THE WEIGHT OF TRUST: HOW A NATIONAL CREDIT BUREAU TOOK CONTROL OF ITS CYBER MANAGED INTELLIGENCE NEEDS

The institution at the center of a nation's financial trust infrastructure was running its threat intelligence operation on manual labor and good intentions. Neither was enough.

A cybersecurity failure at a credit bureau could easily become a national incident. Credit bureaus hold the financial history of millions of citizens and businesses, and lenders rely on them to make decisions. Governments rely on them to understand risk. The entire architecture of financial trust in a country flows through their systems.

For one such institution, operating as the first and only national credit bureau in its country and supervised by the central bank, that weight of responsibility was not lost on the security team. What was lost, increasingly, was time. The time analysts needed to find the real threats inside an overwhelming flood of data.

The institution had invested in security innovation. Its security posture had ambitions to match its national mandate. But ambition and execution were running on two separate tracks, and the gap between them was widening.

According to the World Economic Forum's Global Cybersecurity Outlook 2025, 72% of organizations reported an increase in cyber risk. By 2026, the Forum found AI-driven fraud, phishing, and emerging AI vulnerabilities had become the dominant forces driving cyber risk.

When More Data Creates Less Clarity

The problem was not a lack of investment in threat intelligence. The credit bureau had done what most security leaders are told to do: cast a wide net. It collected intelligence feeds from multiple sources, giving analysts broad coverage of the threats they tracked. On paper, this looked like strong threat intelligence strategy.

In practice, it created a different kind of problem. The volume of indicators of compromise (IOCs) flowing into the SOC was enormous, and much of it was duplicated, overlapping, or simply irrelevant to the institution's specific environment. Analysts had no automated way to filter the noise. Everything required human review, which slowed down the ability to assess risk.

The result was predictable. False positives multiplied, consuming analyst time that should have been directed at genuine threats. The security team was working harder than ever and seeing less of what mattered. The maturity of the CTI program, rather than advancing, was stalling.

> Everything was very manual and done with a lack of process. The volume of false positives drained analyst time and distracted the team from the real threats they needed to be aware of and act on.

This is not an unusual story. The Picus Blue Report 2024 found that even as logging coverage improved across the banking and financial services sector, alert scores actually declined as logging volumes grew, revealing a widening gap between the raw data organizations collect and their ability to act on it. More inputs, without a platform to normalize and prioritize them, can make a security team slower, not faster.

A Regulator with High Expectations

The operational pressure was compounded by the regulatory environment. As a supervised entity of the central bank, the institution was required to comply with a formal cybersecurity framework covering governance, risk management, threat intelligence, and incident response. These were not aspirational guidelines. They were mandatory requirements, subject to examination.

Around the world, financial regulators have moved aggressively to raise the security floor. According to Check Point Research's 2025 Financial Threat Landscape Report, cyber incidents targeting the financial sector more than doubled in 2025, rising from 864 incidents in 2024 to 1,858 in 2025. In response, regulators across major markets from the EU's DORA framework to New York's NYDFS cybersecurity rules have moved to formalize Cyber Threat Intelligence requirements for financial institutions, raising the floor from best practice to regulatory expectation. Falling short carries reputational and regulatory consequences.

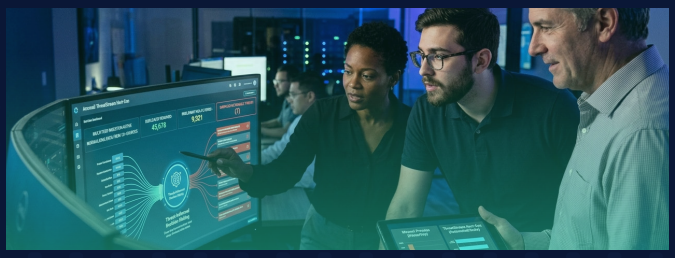
For the credit bureau, meeting the regulator's Cyber Threat Intelligence requirements meant demonstrating a structured, repeatable process for collecting, analyzing, and acting on intelligence. The manual, fragmented operation the security team had been running was not going to pass that test.

> The power of AI and the efficiency it provides help organizations envision what their future state could look like, and that future state is one where analysts spend their time on decisions, not data management.

Cutting the Noise

After evaluating various intelligence options, the credit bureau selected Managed Intelligence as a service, powered by Anomali ThreatStream Next-Gen, deployed on-premises to satisfy data sovereignty requirements, along with Anomali Agentic AI and a dedicated malware intelligence feed.

The case for Anomali ThreatStream Next-Gen rested on a straightforward demonstration. Its aggregation capabilities and threat-informed decision making could ingest the credit bureau's multiple intelligence feeds simultaneously, normalize the data, remove duplicate and irrelevant IOCs, and surface only what was genuinely actionable for the specific environment. What analysts had been doing manually for hours each day, ThreatStream Next-Gen could do automatically, continuously, and at scale.



Anomali Agentic AI addressed the second bottleneck. By ingesting raw threat intelligence and generating structured summaries and reports, it gave analysts a way to bring clear, executive-ready intelligence to leadership without spending days on synthesis. The CTI team could now produce the kind of reporting the regulator expected, and that the C-suite needed, without sacrificing the time required to actually investigate threats.

The effect was a structural shift in how the security operation functioned. Analysts shifted from gatekeeping a queue of noise to investigating and acting on real signals.

Why This Matters Beyond One Financial Institution

Credit bureaus occupy a unique position in the financial ecosystem. They are not consumer-facing in the way a bank or a payments platform is, but their data underpins almost every lending decision made in a market. A breach exposes records and can undermine the integrity of credit assessments across an entire economy.

The threat environment for companies holding this kind of data is severe. Underground markets listed nearly 14.5 million compromised credit cards in 2024, a 20% year-over-year increase, according to Bitsight's 2025 State of the Underground report, reflecting the intense and growing demand among threat actors for financial identity data. Credit bureaus that sit at the center of that data ecosystem are high-value targets by definition.

At the same time, the IBM 2024 Cost of a Data Breach Report found that organizations using threat intelligence identify threats an average of 28 days faster than those that do not, with a breach lifecycle under 200 days costing an average of $1.39 million less than one that extends beyond it. For an institution whose mandate is national financial stability, that speed advantage is operational and existential.

Lessons for Financial Infrastructure Leaders

The credit bureau's experience carries a message that applies to any financial institution sitting at the center of critical financial data: what measures a security team's maturity is how quickly and accurately it acts on intelligence, not how much of it the team collects.

Manual processes that made sense when threat volumes were lower do not scale. And when a regulator arrives expecting a structured, demonstrable CTI program, good intentions and spreadsheets are not sufficient evidence of one.

By unifying its intelligence operation on a single managed intelligence solution, the credit bureau moved from a reactive, labor-intensive posture to one capable of the speed and structure its mandate demands. The analysts are now focused on making critical security decisions about the priority threats that matter. The regulator's requirements are met. And the national credit infrastructure the institution exists to protect is meaningfully more secure.

Ready to move from noise to signal in your threat intelligence operation? Schedule a confidential conversation with Anomali.

SCHEDULE A MEETING