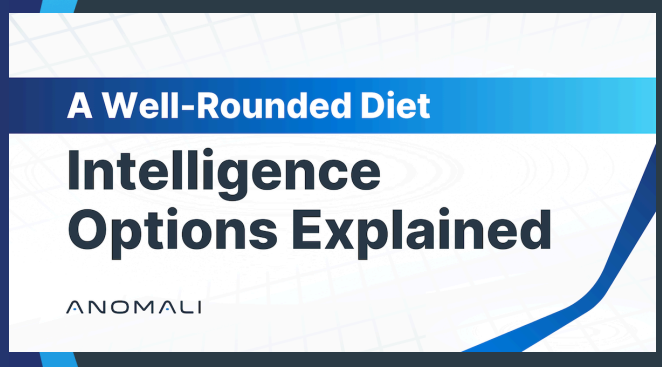
BLOG

Building the Ultimate Defense Requires a Balanced Diet of Threat Intelligence

Just as no elite athlete would consider a training diet that consisted of only bread, no top-notch security team should rely on a solitary source of threat intelligence.



GAGE MELE | FEBRUARY 19, 2025

Share:

As the saying goes, “People cannot live by bread alone.” The same goes for security operations centers (SOCs). A truly effective defense requires visibility across multiple intelligence streams, each serving a unique role in constructing a complete picture of your organization’s threat environment.

A Well-Rounded Diet: Intelligence Options Explained

Here’s an overview of the primary threat intelligence “food groups:”

Open Source Intelligence (OSINT)

OSINT is the bedrock of any threat intelligence strategy, offering broad coverage and insights from public and community-driven sources.

- Value: OSINT's use of publicly available data sources allows organizations to gather intelligence without specialized access or expensive systems while easily adapting their collection methods based on their objectives. This democratized approach enables rapid verification through cross-referencing multiple sources, scales cost-effectively, and naturally evolves alongside new technologies and data sources.
- Capabilities: OSINT provides broad coverage with publicly available threat data and community-driven insights from sources like the Malware Information Sharing Project (MISP), SANS Internet Storm Center (ISC), Cybersecurity and Infrastructure Security Agency (CISA), OpenPhish, and many others.
- Limitations: OSINT is often reactive rather than proactive and may involve compliance risks.
- Challenges: Integrating OSINT often requires significant manual work and tuning. It rarely detects targeted attacks before public disclosure.

The bottom line? While essential, OSINT may leave intelligence gaps, due to its ever-changing nature. It’s the white rice of threat intelligence — filling and tasty but not a complete meal.

Proprietary Research Feeds

By leveraging dedicated threat labs, proprietary research feeds can uncover patterns and campaigns that may not be visible in public sources. These feeds tend to be more specialized. Some premium vendors (see “Premium Intelligence Feeds” below) may also offer this category of intelligence feed.

- Value: Proprietary feeds offer original research from dedicated threat labs.
- Capabilities: These feeds often excel at identifying patterns across multiple data points and uncovering coordinated attack campaigns.
- Limitations: Proprietary feeds may be limited to specific regions or sectors and by the scope of the research team providing the intelligence.
- Challenges: Organizations may struggle to effectively correlate proprietary research with other intelligence.

Overall, proprietary research feeds hold value and can be an important building block in a security strategy. They’re like the seasonal fruits and vegetables of threat intelligence.

Premium Intelligence Feeds

Premium feeds are high-quality, comprehensive threat intelligence feeds that come from high-end vendors, as well as from detection technologies, such as antivirus, firewalls, intrusion detection systems, and intrusion prevention systems. They may include a mix of proprietary research alongside data from other sources, often with additional analysis and context. Premium feeds allow organizations to scale their threat intelligence capabilities by having curated sources that provide a level of specialization and flexibility that can fill critical intelligence gaps.

- **Value:** Premium feeds provide specialized coverage through a curated partner ecosystem, filling specific intelligence gaps.
- **Capabilities:** They provide access to unique data sources and enable organizations to scale intelligence coverage as needs evolve.
- **Limitations:** Premium feeds can be expensive and may require careful integration to avoid duplicating efforts across existing sources.
- **Challenges:** SOC teams may need to prioritize which premium feeds to subscribe to based on their specific threat landscape and available resources.

The prime rib of threat intelligence, premium feeds provide high-quality protein but may be too expensive to eat every day of the week.

ISAC Feeds

Information sharing and analysis centers (ISACs) provide industry-specific intelligence by fostering collaboration among organizations facing similar threats. These feeds offer contextually relevant insights to enhance sector-specific defenses.

- **Value:** ISAC feeds focus on industry-specific intelligence sharing, offering highly relevant insights tailored to region, sector, and other factors.
- **Limitations:** ISAC feeds may lack breadth, as they focus narrowly on specific industries or threats.
- **Challenges:** Participation in ISACs may require significant coordination and commitment from member organizations to maximize value.

ISAC feeds are important staples but are niche and community-focused, sort of like your neighborhood's seasonal potluck.

Workflow

The Power of Integration

Once you've assembled your threat intelligence ingredients, the next challenge is to turn it into a cohesive meal. For example, an OSINT feed might detect a phishing campaign, proprietary research might validate the threat with deeper context, and an ISAC feed might add industry-specific relevance. Together, these feeds help SOC teams track an attack across its entire lifecycle. Combining these sources creates a complete threat picture, allowing your SOC to detect, validate, and respond to threats faster.

To make this work, your threat intelligence platform should:

- Correlate data: Aggregate intelligence from diverse sources into actionable insights.
- Integrate seamlessly: Work with existing tools like SIEMs, SOAR platforms, and EDRs.
- Scale effectively: Support additional feeds as new needs and threats emerge.

Implementation Considerations

Choosing the right threat intelligence platform isn't just about features — it's about how well the platform fits into your organization's needs. Here's what to look for:

- Integration capabilities: Ensure the platform integrates seamlessly with your existing tools, such as security information and event management (SIEM), security orchestration and response (SOAR), and endpoint detection and response (EDR).
- Compliance and security: Platforms developed in regions with strong compliance standards, like the United States, help minimize risk.
- Support and training: Look for a platform with comprehensive support, such as dedicated customer success managers and educational resources.
- Scalability: The platform should allow you to scale effortlessly, adding new feeds as your organization grows or as threats evolve.

A cost-benefit analysis will help you evaluate a platform's ROI by balancing the upfront cost of implementation against the long-term benefits of reduced response times, accelerated threat visibility, and improved overall security posture.

Anomali: Superior Intelligence, Integrated With the Security Workflow

By integrating powerful analytics, advanced AI, and unmatched threat intelligence into a unified platform, Anomali delivers what no other solution can: a complete end-to-end system for detecting, analyzing, and responding to threats. Whether you need to correlate disparate data sources, automate tedious tasks, or gain deeper insights into attacker behavior, Anomali helps your team stay ahead of even the most sophisticated adversaries.

Anomali delivers:

- Industry-leading threat intelligence: Anomali ThreatStream ingests and correlates data from OSINT, proprietary research feeds, ISACs, and premium intelligence sources to give a comprehensive and actionable understanding of threats to your threat hunters, security researchers, analysts, and IT teams.
- AI-Powered Copilot: Anomali's AI-Powered assistant enhances your SOC's capabilities, helping teams work faster and smarter. Its NLP interface empowers analysts of all skill levels to do more without learning proprietary query languages.
- Unified platform: Anomali is the only solution that combines extract-transform-load (ETL), SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP in a single, cohesive platform. This ensures that your SOC has the visibility, analytics, and automation needed to strengthen defenses and reduce risk — all in one place.

Anomali's AI-Powered Security and IT Operations Platform delivers mind-blowing speed, scale, and performance at a fraction of the cost of competing solutions. Its cloud-native approach modernizes the delivery of legacy systems to deliver security analytics that enable leading organizations to detect, investigate, respond to, and remediate threats in one integrated platform.

Ready to build the ultimate defense for your organization? Schedule a demo.

Gage Mele

Gage Mele is the Manager of Cyber Intelligence at Anomali. As an expert in cyber security, his passion lies in Threat Intelligence, and he has covered the space for a decade.

Discover More About Anomali

Get the latest news about cybersecurity, threat intelligence, and Anomali's Security and IT Operations platform.

SEE ALL RESOURCES

BLOG

How AI is Transforming Threat Intelligence Platforms

LEARN MORE

BLOG

The Primary Sources of Cyberthreat Intelligence

LEARN MORE

BLOG

Elevating Threat Intelligence and Security Operations With Anomali's Latest Innovations

LEARN MORE

Propel your mission with amplified visibility, analytics, and AI.

Learn how Anomali can help you cost-effectively improve your security posture.

SCHEDULE A DEMO

ANOMALI

808 Winslow Street,
Redwood City, CA,
94063, United States

+1 844 4 THREATS (847328)
+44 8000 148096 (International Toll-Free)

Platform and Products

- Anomali Platform
- Anomali Copilot
- Anomali Security Analytics
- Anomali ThreatStream

Marketplace

- Anomali Marketplace
- Threat Intelligence Feeds
- Threat Analysis Tools and Enrichments
- Security System Partners
- Marketplace for Partners

Partners

- Partners Overview
- Join the Technology Partner Program
- Anomali SDKs
- Threat Intel Sharing
- Partner Portal Login

Resources

- Resource Library
- Blog
- Events
- Support
- Glossary

Company

- About Anomali
- Careers
- Contact Us
- Leadership
- Press Room
- Schedule Demo