Recorded Future®

INVESTBANK Proactively Protects Customer Data While Reducing MTTR by 80% with Recorded Future

Leading Jordanian financial institution INVESTBANK uses Recorded Future to get actionable threat intelligence and streamline orchestration for more effective cybersecurity operations.

الاستثماري INVESTBANK

14+ Hours saved per week on vulnerability research

80% Reduction in MTTR

Use Cases: Dark web monitoring; Brand impersonation detection; Vulnerability disclosure monitoring.

Goal: Enable proactive security management and reduce mean time to respond (MTTR) with detailed threat context and improved cybersecurity orchestration.

Challenge: Quickly accessing accurate and actionable threat intelligence from multiple sources to get ahead of threat actors who target sensitive customer data and abuse brand assets.

Solution: The Recorded Future Intelligence Cloud featuring:

- Brand Intelligence
- Threat Intelligence
- Vulnerability Intelligence
- Recorded Future for Splunk Integration
- Collective Insights

Outcomes:

- Improved response time with relevant threat data
- Increased capacity and elimination of manual tasks by automating security workflows within Splunk
- Prevention of digital risks from impacting customer relationships and diminishing brand reputation
- Prioritization of critical vulnerabilities for remediation

Security and trust form the foundation of every customer's relationship with their bank. As a leading financial institution in Jordan, INVESTBANK is unwavering in its commitment to safeguarding customers' personal and financial data and prioritizes the security of its customers' information, as well as their hard-earned money.

"Our goal is to ensure customers feel that INVESTBANK is a true partner," said Riyad Jazmawi, Head of Information Security at INVESTBANK. "Our success as a bank depends on our ability to deliver robust, secure services and demonstrate that we genuinely care about our customers' data and accounts."

Since its establishment in 1982, INVESTBANK has built and maintained a reputation for providing customers with premium, personalized digital banking solutions and tailored customer service experiences. Committed to maintain and strengthen this reputation, INVESTBANK is determined to provide the highest level of security to ensure the peace of mind to their clients.

The security team at INVESTBANK vigilantly monitors for cybersecurity threats, including misuse of the bank's branding and critical customer data leaks. They're also responsible for protecting customers from social engineering and phishing attempts through fraudulent websites and preventing personal banking information from being leaked and sold on the dark web.

Jazmawi's team is under constant pressure to proactively detect and manage threats across this rapidly expanding ecosystem. Time is of the essence when it comes to detecting and resolving threats before they impact customers.

Actioning Threat Intelligence Automatically

Jazmawi and his team used to rely on open-source threat intelligence data. Although broad in scope, the data lacked accuracy and was often incomplete. It was extremely time-intensive to comb through the data and uncover quality information about relevant or pressing threats, making it challenging to mitigate vulnerabilities and take action.

"We lacked visibility into what was happening on the dark web," Jazmawi recalled. "Because of the acceleration of cyber threats in time and volume, we needed to respond to cyber threats quickly."

Mean time to respond (MTTR) is one of INVESTBANK's core KPIs, and reducing MTTR is a strategic priority for Jazmawi. It's one of the reasons they sought help from Recorded Future.

"With Recorded Future, we can mitigate cybersecurity risk, avoid unforeseen events, and take informed actions in response to evolving threats faster and more efficiently," Jazmawi said.

INVESTBANK quickly adopted the Recorded Future Intelligence Cloud, which collects, structures, and analyzes data from multiple sources—including the dark web, open web, and customer telemetry—and automatically surfaces actionable insights. With these insights, the INVESTBANK security team can immediately react to bad actors by updating or sending indicators of compromise (IOCs) to their endpoint detection and response (EDR) system and antivirus solution.

Automating Security Workflows with Splunk

Improved orchestration is key for improving response times and reducing the lift of cybersecurity tasks. INVESTBANK used Recorded Future's Splunk Integration to significantly decrease the time spent on alert investigation and response — from a couple hours per day to minutes.

"Some activities require us to manually search the source of the connection, perform investigations, and reflect the outcomes on our security devices like firewalls. The integration with Splunk means all this is done seamlessly without any human intervention," said Jazmawi.

> **"The tasks we used to accomplish in a day now take just a few minutes. In many cases, it only takes a few seconds to analyze the threat actor and block it if we find there's significant risk to the bank."**
>
> *Riyad Jazmawi,*
> *Head of Information Security, INVESTBANK*

The INVESTBANK security team streamlines security operations workflows using pre-defined playbooks, creating seamless connections between tools and information.

"This integration fills in the gaps we have in our security orchestration and automation strategy and provides new perspectives on how we integrate technologies to talk to each other seamlessly. This, of course, has a very useful outcome for our SOC, which manages the security of the entire environment 24/7." Jazmawi explained.

Recorded Future correlates and enriches internal data with external insights to accelerate threat identification, prioritization, and remediation. Uncovering details about the most relevant threats has significantly impacted the information security team's efforts. After switching to Recorded Future, Jazmawi's team reduced their mean time to respond (MTTR) by 80%.

Catching Malicious Domain Registration in Real Time

Like many financial institutions, INVESTBANK is vulnerable to abuse of its logo and threat actors impersonating its executive team. The open-source data Jazmawi and his team used before Recorded Future didn't provide reliable visibility into fraudulent domains or misuse of their brand assets. This lack of comprehensive information left the team in the dark about activity that could directly impact customers and damage their reputation.

The information security team started using Brand Intelligence, and now receive real-time notifications with detailed information whenever someone registers a domain with a name close to INVESTBANK. This information lets them identify malicious sites soon after they appear and issue a takedown request before customers have a chance to interact, jeopardizing INVESTBANK's reputation.

"Brand Intelligence allows us to stop an attack before it even starts," Jazmawi said. "We can also track instances of brand abuse more effectively and report that information to regulators and other banks in our region, which helps everyone in our sector."

Bad actors use the dark web to trade the data they steal from victims, so having visibility enables organizations to take the necessary action before criminal use. The INVESTBANK security team created many alerting and amplification use cases and now, whenever someone posts data belonging to INVESTBANK or their clients on the dark web, the team receives an immediate notification.

"Having visibility is crucial to INVESTBANK because we can protect our customers from social engineering attacks and stop any attempts to compromise their accounts or abuse card data," says Jazmawi.

> **"Working with Recorded Futures enables us to maintain our position in the market as a pioneer in innovative and secure digital services, increasing the trust of clients in our services."**
>
> *Riyad Jazmawi*

Getting Proactive Visibility into Zero-Day Attacks

As Jazmawi's team becomes more informed, they're also becoming more proactive. The next step for the information security team was to gain visibility into potential weaknesses and immediate notifications about zero-day exploits.

One of the biggest challenges at a fast-moving organization with many digital services is maintaining continuous awareness of vulnerabilities alongside new updates and releases. INVESTBANK relies on Vulnerability Intelligence from Recorded Future to turn that challenge into an opportunity.

> **"Vulnerability Intelligence provides access to a large database of exploits and vulnerabilities so that we can remit them faster and implement compensation controls until a patch is released."**
>
> *Riyad Jazmawi*

Recorded Future provides alerts about vulnerabilities not yet known to the public so the INVESTBANK team can take action to protect the organization's reputation. They also gain insights into threat actors' intentions and techniques so they can adapt quickly and fortify their defenses going forward.

Using Vulnerability Intelligence also reduces time spent dealing with new zero-day and critical vulnerabilities, saving up to two hours a day reviewing and taking action against vulnerabilities.

"Quality data and visibility at the sector level enabled us to emphasize and enhance the collaboration with other companies in the same sector in Jordan," Jazmawi said.

Proactively Understanding the Threat Landscape with Collective Insights

Every financial institution is vulnerable to cyber attacks, but there's strength in numbers. Recorded Future's Collective Insights capability allows INVESTBANK to consolidate detections and events from their security tools in a single dashboard, connecting threat data specific to their industry and region with data from within their organization. It enables the security team to correlate data and set priorities of action based on trends and patterns.

"Collective Insights has made it possible to connect the dots between the big picture of what's happening in the wild with what's happening in our organization to holistically understand our threat landscape. This kind of visibility helps us protect our clients better, and enables transparency and trust between INVESTBANK and our clients," Jazmawi said.

Through Collective Insights, the team can also contribute to the growing pool of cybersecurity insights, strengthening their sector's defenses.

A Collaborative Partner Who Supports a Strong Cybersecurity Strategy

INVESTBANK values partnership in all its customer relationships and expects its vendors to provide the same level of collaboration and support they extend to their clients. Recorded Future has proven to be a true partner to their clients by prioritizing client security and helping INVESTBANK bolster its defenses.

"Recorded Future is our trusted partner that we can rely on to support our cybersecurity strategy," Jazmawi said. "Their superior support and customer service really set them apart from their competitors. It's been a totally positive experience working with them and we will absolutely continue with this strategic partnership in the future."

With strengthened data protection measures in place, INVESTBANK continues to place stronger safeguards around sensitive information, ensuring clients trust their data is safe and can bank with even more confidence.