. Now part of Mastercard.

✔ STRENGTHS

- Largest TI dataset — 1M+ sources, Intelligence Graph with 200B+ nodes
- Strong brand recognition; Forrester leader, widely referenced by analysts
- Deep dark web & geopolitical intelligence; Insikt Group analyst content
- Broad module coverage: identity, brand, 3rd-party risk, payment fraud

✘ WHERE THEY FALL SHORT

- Intelligence without action — no native SIEM, SOAR, or detection engine
- High cost; per-user/per-module pricing adds up fast for full coverage
- Operationalization still requires manual effort and custom integrations
- User-reported: alert noise, information overload, complexity to tune

CrowdStrike Falcon Intel

Endpoint-first platform. TI is a module inside the Falcon ecosystem.

✔ STRENGTHS

- Telemetry-driven intel — trillions of events daily from deployed sensors
- Adversary profiles on 265+ named threat actors (e.g., Fancy Bear)
- Tight EDR-TI loop: intel auto-enriches endpoint detections in real time
- Cloud-native, easy deployment; strong brand from EDR market leadership

✘ WHERE THEY FALL SHORT

- TI is an upsell, not the core — requires full Falcon platform buy-in
- No native SIEM; log aggregation is limited vs. a true SecOps platform
- Expensive; licensing complex; many features require additional SKUs
- Weak coverage for non-endpoint data (cloud-only, on-prem environments)

COMPARISON VIEW

What Matters to Buyers

CAPABILITY	ANOMALI	RECORDED FUTURE	CROWDSTRIKE FALCON
Time to Value	✔ Fast – cloud-native, pre-integrated	△ Moderate – tuning required	△ Fast for EDR users; slow for others
Operational Complexity	✔ Low – one platform, one data lake	✘ High – point solution, many integrations	✘ High – platform lock-in required
Intel + SIEM Integration	✔ Native – built-in, same data layer	✘ None – requires 3rd-party SIEM	△ Limited – Falcon Next-Gen SIEM only
Analyst Productivity	✔ Agentic AI automates triage & response	△ Strong intel, manual operationalization	△ EDR-focused; limited for SOC analysts
Scalability / Cloud	✔ Petabyte-scale, 15yr historical intel	△ Cloud-native but volume cost escalates	△ Cloud-native but endpoint-centric scope
Flexible Deployment	✔ Cloud, VM, on-prem, air-gapped	✘ SaaS only	✘ Cloud-only

✔ Advantage △ Partial / Conditional ✘ Gap

SALES POSITIONING

3 Messages That Win Deals

01 One Platform. No Integration Tax.

vs. Recorded Future

Recorded Future gives you intelligence, but you still need a SIEM, SOAR, and EDR to act on it. Anomali's TI, SIEM, XDR, and SOAR are all built on the same data lake — no duct tape, no maintenance overhead, no data latency between tools.

Proof point: Anomali customers reduce security costs by 50%+ and improve detection by 88%.

02 Intel You Own — Not Intel You're Locked Into.

vs. CrowdStrike Falcon

CrowdStrike's threat intelligence is powered by their endpoint telemetry — which means you need to be a Falcon customer to get value. Anomali aggregates 200+ intelligence sources and works with your existing stack. You're not trading one lock-in for another.

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

03 AI That Acts, Not Just Alerts.

vs. Both

Both competitors generate intelligence. Anomali's Agentic AI closes the loop — it identifies threats, diagnoses root causes, and initiates response actions autonomously. Ask them: how many analyst hours does your TI platform save per week? We can answer that.

Proof point: 70+ AI models. Agentic Copilot. Automation with integrity — explainable, auditable.

OBJECTION HANDLING

Common Objections & Talk-Track Responses

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

Recorded Future is excellent intelligence — but intelligence alone doesn't close incidents. Anomali operationalizes that intelligence inside your SIEM and SOAR without replacing it. In fact, Anomali's marketplace can ingest Recorded Future feeds. You're not choosing — you're consolidating around a platform that can act on what RF delivers.

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

Falcon's intel is strong for endpoint context — but it's scope-limited to your Falcon telemetry. What about cloud workloads, insider threat, network-based IOCs, third-party risk? Anomali aggregates 200+ sources and works alongside Falcon, not against it. You're not limited to what CrowdStrike sensors see.

"Anomali is a TI company. Can it really replace our SIEM?" Platform Story

This is the repositioning question — and it's fair. Anomali was built as a TI platform by the founder of ArcSight, the original SIEM. The reason he built something new is because SIEMs weren't designed around intelligence. Anomali's data lake is — and it handles petabyte-scale log ingestion with 15 years of hot storage at a fraction of Splunk's cost.

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

Ask every competitor this: 'How does your AI take action, not just surface alerts?' Anomali's Copilot uses 70+ AI models and agentic capabilities — it doesn't just flag a threat, it diagnoses the root cause and can initiate remediation. We're careful about what we claim, which is why we can back it up with customer outcomes.

RECOMMENDATIONS

How to Sharpen the Competitive Edge

Build a Displacement Playbook

Create a dedicated battle card and landing page for each competitor — private, not public. Sellers need a fast-read, deal-specific asset that maps Anomali's strengths to the specific gaps in the prospect's current tool. The RF card and the CS card should feel different because the buyer and the objections are different.

Anchor on the 'Built-In-House' Story

Neither RF nor CrowdStrike can say what Anomali says: every capability was built on the same data lake, from the same codebase. That's not a feature — it's a structural advantage. Give sellers a one-liner they can repeat: "Every other platform is integrated. Ours is native." Reinforce this at every stage of the funnel.

Arm Sellers With Customer Proof

The 50% cost reduction and 88% detection improvement stats are powerful — but they need industry-specific versions. A financial services CISO needs a financial services story. Prioritize 2-3 case studies in key verticals (finance, public sector, healthcare) that sellers can drop into competitive deals with named outcomes.

Questions? Let's dig in.