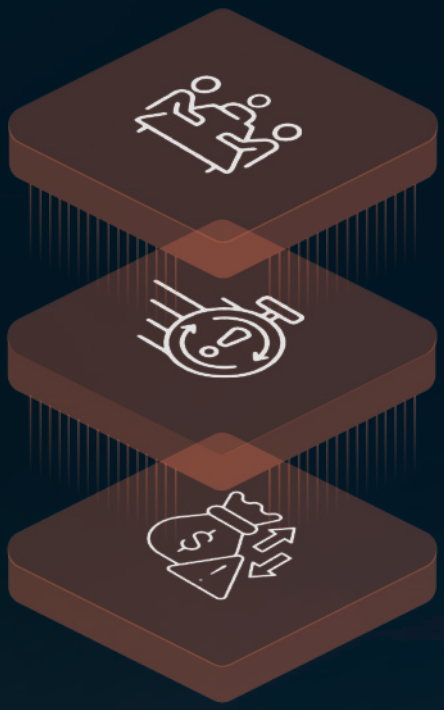
Modern MSSP Services Powered by ThreatConnect:

Deliver High-Margin, Differentiated Offerings That Reduce MTTR and Prove Value



Your Customers Don't Want More Alerts.

Your customers are drowning in alerts. Their SIEMs are noisy. Their tickets are piling up. And they're tired of being told that "more data" is the answer.

It's not, and your margins can't take the hit from all that waste.

What they need - and what they'll pay for - is a partner who can help them make sense of it all. A partner who doesn't just forward alerts, but provides real insight:

What's happening?	Why does it matter?	What should we do about it?

In a market where **95% of organizations fall short** of response time best practices [Source: CrowdStrike Global Security Attitude Survey], MSSPs who reduce MTTR win - and retain - more customers.

If you're delivering copy-paste detections, you'll be replaced by the next MSSP with a flashier dashboard and a cheaper price.

But if you're delivering context, prioritization, and action - the things that actually drive down risk and response time - you're not just a vendor. You're indispensable.

ThreatConnect helps MSSPs deliver what customers actually want:

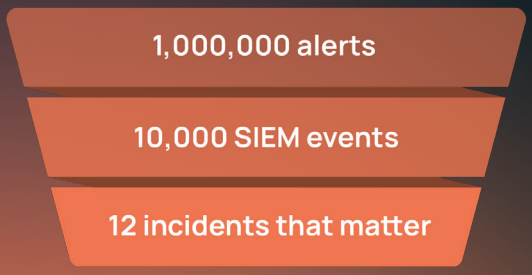
insight, not noise.

From Alert Pipeline to Value Partner

84% of security analysts say they are concerned about missing out on threats or incidents because of the number of alerts and data they're faced with. [Mandiant - Global Perspectives on Threat Intelligence]

84% report feeling burned out [1Password]

The average cost of a breach is $4.88 million in 2024, a 10% increase from prior years.
[IBM Cost of Data Breach Report]



Top

Middle

Bottom

The MSSP that gets to the bottom faster wins.

Core MSSP Services Powered by

At a Glance

Service	What It Is	Key Benefit
Threat-Informed Response	Embedded context in every alert	Lower MTTR, smarter triage
TI-Informed Detections	Curated feeds for each customer	Fewer false positives
Threat Management Enablement	Self-service intel access	Collaboration without cost
Domain Monitoring	Automated phishing defense	High-margin add-on
Vulnerability Prioritization	Actionable vuln context	Defensible remediation focus
Supplier Threat Monitoring	Visibility into third-party exposure	Early warning without access
RFI Enablement	Structured intel intake	Faster answers, less overhead
Advisory & Hunt	Proactive, strategic services	Revenue + retention

The ThreatConnect MSSP Impact Model

Each service is built around three questions:

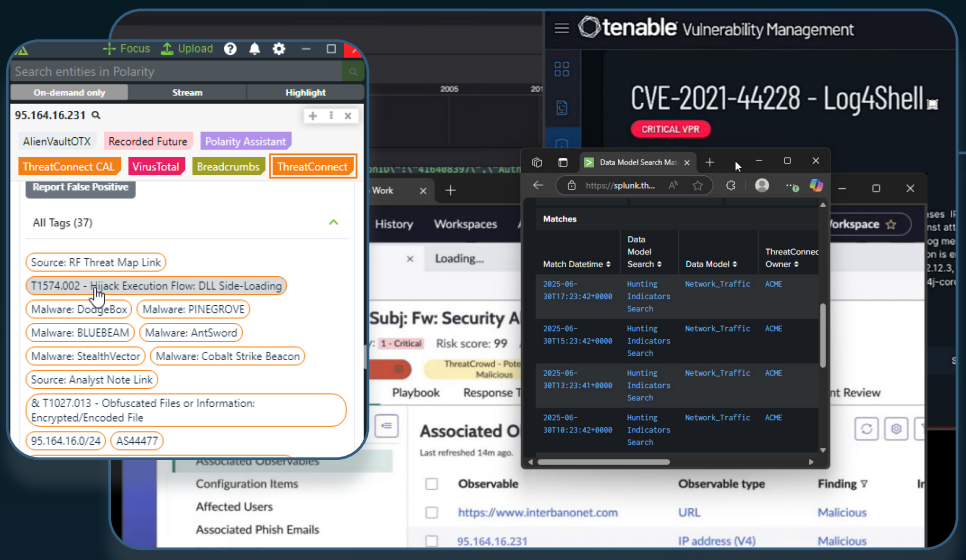
What's costing you time or trust?

What does ThreatConnect enable you to do?

What measurable outcome do you deliver to customers?

Let's walk through each of the services listed in the table above.

Threat-Informed Response



Traditionally, alerts pop up without meaningful context, and require complex integrations or multiple tools to triage.ThreatConnect provides high fidelity enrichment in whatever tool your analysts are using.

Your Struggles

Your analysts aren't just overloaded - they're overwhelmed. Customers expect answers, but your team is stuck playing whack-a-mole with alerts.

- **62% of SOC alerts are disregarded** [Source: Vectra, Global Perspectives on Threat Intelligence]
- **55% of teams say they've missed critical alerts due to ineffective prioritization** [Source: Mandiant, Global Perspectives on Threat Intelligence]
- **84% of cybersecurity professionals are worried about missing real threats due to alert volume** [Source: CrowdStrike Global Security Attitude Survey]

Burnout rises. SLA misses stack up. And your customers start questioning the value you bring.

Our Service

ThreatConnect embeds threat intelligence directly into the alert workflow - so your analysts don't have to guess.

When your team triages an alert, they instantly see:

- Who the threat actor is
- What TTPs are in play
- Whether it's been seen before - in your environment or across the global intel networ

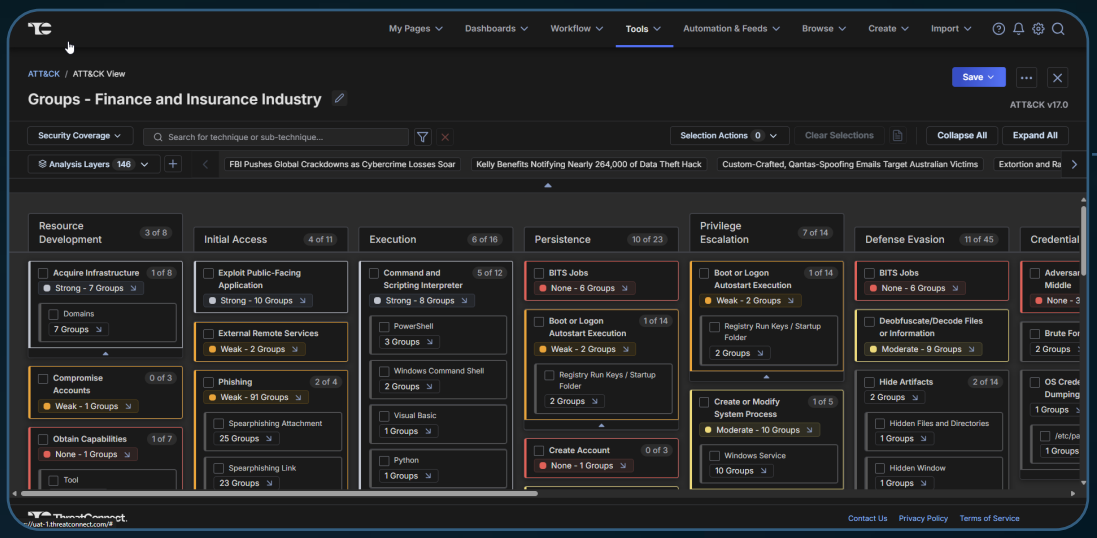
This happens right inside your existing tools - SIEM, EDR, ticketing, even email. No tab-switching. No context lost.

It's not just faster. It's smarter.

Your Outcomes

- **Lower MTTR:** Clear, contextual decisions lower MTTR and reduce analyst time - protecting your margins while improving results.
- **Smarter Escalation:** Context enables confident, defensible decisions - on the spot
- **Stronger Client Trust:** Show your value with clear, contextual answers your customers understand.

Threat Intelligence-Informed Detections



ATT&CK-based insights align to your industry vertical and help you understand your strengths, gaps, and risks.

Your Struggles

You're sending alerts, but your customers are still asking: "Why are we paying for this?"

- **Too many detections turn out to be noise**
- **SIEM dashboards don't tell a compelling story**
- **Off-the-shelf intel feeds generate more questions than answers**

Worse, when you try to fine-tune detections, you're working blind - without context about what really threatens each customer.

Our Service

ThreatConnect lets you deliver intelligence-informed detections that actually make sense.

Feed each customer's SIEM with curated, **risk-weighted** indicators tailored to their environment, industry, and threat profile. That means:

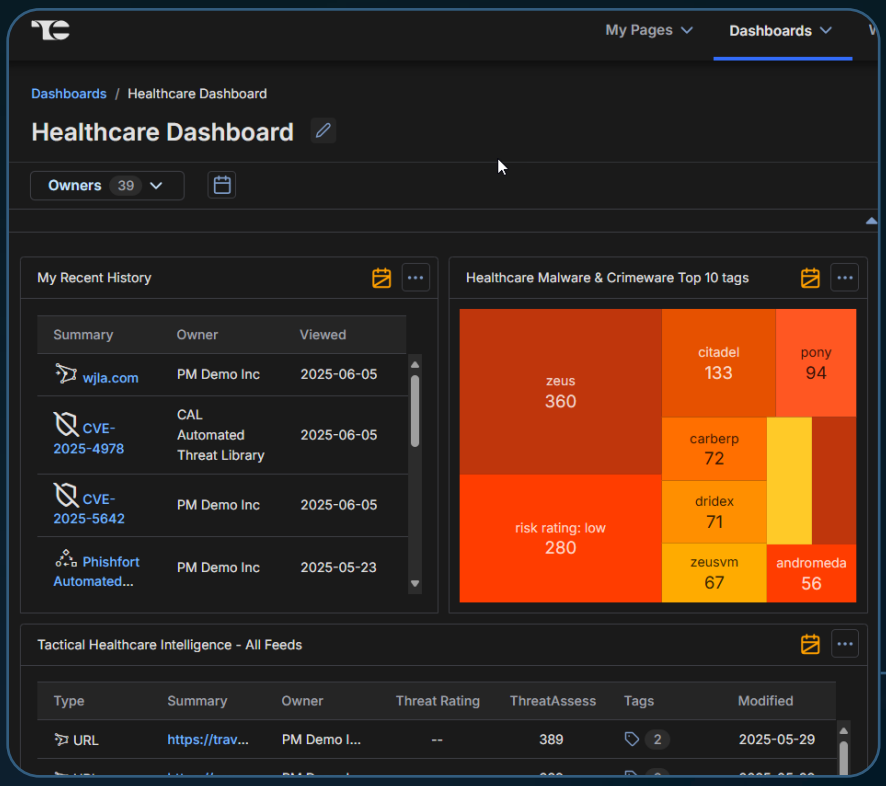
- Fewer irrelevant alerts
- Better fidelity on what gets flagged
- Clear rationale for every detection you push downstream

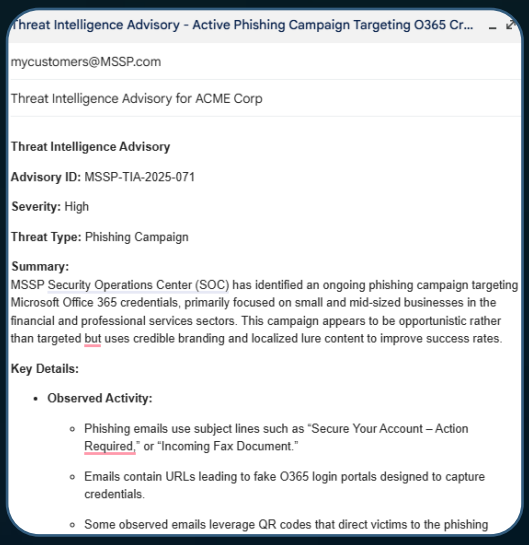
With ThreatConnect, you're not just adding IOCs to a feed. You're aligning detection strategy to actual risk.

Your Outcomes

- **Fewer False Positives**
  48% of teams say more than 40% of alerts are false positives [Source: CrowdStrike Global Security Attitude Survey]
- **Proactive Wins for QBRs**
  Demonstrate that you flagged an attack campaign targeting their industry - before impact
- **Higher SIEM ROI**
  Make the most of their investment by showing real signal over noise

Threat Management Enablement





Traditional means of exchanging intelligence can mean critical insights disappear into the ether. ThreatConnect provides bespoke dashboards with key insights: a single source of truth.

Your Struggles

Customers want transparency - but giving it to them is messy.

- They ask for more intel access, but you can't expose internal tools
- They want to collaborate, but email chains and PDF reports don't scale
- Every custom request chips away at your margins

You're stuck between control and customer satisfaction.

Our Service

ThreatConnect gives your customers their own secure intelligence workspace - no heavy lift required.

Each customer gets access to a private ThreatConnect Org where they can:

- Investigate threat actors and campaigns
- Enrich indicators using the same intel you trust
- Submit structured RFIs - without clogging your analysts' inboxes

No new infrastructure. No risk of exposing backend tools. Just a better experience for both sides.

Your Outcomes

- **Shared Context = Stronger Partnership** Customers see what you see - no need to repackage it manually
- **No Extra Headcount or Custom Builds** ThreatConnect handles the heavy lifting so your team doesn't have to
- **Modern Experience That Scales** Move beyond static reports to a collaborative, on-demand model customers love

Domain Monitoring

ThreatConnect offers multiple tools for staying on top of expensive, damaging business impacts.

Your Struggles

Brand protection is one of your customers' biggest blind spots - and one of your biggest opportunities.

- They're not monitoring for spoofed domains or impersonation
- Most providers only detect phishing after it hits the inbox
- Running manual checks doesn't scale across dozens (or hundreds) of clients

Our Service

ThreatConnect automates domain-based threat monitoring across your customer base.

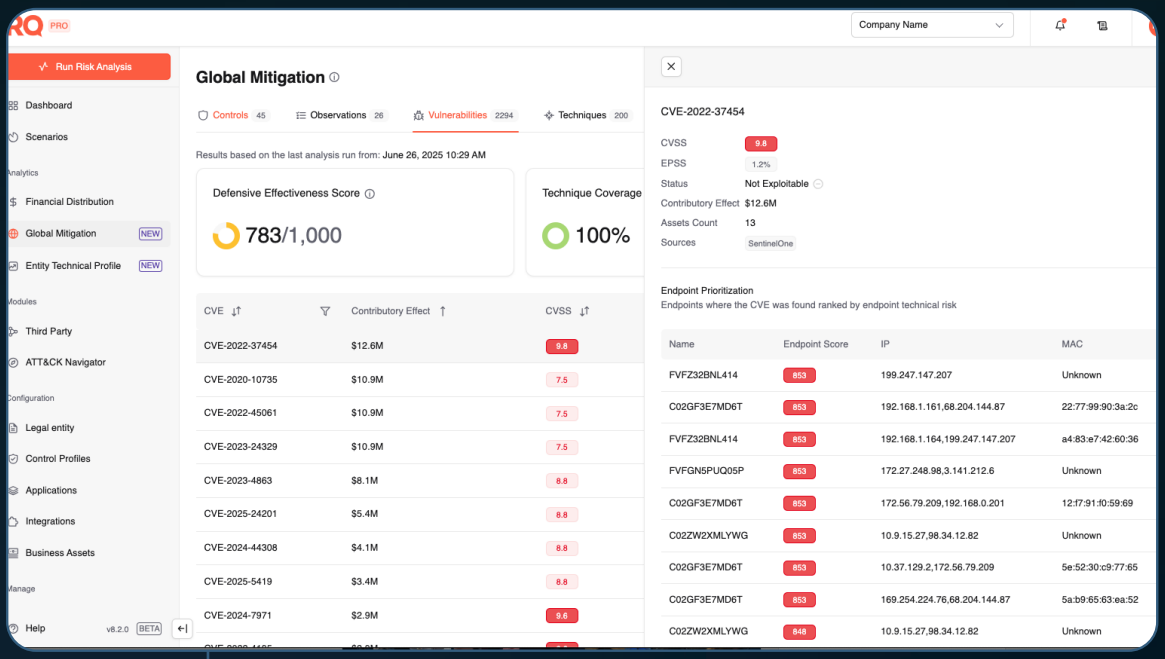
You can inventory critical domains, scan continuously for lookalikes or malicious registrations, and catch phishing infrastructure before it's weaponized.

Plus, with visibility into OSINT and dark web chatter, you can alert customers to risks they didn't even know existed.

Your Outcomes

- **Brand Protection as a Service**
  Offer domain monitoring as a premium capability - or bundle it into your core offering
- **Catch Threats Before Impact**
  Intervene early, before spoofed domains get used in attacks
- **Sticky, High-Margin Service**
  Automated, scalable, and valuable - everything you want in a modern MSSP feature

Vulnerability Prioritization



ThreatConnect's vulnerability insights go beyond generic CVSS scores to insights highly tailored to your customers' business.

Your Struggles

You're handing customers a list of CVEs, and they're handing back silence - or worse, blame.

- Vulnerability reports feel like homework
- Patch teams don't know where to start
- When the wrong thing gets exploited, they blame you

Without prioritization, you're not providing protection. You're providing paperwork.

Our Service

ThreatConnect helps you prioritize vulnerabilities that actually matter.

We correlate each CVE to:

- Real-world exploitability
- Active threat actor behavior
- Known exposure in the customer's environment

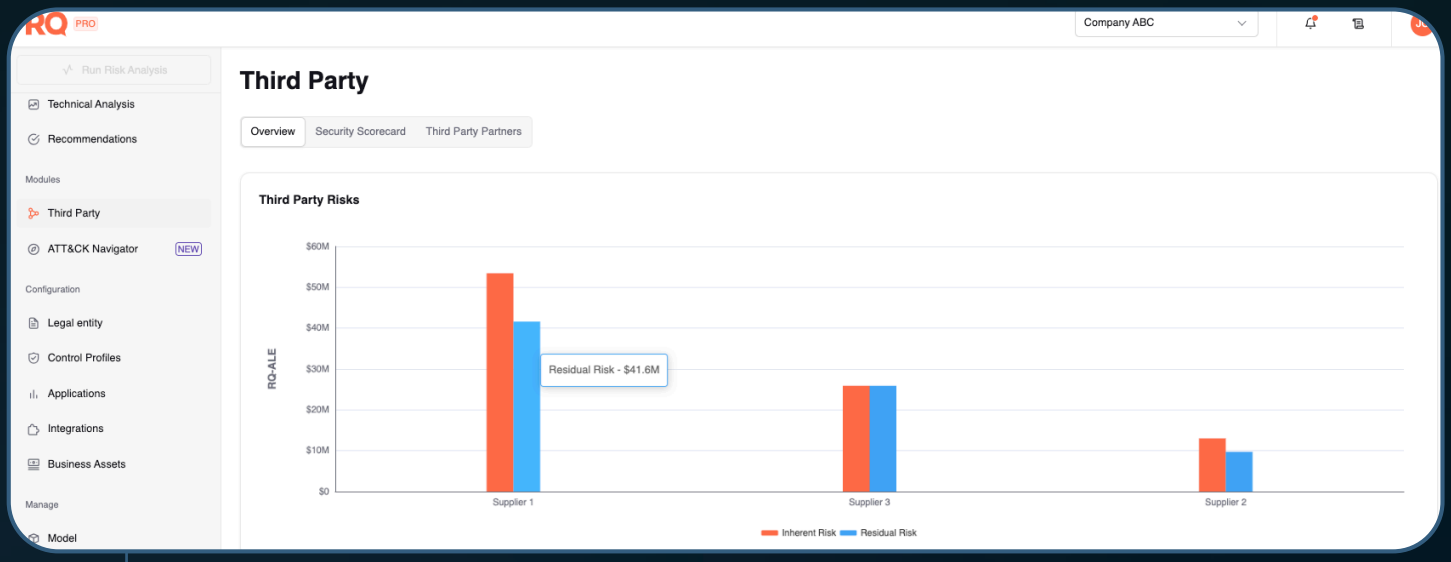
Instead of "here's 300 vulns," you deliver "here's the 3 you need to patch now, and why."

Your Outcomes

- **Prove What Matters**
  Replace spreadsheets with risk-backed recommendations customers can act on
- **Focus Remediation, Not Just Detection**
  Help patch teams work smarter, faster, and with confidence
- **Show ROI**
  Prioritized remediation = measurable risk reduction (85% of Known Exploited Vulnerabilities remain unremediated after 30 days)

  [Source: Verizon DBIR 2024]

Supplier Threat Monitoring



Track real dollar risk values for each supplier, customer-by-customer.

Your Struggles

Your customers are exposed - but not by their own systems.

- Third-party vendors create invisible risk
- Customers don't know when a partner is compromised
- Supply chain attacks are up, and you don't want to get blindsided

If you're not watching their suppliers, who is?

Our Service

ThreatConnect lets you track threats targeting your customers' vendors and partners - before the damage spreads.

Monitor:

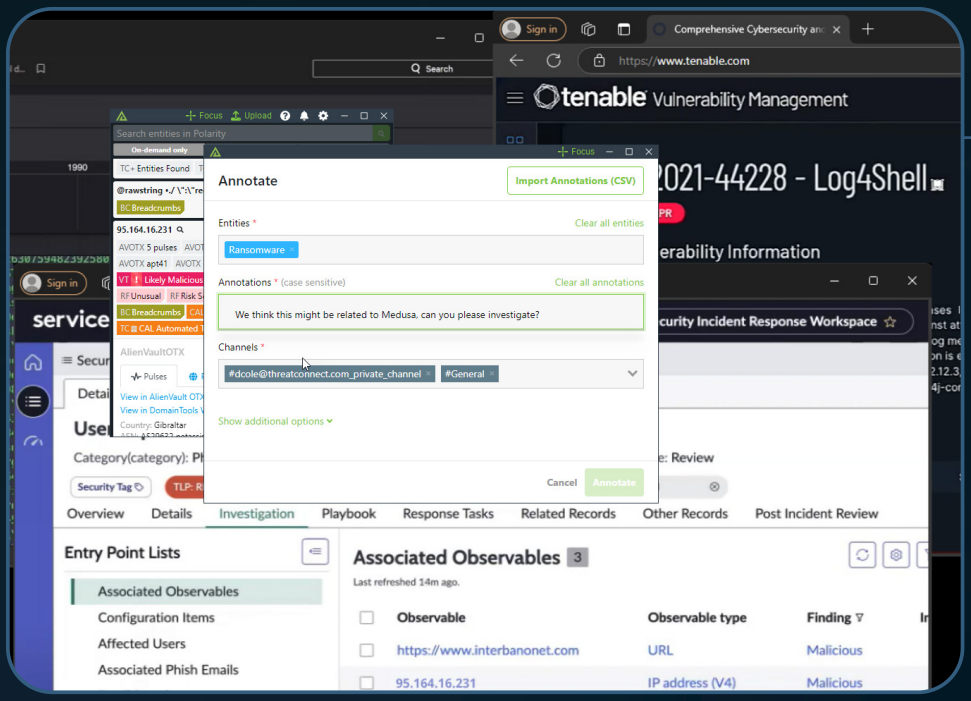
- OSINT and dark web chatter mentioning key suppliers
- Infrastructure tied to third-party compromise
- Campaigns using shared software, tools, or platforms

Give your customers visibility into risk beyond their perimeter.

Your Outcomes

- **Become the Early Warning System**
  Help customers spot compromise before it impacts them directly
- **Identify Risk Without Needing Direct Access**
  No integrations or supplier buy-in required
- **Deliver Insights No One Else Can**
  Make supplier intelligence part of your core value, not a post-breach apology

RFI Enablement



Customer Request → Routed Intake → Analyst Response

Your Struggles

Your customers want intel - but they don't know how to ask for it.

- You get vague emails with unclear requests
- Prioritization becomes a guessing game
- Analysts waste time chasing missing context

This isn't just inefficient - it delays action and frustrates everyone.

Our Service

ThreatConnect gives you a structured, trackable way to manage intelligence requests.

With a built-in customer-facing RFI portal, you can:

- Let customers submit questions with the right metadata upfront
- Categorize requests by urgency, topic, or customer environment
- Route tasks automatically into the correct workflow or queue

No more email chains. No more guesswork. Just actionable input at the source.

Your Outcomes

- **Clean Intake of Actionable Requests**
  Reduce back-and-forth and get to work faster
- **Faster Service Delivery**
  Every vague email costs your team time - and eats away at your margin. Structured RFIs fix that.
- **Higher Customer Satisfaction**
  You look smarter, faster, and more in control

Bonus Services

These services aren't just easy to deliver - they're high-margin by design.

Consultative Advisory

Help your customers think like defenders - not just alert consumers.

With ThreatConnect, you can deliver high-value advisory services:

- Build and review threat models tied to business context
- Validate customer detection strategies
- Interpret actor campaigns and industry-specific risks

This isn't managed security. It's managed insight.

Threat-Informed Hunt

Don't just wait for alerts - go find the threat.

Use ThreatConnect's overlays, TTP modeling, and ATT&CK-based threat scoring to:

- Identify attacker behavior in your customers' environments
- Conduct high-confidence hunts without guesswork
- Deliver tangible, threat-driven reports your customers will want to read

These services aren't just differentiators. They're revenue drivers.

Why MSSPs Choose ThreatConnect

Service	Reduces MTTR	Protects Margin
Threat-Informed Response	Immediate context for faster triage	Less analyst time per alert
TI-Informed Detections	Better signal = less triage	Fewer false positives to chase
Domain Monitoring	Early detection of threats	Fully automated, scalable offering
Vulnerability Prioritization	Focused patching = faster closure	Less time spent on low-impact vulnerabilities
Supplier Monitoring	Find threats before they hit	No need for access/integration
RFI Enablement	Actionable, structured requests	Less wasted time, higher efficiency
Advisory & Hunt	Proactive defense, not reactive	High-value, premium services

↑ **Operational Effectiveness**
97% report improvements in the **effectiveness of operational** tools like SIEMs, SOARs, and EDRs

↑ **Time Savings**
90% report **time savings** › 50%

↓ **MTTR**
67% report › 50% **reduction in MTTR**

↓ **False Positives**
63% say that ThreatConnect **reduced their false positive rates**

↑ **Collaboration**
79% report that ThreatConnect **improves collaboration between teams**

> **ThreatConnect narrowed 200M SIEM events to 12 incidents."**
> - Head of Threat Intelligence

> **ThreatConnect cut close time by 300% in month one."**
> - Director of Security Operations

> **Our IR time went from 7 hours to 37 minutes."**
> - CISO

You're not just securing networks. You're securing your business model.

Ready to reduce MTTR, increase margin, and turn your analysts into advisors? Let's talk.

Let's build the next generation of MSSP services - together.

sales@threatconnect.com

www.threatconnect.com

+1-703-229-4240

ThreatConnect.

ThreatConnect powers smarter, faster, and more resilient cyber defense by uniting threat intelligence, security operations, and cyber risk management. Our Intel Hub platform brings threat and risk data together to help organizations prioritize what matters most, operationalize defenses more efficiently, and communicate cyber risk in business terms. Trusted by over 250 global enterprises, ThreatConnect enables security teams to adapt to evolving threats, make better decisions, and prove their impact - from the SOC to the C-suite.