Customer Story

Large Central Bank

European institution achieves greater network visibility, improved threat detection, and decreased incident response time

The nature of large central banks, managing the currency and monetary policies for a country or group of countries, makes them especially attractive targets for criminal gangs and state-sponsored attacks. As cyberattacks on financial institutions continue, the need to rapidly respond to serious threats is of vital importance.

The bank profiled in this case study, as well as other central bank customers of Stamus Networks, rely on Stamus Security Platform as a key piece of their cyber defense. The bank manages over one trillion euros in assets, a number that is common among central banks that use Stamus Security Platform.

This Large Central Bank is based in Europe and uses Stamus Security Platform to:

- Eliminate Blind Spots: deploying Stamus Network Probes throughout the network enables visibility into all areas of their network data and traffic flows including both north-south traffic and lateral movement
- Seamlessly Integrate with other Systems: the flexibility of Stamus Security Platform allows them to complete their security tech stack with a network solution that easily integrates network telemetry with their other tools
- Prioritize Alerts: with Declarations of Compromise™, automatic notifications of the most serious and imminent threat events became available in near real-time, decreasing response times and optimizing staff resources

SNAPSHOT

Organization type: Large Central Bank

Challenge – The customer's legacy IDS limited their ability to rapidly identify and respond to imminent threats and lacked full network visibility.

Solution – Using the Stamus Security Platform, the bank eliminated blind spots on the network, prioritized alerts, and seamlessly integrated network telemetry into their existing tech stack.

Outcome – As a result of implementing SSP, the bank improved their threat detection, decreased their incident response rate, and increased their confidence in the safety of their data.

BACKGROUND

The Large Central Bank (LCB) exists to keep prices stable and set monetary policy for their home country. Due to the sensitive nature of their operations, the LCB is a target of various sophisticated cyber threats from attackers seeking both financial and political gain. Due to the nature of the threats they face and strict regulations they must comply with, the LCB designed their security infrastructure differently than the typical Stamus Security Platform user.

For example, the LCB has a much larger SOC team – over 30 people – than many smaller financial organizations. This is because the leadership is reluctant to rely on automation when dealing with advanced persistent threats (APTs) and other sophisticated attacks. Instead, the LCB places their trust in their SOC analysts to investigate and respond to threats. Additionally, they prefer to manage a largely on-premise IT infrastructure rather than relying solely on a cloud-managed system.

These decisions result from a need to keep their sensitive customer data and critical infrastructure secure due to the regulations and statutory requirements laid forth by the International Monetary Fund (IMF), European Union Agency for Cybersecurity (ENISA), Network and Information Systems Directive (NISM), and the EU's General Data Protection Regulation (GDPR).

The threats faced by this bank are often serious and sophisticated. These threats, in addition to the LCB's crowded tech stack and unique security practices, present some challenges when it comes to employing a new security tool.

Many of these challenges result from their use of a legacy intrusion detection system (IDS). This LCB came to Stamus Networks seeking to replace their legacy IDS with a network detection and response (NDR) platform that would easily integrate into their

EXPECTATIONS

- No single solution provider or single tool will solve all problems and function as a single line of defense
- They rely on a layered defense strategy, using multiple tools from multiple sources, including NDR, EDR, SIEM, SOAR, IDS, NSM, and others
- This ensures a robust defense

existing infrastructure, be flexible enough to adapt to their evolving architecture, help decrease their incident response time, and increase their visibility into network activity. Essentially, they wanted to retain the network security benefits provided by legacy IDS while mitigating the challenges that often come with it.

CHALLENGES

One of the primary challenges faced by this customer was the lack of visibility into network activity provided by their legacy tools. Traditional IDS has limited ability to analyze and aggregate internal and perimeter traffic, simultaneously. The LCB had only deployed network sensors at perimeter gateways, which was acceptable for monitoring north-south traffic but denied them insights from other parts of the network which is required for detecting lateral movement and other advanced threat behaviors.

The LCB also faced challenges prioritizing their security alerts and events. Organizing, prioritizing, and triaging alerts was an arduous and labor-intensive task. They needed a network-based detection system that could help them prioritize by escalating and correlating the most serious and imminent alerts directly to their analysts. This would give them the fastest possible response time, reducing risk. Ideally, this system would deliver high-fidelity triggers with correlated evidence into their security orchestration, automation and response system (SOAR) while also preserving historical event data and related protocol, flow, packets, and file transaction logs for future investigation.

TOP CHALLNEGES

- Limited visibility into network activity provided by legacy tools
- Difficulty integrating a new tool into their existing security infrastructure
- Long incident response times
- Challenges with their crowded tech stack and unique security practices
- Managing a large SOC team and on-premise IT infrastructure
- Protecting against sophisticated cyber threats
- Complying with strict legal requirements and regulations.

The challenges of storing all this event data — as well as the telemetry from their other tools — was not lost on this customer. They needed to ensure that their new network-based detection system was capable of cost-effectively storing data in a way that was consistent with their architecture.

While the LCB currently operates an on-premise physical IT infrastructure, they wanted their network security solution to support cloud deployments as well. This flexibility was important to maintain their options if they transitioned some applications in the future. In other words, they needed a solution that could scale and adapt as they did. Additionally, they wanted a system that could ingest threat intelligence from multiple sources — not just from outside experts, but also from their internal independent threat research teams.

Finally, the LCB was looking for a network security vendor that would not only help them initially deploy and learn the system, but one that would behave as a true partner with them. They wanted a provider committed to continuous improvement and a roadmap that evolved with their needs and with the changing threat landscape. And they needed this partner to regularly work with their SOC team to ensure that they continued to receive maximum value as their needs and infrastructure evolved over time.

SOLUTION

The Large Central Bank chose to deploy the Stamus Security Platform (SSP) with the Stamus NDR license tier. SSP is an advanced network detection and response (NDR) solution that exposes serious and imminent threats against critical assets, enables rapid response, and easily integrates into existing tech stacks. It answered our customer's challenges by providing increased visibility into their network, a flexible cloud and on-prem deployment model, and response-ready, high-fidelity, prioritized alert notifications with quickly accessible evidence and context.

By deploying Stamus Network Probes at multiple points in their network, the LCB eliminated blind spots and increased visibility throughout their network. Previously, their network sensors were only at their gateways, which offered no visibility into internal-only network activity - a significant blind spot. Stamus Network Probes were placed throughout the network including internal locations with scalability for east-west traffic inspection. They perform deep packet inspection to analyze all network traffic and perform real-time threat detection, capture network protocol transactions, and enrich results with extensive metadata. This increased network presence now gives the LCB visibility into all types of traffic across their network, including north-south and east-west movement.

Before using SSP, this Large Central Bank did not have an effective method to prioritize alerts. Their legacy IDS created “alert fatigue” which is caused by an overwhelming number of alert events with no simple, effective way to find a legitimate, imminent threat. SSP solves this problem by providing high-fidelity, response-ready, and prioritized alert notifications with correlated evidence — called Declarations of Compromise™ (DoCs).

A DoC highlights a single, specific threat and the asset (or assets) it is impacting. It produces a detailed attack timeline of the threat’s activity on the network with related context surrounding the impacted asset(s). These events are automatically escalated, and the SOC is notified via webhook in their SOAR and web chat systems. For the LCB, this means no more tedious searching for the serious threats in their legacy IDS “alert cannon” logs.

Now, they are simply notified of the serious and imminent threats, enabling them to respond sooner than they could before. SSP includes DoC coverage for known threats, and more are added weekly by the Stamus Labs threat research team. Additionally, the LCB integrates their internally-developed threat intelligence and creates custom DoC escalations when needed.

SOLUTION SUMMARY

- Implemented Stamus Security Platform to improve visibility into all areas of the network
- Integrated Stamus Security Platform with existing security tools
- Receive near real-time notifications of serious and imminent threats through Declarations of Compromise™
- Use a layered defense strategy with multiple tools and solutions
- Retain all the benefits of legacy IDS while mitigating its challenges

Using Stamus Security Platform also helped address the LCB’s challenge of storing and accessing network data from their multiple telemetry sources. While SSP is an NDR platform, it is built on the powerful Suricata network analysis and threat detection engine, enabling SSP to gather, correlate, aggregate, analyze, and store millions of data elements from IDS and network security monitoring (NSM) data. This allows the SOC team to not only analyze their network activity in real-time, but also access, investigate, and classify historical event data as well. This has proved incredibly useful to the LCB for forensic purposes as well as threat hunting.

One of the greatest challenges faced by this Large Central Bank, as well as many other organizations, is the need for their network detection and response (NDR) system to integrate into the current infrastructure and adapt to the inevitable changes. The LCB needed a platform that was flexible in its ability to seamlessly integrate with other existing tools, as well as being flexible in the way it is deployed — on-premise, in their datacenter, and in the cloud.

Stamus Security Platform tackled both challenges with ease. As an open and extensible system, SSP is unparalleled in its ability to integrate with other systems. There was no issue fitting SSP into the LCB's existing security tech stack. As for deployment options, Stamus Network Probes and the Stamus Central Server can be installed on-premise, in the cloud, or in combination of both. For the LCB, this translates into freedom to adopt any future architectural changes with confidence that their network security system will continue to function effectively.

Finally, SSP offered the Large Central Bank the partnership they had hoped for. Stamus Networks continues to add capabilities to SSP, delivering software releases throughout the year. And the Stamus Networks team continues to conduct training sessions, exercises, and workshops with the LCB analysts to ensure that they continue to receive maximum value from their SSP deployment.

OUTCOME

The Stamus Security Platform gives this Large Central Bank dramatically improved threat detection through network analysis and threat detection, resulting in decreased incident response time, allowing the LCB to keep their data and their nation more secure.

The head of cyber security and governance at the Large Central Bank had this to say about SSP:

"Stamus Networks has provided us with the most effective solution within our security stack. Their dedication to supporting us has been unmatched by any other vendor. We are excited to continue expanding our deployment of the Stamus Security Platform."

> *Stamus Networks has provided us with the most effective solution within our security stack. Their dedication to supporting us has been unmatched by any other vendor. We are excited to continue expanding our deployment of the Stamus Security Platform.*
>
> - Head of cybersecurity and governance at the Large Central Bank

With Stamus Security Platform, the LCB has been able to mitigate the network security challenges presented by their former legacy IDS and the risks those challenges present, while also reaping the benefits provided by an effective next-generation network detection and response (NDR) solution.

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMVS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

✉ contact@stamus-networks.com
www.stamus-networks.com