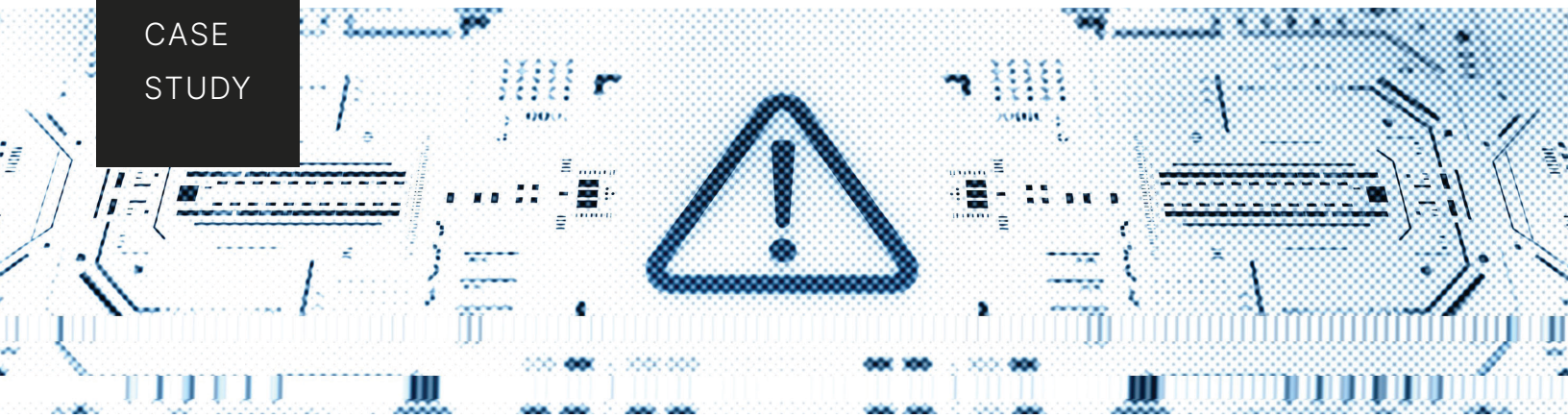
Recorded Future®

CASE STUDY



Bitdefender's MDR Threat Hunters Detect and Stop Threats Faster with Recorded Future®

Bitdefender

Use Cases:

Dark web monitoring; Threat hunting; Threat detection; Alert triage; Leaked credential discovery & remediation

Challenge:

Excessive time to detect and respond to cybersecurity threats.

Solution:

The Recorded Future Intelligence Cloud

Outcomes:

- Additional, actionable and trusted threat intelligence, integrated into existing security workflows
- Proactive, more efficient threat hunting
- Improved risk prioritization
- Advanced CTI function and capabilities

> "The amount of time and work that it saves to have additional threat intelligence aggregated into one place is a huge force multiplier"
>
> *Sean Nikkel, Lead CTI Analyst, Bitdefender MDR*

Every minute counts when dealing with a security incident. Unfortunately, with cybersecurity skills in high demand and short supply, many organizations lack the resources to stop attacks in a timely manner. That's why enterprises turn to Bitdefender for its managed detection and response (MDR) services, and why the Bitdefender team leverages Recorded Future, alongside Bitdefender's own threat intelligence for timely, actionable threat intelligence.

The cyber threat intelligence (CTI) team at Bitdefender's MDR service understands the importance of closing any gap that gives threat actors an advantage, and that means having the right expertise in the right hands at the right time. And while the CTI team uses a variety of useful internal tools and data including its own threat intelligence, as well as third-party tools, Recorded Future plays a key role in aggregating and correlating data for a comprehensive image of the threat landscape, while helping to validate or add context to internal and third-party data.

The two companies have a strong partnership as, Recorded Future incorporates some threat intelligence from Bitdefender feeds containing vulnerabilities, IP and Web resources reputation as well as operational insights into the Recorded Future Intelligence Cloud.

"The amount of time and work that it saves to have additional threat intelligence aggregated into one place is a huge force multiplier, and our main goal is to stay as far ahead of attackers as we can," says Sean Nikkel, lead CTI analyst for Bitdefender MDR.

A Complete Solution Enables a Faster Time to Market

Prior to launching the Bitdefender MDR service, the team evaluated several threat intelligence solutions on the market to find the one that best supported their use cases. Their main use cases included monitoring for exposed risks for MDR customers, validating internal data, and diving deeper into research and analysis.

"Recorded Future checked a lot of the boxes for the requirements we needed to get operations going — and everything was in the box, ready to go on day one," says Nikkel. "It is a useful platform because Recorded Future already has access on the dark web that adds deep context to our own insights in a scalable way, giving us visibility into a large number of sources, including a part of our proprietary threat intelligence. Using Recorded Future also addresses a top customer request to have dark web monitoring from an intelligence team."

> Recorded Future has bolstered the way we communicate among the different teams in an automated, repeatable way, enabling us to shave more time off the response"
>
> *Sean Nikkel,*
> *Lead CTI Analyst, Bitdefender MDR*

Intelligence Enables Proactive Risk Mitigation

Recorded Future's threat intelligence helps the Bitdefender MDR team proactively manage their customers' risk. "Awareness is the first step. It's understanding what's exposed and where, and how it can be used against you. Knowing these threats to our customers' environments helps us help them mitigate risk," says Nikkel.

By leveraging the platform from Recorded Future, the Bitdefender MDR team identifies gaps in its customers' environments and makes recommendations for proactively shoring up defenses to protect against active threats in the wild. The CTI team also leverages alerts to quickly detect threats. The infostealer malware logs, for example, provide timely information about identity compromises.

Within minutes of getting an alert for leaked credentials, the CTI team pushes notifications to customers through their security account managers and takes steps through proactive hunting to check for signs of compromise on potentially affected accounts. The Recorded Future Intelligence Cloud helps the Bitdefender MDR team act to protect their customers quickly.

Recorded Future Empowers Threat Hunters to Work Smarter

To ensure information gets to the right person at the right time, the CTI team leverages Recorded Future's APIs to integrate the intelligence feeds alongside other threat intelligence sources into Bitdefender's SOAR. When there's an alert, the intel team opens a research case and pushes that into a ticket for the SOC or customer success team. "Recorded Future has bolstered the way we communicate among the different teams in an automated, repeatable way, enabling us to shave more time off the response," says Nikkel. Integrations have helped the CTI team continue to refine processes as new additional capabilities from the Recorded Future platform are introduced, and the CTI team plans to continue building more.

This view also helps Bitdefender's team uncover external risks that customers wouldn't otherwise be aware of. This includes shadow IT, like code for a discontinued project on a GitHub page, or a recently registered domain that resembles the customer's domain.

Prioritization is critical for threat hunters and security analysts to protect a wide range of customer environments. While many intelligence feeds offer good information, Nikkel says, they often lack context to help drive action.

"Recorded Future allows me to gain access to extra contextual information," says Nikkel. "This data helps me understand where I need to prioritize versus just receiving a dump of 70 indicators that lack context."

Together with the existing intelligence sources, the information in the Recorded Future Intelligence Cloud helps facilitate the threat hunting process, as well as incident response. The CTI team can research potentially malicious indicators to find out more about them through Recorded Future and enable the SOC's investigation and assessment.

The end result is a more mature CTI function that benefits Bitdefender MDR's threat hunters and customers. "When you have an intelligence feed where things are repeatable and scalable, you can easily find context and additional information to help you with your investigations. All these capabilities have helped mature our team's processes and provided better outcomes for our customers," says Nikkel.