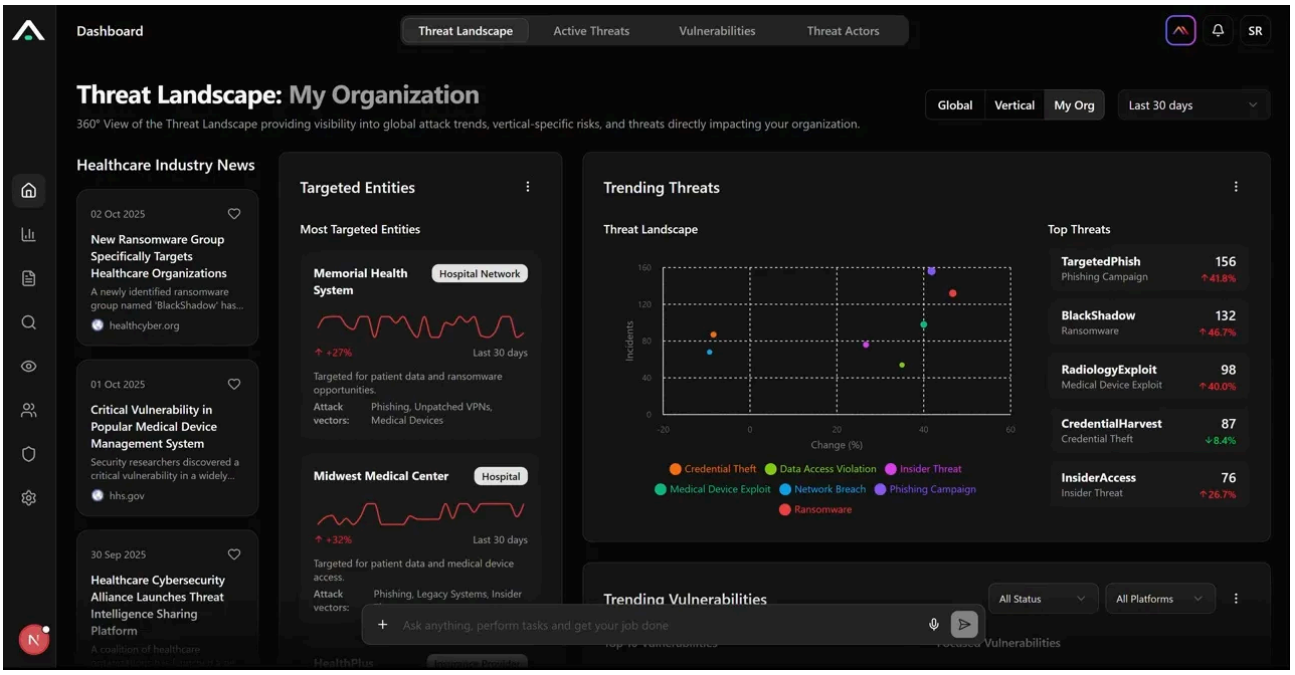
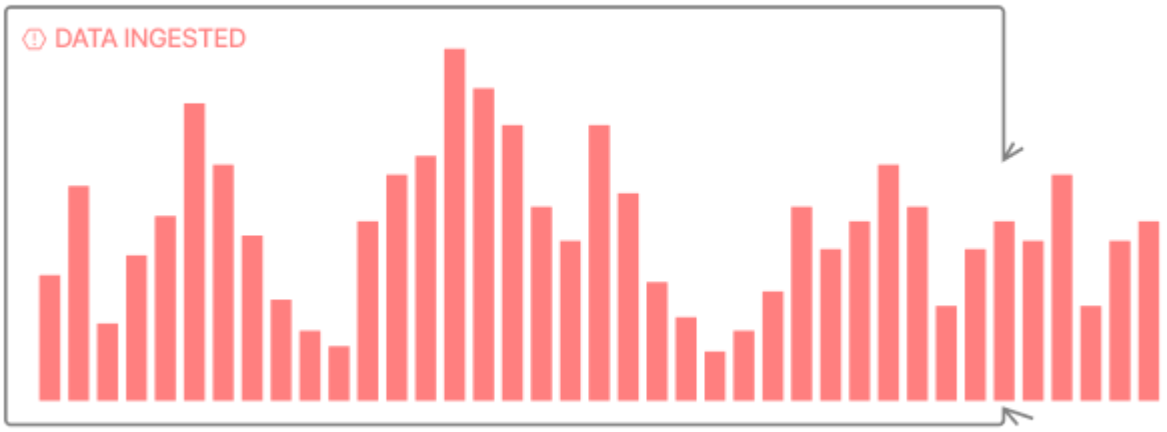
Anomali | AI Threat Intelligence & Agentic SOC Platform

Archived: 2026-04-05 19:52:55 UTC

Centralize all security telemetry, enrich it with real-world threat intelligence, and partner with our specialized AI agents to automate detection, investigation, and response.

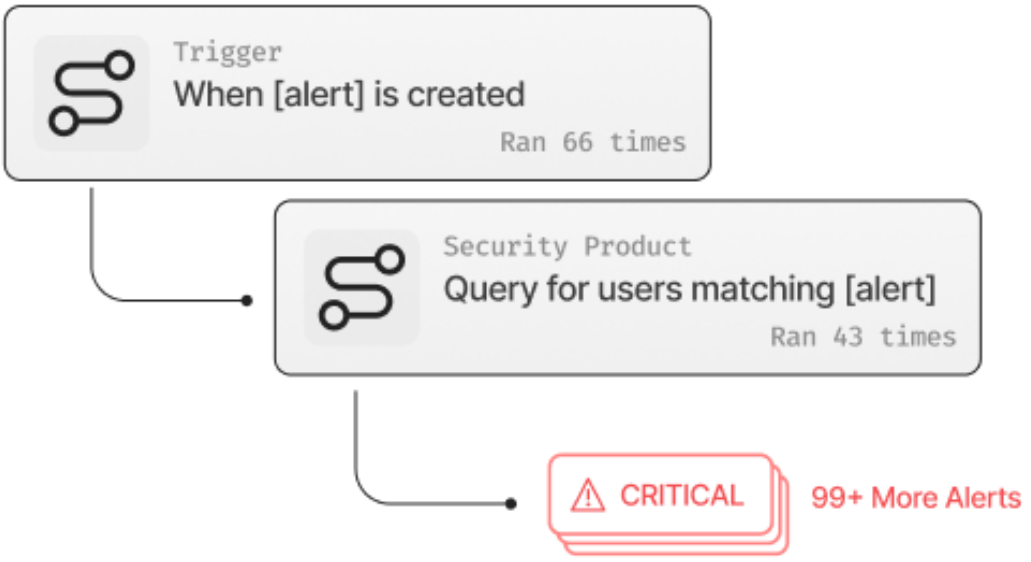


Trusted partner of Fortune 500 Companies

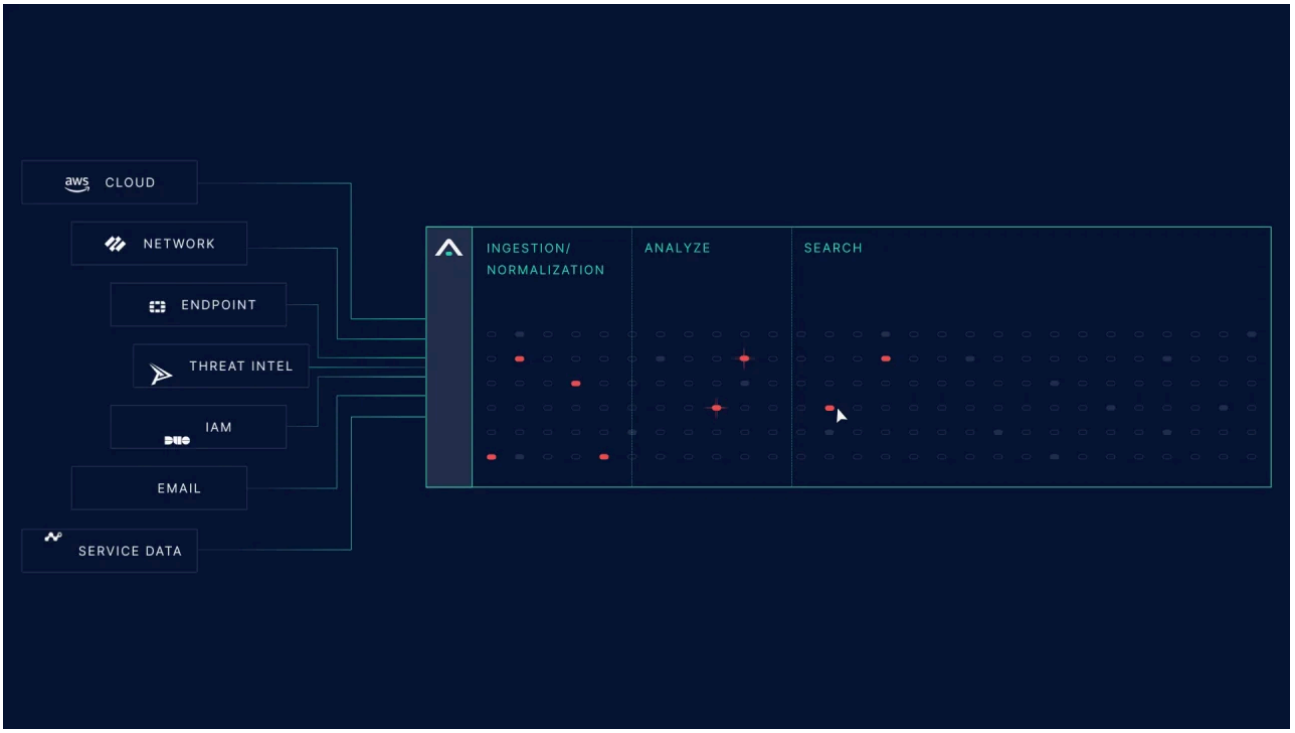


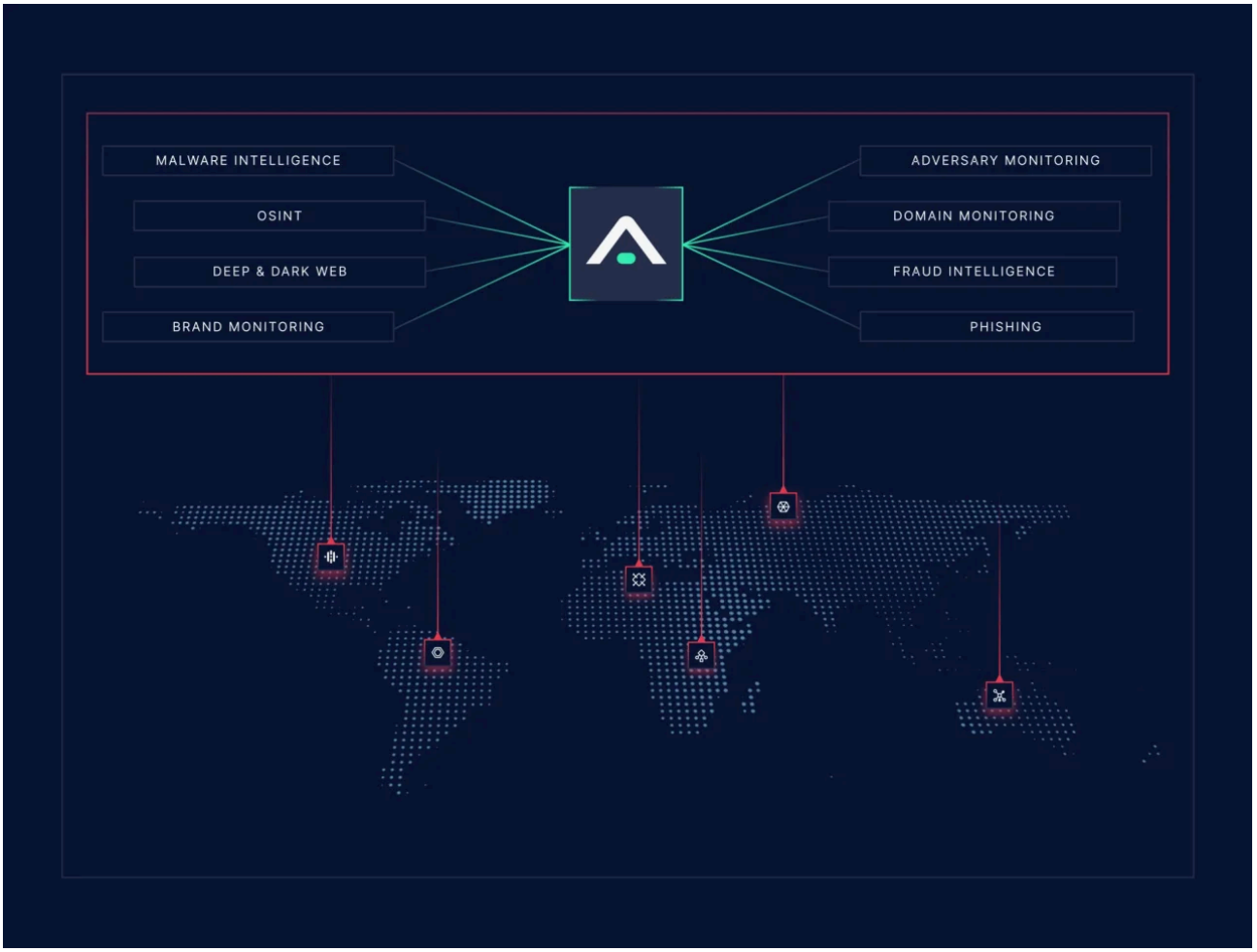
Legacy SIEMs can’t keep up with today’s data volumes.

Standalone intelligence feeds don’t operationalize.



Automation without context creates noise, not outcomes.





Tell me about IP 118.248.255.174

What are the top threats to my organization?

Cl0p is a Ransomware-as-a-Service (RaaS) operation first observed in 2019, known for its advanced anti-analysis and anti-virtual machine detection capabilities. The group rose to prominence in Q2 2023 by automating the exploitation of file transfer vulnerabilities, including MOVEit Transfer and GoAnywhere MFT. The group has been known to exploit zero-day vulnerabilities, such as the CVE-2023-34362 vulnerability in Progress Software's MOVEit Transfer solution. In this campaign, they used a SQL injection vulnerability to install a web shell called LEMURLOOT, enabling data theft from underlying databases.The IP address 118.248.255.174 is identified as a malicious IP (mal_ip), an APT IP (apt_ip), and a scanning IP (scan_ip) with high confidence levels ranging from 98 to 100. It has been tagged with various sources such as Mandiant, Anomali Adversary Intelligence, and cinsscore:ci-badguys OSINT. It is located in China and is part of the China Unicom Shandong province network. The IP is associated with the threat actor APT28, known for state-sponsored activities and information theft. Tags related to APT28 include Fancy Bear and Iron Twilight.

Analysts pivot across years of data and intelligence in seconds.

Context-driven prioritization reduces false positives and alert fatigue.

Threat intel informs every stage of the SOC workflow, not just reports.

Eliminate SIEM tax and manual effort while scaling data retention.

Security telemetry from across your environment flows into a single, high-performance data lake.

ThreatStream Next-Gen adds adversary and campaign context, turning raw signals into prioritized risk.

AI-driven agents guide analysts and automate response, accelerating outcomes without sacrificing oversight.

An exceptional / state of art product with a great customer focused team to enable the organization improve its cyber posture proactively.

Excellent TIP to concentrate & correlate Feeds from all kind of sources. Need to maturing in the capability to produce reports and with Sighting.

Anomali provide a knowledge system that provides our organisation with a tool that helps us getting more insight and overview in the financial threat landscape, combined with extended connectivity possibilities related to external intelligence sources makes this a powerful tool.

Once products are deployed, the process runs smoothly. Produces huge numbers of Threat Intel, which were filtered and customized to our requirements. Anomali support is outstanding, and dedicated to satisfy our requirements.

Anomali has been one of the only platforms we've seen that allows us to tag our own intelligence, apply confidence ratings and collaborate with other intel sources to get a better picture of the attacker infrastructures, etc at a play in Cyber Attacks.

From the moment we implemented Anomali we immediately felt like family. They supported us in the first steps when during our learning phase with the product and now they check in on a regular basis to ensure that we're using the product to it's fullest extend and capabilities. Whenever we have a support issue, they are always available to help and does it with an amazing attitude.

I could say these data set is designed for practitioner. 1. Input - All kind of (unstructured + structured) data could processed properly. 2. Output - The type of export also clearly organized. So It saves time to customized/beautify.

From the moment we implemented Anomali we immediately felt like family. They supported us in the first steps when during our learning phase with the product and now they check in on a regular basis to ensure that we're using the product to it's fullest extend and capabilities. Whenever we have a support issue, they are always available to help and does it with an amazing attitude.

Anomali has been one of the only platforms we've seen that allows us to tag our own intelligence, apply confidence ratings and collaborate with other intel sources to get a better picture of the attacker infrastructures, etc at a play in Cyber Attacks.

I could say these data set is designed for practitioner. 1. Input - All kind of (unstructured + structured) data could processed properly. 2. Output - The type of export also clearly organized. So It saves time to customized/beautify.

An exceptional / state of art product with a great customer focused team to enable the organization improve its cyber posture proactively.

Anomali provide a knowledge system that provides our organisation with a tool that helps us getting more insight and overview in the financial threat landscape, combined with extended connectivity possibilities related to external intelligence sources makes this a powerful tool.

Gartner peerinsights™

Once products are deployed, the process runs smoothly. Produces huge numbers of Threat Intel, which were filtered and customized to our requirements. Anomali support is outstanding, and dedicated to satisfy our requirements.

Gartner peerinsights™

Excellent TIP to concentrate & correlate Feeds from all kind of sources. Need to maturing in the capability to produce reports and with Sighting.

Hugh Njemanze and his team at Anomali have taken security analytics to a new peak and they continue to relentlessly innovate. Moreover, we have used their platform to deliver business analytics. They have led the market in AI and ML, which has increased our productivity and our effectiveness with our management and board. Using The Anomali Platform is a competitive advantage for us. Finally, when Anomali says they partner with their customers, they mean it. Keep innovating!

10x

10x Banking, a financial services technology company with a mission to move banks from monolithic to next-generation core banking solutions delivered through the world's most comprehensive and powerful cloud native SaaS bank operating system, uses Anomali ThreatStream and Lens to help operationalize threat intelligence for their security team.

Anomali uniquely innovates from our perspective as customers vs. the vendor or the analyst communities. They speak business and have attended one of our board meetings. Their approach is the modern path of managing security to drive business. They are all about use cases and automation. Not to mention the cost savings. They serve the who's who globally in our sector.

When I first met Anomali, I thought that they were a SIEM 3.0 with the best intelligence. I now think differently and am less focused on acronyms. As a CISO, I need to protect my organization and deliver shareholder value. Anomali is my partner.

As one of the prominent banks in the United Arab Emirates, we manage assets and transactions for thousands of customers. One of our main commitments to our customers is security and we achieve this through solid partnerships with industry experts such as Anomali. By bringing in industry experts, we expect to gain advanced levels of security that will help us to further heighten our defenses and intercept any possible exploitation by cybercriminals.

The financial services industry continues to be among the most targeted in the world, with cybercriminals always attempting to make inroads directly through banks' networks or by going after consumers directly. Anomali has proven its ability to deliver on the promise of advanced threat intelligence, which supports us in helping our users to remain secure and better prepared. By adding them to our lab environment, we are confident that defensive capabilities will strengthen for all involved.

We leverage market-leading tools to give our company a competitive advantage and our 24/7 SOC a leg up on bad actors. With Anomali, we improve on both of these goals. By adding intelligence, we achieve a high level of

certainty that enhances prioritization of the most serious threats our customers face, while improving our mitigation decisions.

All public organizations are targeted by nefarious actors with extreme frequency, Oklahoma is no exception. Since the beginning of the current global health crisis, we've experienced a spike in related attacks. Anomali will show us who the attackers are, when they are coming after us, and provide context needed to prioritize and speed our response to the most serious threats we face.

The time it takes to analyze a threat has gone down from 30 minutes to just a few minutes, time that adds up over the course of investigating many malicious IPs every week. There has been a substantial decrease in terms of meantime-to- know.

Before Anomali, we had tons of information without context. We had to look through thousands of alerts quickly just to see what stood out and then react to those. Anomali enabled us to spend less time dealing with noise, and more time focusing on critical issues.

From the moment we implemented Anomali we immediately felt like family. They supported us in the first steps when during our learning phase with the product and now they check in on a regular basis to ensure that we're using the product to it's fullest extend and capabilities. Whenever we have a support issue, they are always available to help and does it with an amazing attitude.

Anomali has been one of the only platforms we've seen that allows us to tag our own intelligence, apply confidence ratings and collaborate with other intel sources to get a better picture of the attacker infrastructures, etc at a play in Cyber Attacks.

I could say these data set is designed for practitioner. 1. Input - All kind of (unstructured + structured) data could processed properly. 2. Output - The type of export also clearly organized. So It saves time to customized/beautify.

An exceptional / state of art product with a great customer focused team to enable the organization improve its cyber posture proactively.

Anomali provide a knowledge system that provides our organisation with a tool that helps us getting more insight and overview in the financial threat landscape, combined with extended connectivity possibilities related to external intelligence sources makes this a powerful tool.

Once products are deployed, the process runs smoothly. Produces huge numbers of Threat Intel, which were filtered and customized to our requirements. Anomali support is outstanding, and dedicated to satisfy our requirements.

Excellent TIP to concentrate & correlate Feeds from all kind of sources. Need to maturing in the capability to produce reports and with Sighting.