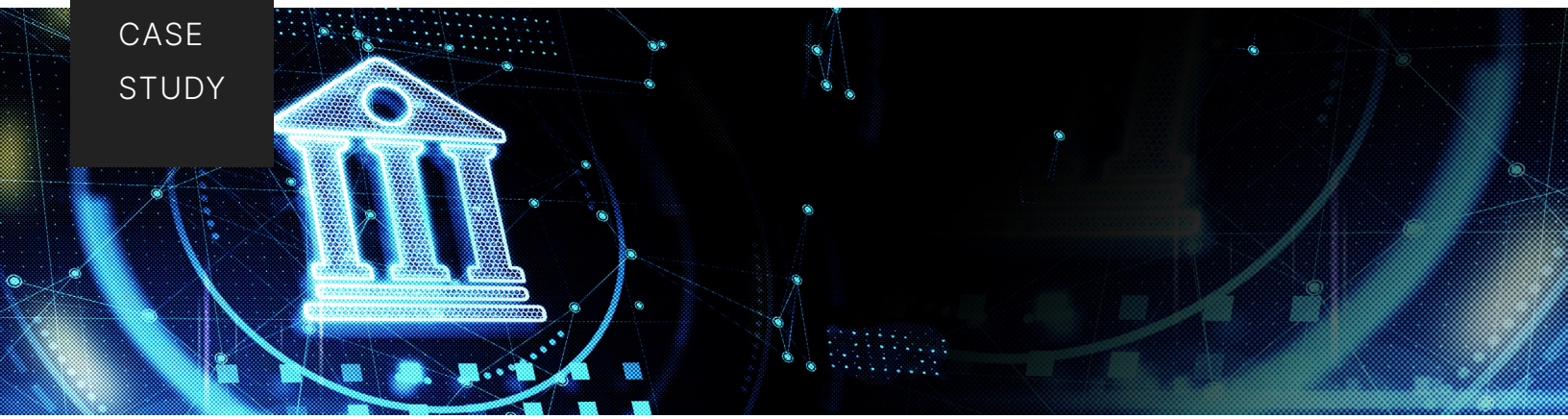
CASE STUDY



Citizens Financial Group Banks on Threat Intelligence to Up-level Resilience

American bank holding company Citizens Financial Group integrates Recorded Future to assess risk, speed response, hunt threats, and deliver finished intelligence

Use Case:

- Threat Hunting (Advanced Detection & Validation)
- Advanced Threat Research and Reporting
- Dark Web Investigation

Challenge:

Reducing time and effort to research threats, assess risk, and deliver actionable reports to stakeholders

Products:

Recorded Future Threat Intelligence

Outcomes:

- Faster detection and better understanding of relevant threats
- Improved focus on specific threat actors
- Enhanced collaboration across security teams to build resilience
- Upleveled junior analysts' skills
- Greater confidence in team's priorities

Trusted financial services companies protect their reputation by assessing risk at every turn. Advanced businesses like Citizens Financial Group rely on premium threat intelligence to research threats, speed incident response, promote collaboration, and build out proactive security practices.

"We were relying heavily on open-source intelligence and looking to do more," says Lea Cure, Manager of Citizens' Threat Intelligence team. "We wanted to acquire more reliable and mature threat intelligence to improve security operations and disseminate high quality finished reports to our stakeholders."

To that end, Cure engaged Recorded Future to add the in-depth assessment, context, and analysis the team could not obtain using open or public intelligence sources and peer-sharing networks alone.

Intelligence Turbocharges Operations

The Citizens Financial Group team quickly began integrating threat intelligence into strategic cybersecurity initiatives as well as day-to-day operations. Leveraging Recorded Future's Intelligence Cloud represented a powerful upgrade from open-source intelligence, saving the team valuable time in identifying, investigating, and mitigating risk.

"Recorded Future saves us a ton of time by alerting us to targeted threats," Cure says. "Being able to access and scrape more data on closed sources is extremely valuable, especially for applications like Telegram and Dark Web sources. The fact that our analysts can be alerted to relevant intelligence in a timely manner significantly improves our workflows."

Cure says the team leverages Recorded Future's advanced query capabilities to quickly find actionable insights. "Previously we would spend a significant amount of time researching open sources to add contextual information to our assessment. With Recorded Future, we are able to specify exactly what we are searching for and exclude information that isn't

> **“With Recorded Future, we are able to specify exactly what we are searching for and exclude information that isn’t relevant, saving us at least 10 hours per week.”**
>
> *Lea Cure*
> *Threat Intelligence Team Manager*
> *Citizens Financial Group*

relevant, saving us at least 10 hours per week,” Cure says. “All the noise is filtered down so we can spend our time and resources digging into the things that are relevant to us. Recorded Future is doing the work for us so we can just focus on taking action.”

A deeper understanding of threats, threat actors, and attacker tactics, techniques, and procedures (TTPs) helps the security team identify and fill gaps in monitoring and detection coverage. Cure says the team will delve into attacker history and explore the possibilities of multiple threat actors and campaigns.

“Recorded Future’s Sigma rules provide valuable technical insights to our threat hunters. By understanding how specific malware functions, we can develop hunt hypotheses to identify similar behaviors within our environment,” she explains. “Then we can ask things like, ‘Do we have the proper tools and logging and monitoring in place for these threats? Would we be able to find and identify those signatures within our environment?’”

From Assessing to Avoiding Risk

Beyond researching known threats, the Citizens Bank security team uses real-time threat intelligence to improve tactical and strategic security operations throughout the risk management lifecycle.

Helping defenders take the offensive

Citizens integrates threat intelligence into proactive exercises designed to assess and bolster defenses. “We work closely with our Red Team during their ‘recon’ phase of engagements by providing them with types of techniques used by threat actors, last known usage of techniques, and technical details about the TTPs they used,” the threat intelligence manager explains. “We leverage Recorded Future to look at previous campaigns and attacks to determine what methods threat actors used so the team can mimic the activity as they attempt to evade our network defenses.”

Hunting for threats ‘in the wild’

The company also relies on threat intelligence to build its growing threat hunting practice. Threat hunters leverage detections created by Recorded Future’s Insikt Group to hunt for threat actor activity within their environment. “Recorded Future is a great place to do research as we build and run threat hypotheses within our environment,” Cure says. “Our threat hunters can use the Sigma rules provided by Recorded Future’s Insikt Group and the historical information on previous attacks and TTPs to query our tools and see if we’d be able to identify an attack.”

Mitigating third-party risk

Like most financial services organizations, Citizens places a premium on monitoring third-party risk. Recorded Future Threat Intelligence helps with monitoring and communicating risk to Tier One suppliers and critical technology vendors. Cure says, “Being able to use the platform to find mentions of our supply chain partners on the dark web and ransomware extortion sites helps us communicate risks that partners might not be aware of before something bad happens.”

Keeping high-level stakeholders informed

The Citizens Bank Threat Intelligence team produces and delivers regular quarterly, mid-year, and end-of-year reports to high-level stakeholders. Along with using the platform to conduct in-depth analysis, leveraging insights from Recorded Future’s Insikt Group streamlines the process of delivering finished intelligence.

“Our analysts are able to utilize a lot of information about threats from end-of-year reports that Recorded Future’s Insikt Group publishes,” Cure says. “We are able to repurpose the information included in their reports which allows us to focus our time and resources on developing meaningful assessments for our internal stakeholders. Having access to that intelligence really simplifies their job.”

In addition, the platform equips analysts to explain ‘what’s happening in the wild’ to their cyber defense teams. “Instead of just producing a high-level executive report, we can get very detailed and technical in explaining the legitimate tools or techniques that a particular threat actor uses and take an in-depth look at the attack kill chain.”

Teams Thrive on Insight

By modernizing many facets of security operations, leveraging threat intelligence empowers security professionals to educate themselves and promotes strategic interactions between teams. “Increasing our

focus on collaboration across departments is a big focus for us this year," the Threat Intelligence team lead explains. "Recorded Future gives us a one-stop shop for doing the research needed to respond to requests for information (RFI) that come our way. We're able to access data, especially within dark web marketplaces and forums, that the average person or analyst doesn't have access to, and that's extremely valuable to other teams."

Deeper understanding for analysts

Streamlining day-to-day operations helps the company to upskill and unburden valuable cybersecurity professionals. "Recorded Future is a very thorough resource that allows newer or more junior analysts to uplevel their skills, educate themselves and learn a lot about what they're finding in the platform," Cure explains. "Our seasoned analysts can also dig in as they make assessments and, instead of just saying 'there's a threat out there that we should care about,' they can understand and explain threats on a much deeper level."

What Happens Next?

Having benefited from Recorded Future on multiple fronts, Citizens Bank plans to expand its use of threat intelligence as they innovate to strengthen security. "We expect to see some valuable use cases as we start digging into Recorded Future's payment fraud and identity intelligence offerings," says Cure who adds: "I would recommend investing in rich threat intelligence to any company in a heavily targeted industry. Recorded Future lets us be more strategic and proactive, and act more quickly than we could using open-source intelligence alone."

> **"Recorded Future is a very thorough resource that allows newer or more junior analysts to uplevel their skills, educate themselves and learn a lot about what they're finding in the platform."**
>
> *Lea Cure*
> *Threat Intelligence Team Manager*
> *Citizens Financial Group*

ABOUT RECORDED FUTURE

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com

© Recorded Future®, Inc. All rights reserved. All trademarks remain property of their respective owners.