Recorded Future®

CASE STUDY

Aera Technology Shifts to Proactive Security Posture with Intelligence from Recorded Future®

Aera Technology eliminates false positives and focuses its security efforts on the most pressing threats.

Aera

USE CASE

- Leverage intelligence to build proactive security posture

CHALLENGE

- Having to vet too many false positives slowed the team down, and diverted efforts away from higher-value security program initiatives

SOLUTION

- The Recorded Future Intelligence Platform, SecOps module

OUTCOMES

- Aera's security team cut the time to investigate false positives to zero, saving hours a day
- Automate specific web application firewall security rules
- Security team can spend more time on strategic aspects of their security program
- Shortened time, and in many cases automated, time to mitigation
- Real-time, trusted threat intelligence keeps security posture ready for current and evolving threats.

Better Visibility Enables Better Decisions

Security teams everywhere find themselves in a constant battle to stay ahead of the latest threats. Unfortunately, the amount of threat data generated daily overwhelms internal teams. There's too much data to consume, ingest, and distill down into intelligence that can be put to immediate use. To solve this challenge, Aera Technology turned to Recorded Future for the trusted intelligence that would help its security team keep its defenses aligned with threats in near real-time and to eliminate false positives it was being forced to validate constantly.

Aera Technology is bringing the self-driving enterprise to life. Since its founding in 2014, Aera Technology has dedicated itself to delivering its cognitive operating system that seamlessly integrates with enterprise business-technology systems so that enterprises can execute better real-time business decisions. Armed with these AI-driven insights, Aera Technology's customers can now respond to rapid digital transformation more effectively.

"We're enabling organizations to be more proactive in doing business right through better insight," says Cosmin Anghel, security operation center manager at Aera Technology. Protecting their data, systems, and proprietary information is crucial to Aera Technology's long-term success. "We are an innovative and forward-thinking company, and we want to innovate in security, too. We don't want stagnant security controls in place. We want to be able to stop incidents before they happen. A breach for us would be significant, whether impact, costs, or potential loss of reputation," says Anghel.

With that need to protect their systems and data, Aera Technology and its five-member security team built a robust and mature security practice. "We are covering 360 degrees of our environment," adds Anghel. The security team at Aera Technology wanted to grow more efficient and proactive toward threats and continuously calibrate their systems to an optimal security posture.

The best way for the Aera security team to get that efficiency, explains Eduard Ungureanu, security operations engineer at Aera Technology, was to integrate intelligence into their processes to improve their visibility into the most current threats.

Using Intelligence to Stay Ahead of Pressing Threats

The team was dealing with lots of alerts that were proving time-consuming to verify. What's more, the team could not deploy defensive updates and mitigations quickly enough. "We didn't want to block valid traffic or transactions, so we had to manually validate everything before we could update our systems, such as our web application firewall," explains Ungureanu.

This occurred dozens of times a day, and it also cost the security team hours each day prioritizing follow-up. "We simply needed to move faster, much faster," says Ungureanu. "It's all about moving from reacting to security threats to preventing them, and also being able to correlate threat information with our environment," says Anghel.

Intelligence Streamlined into Existing Workflows

That's why, to get the intelligence the team sought, Aera Technology turned to Recorded Future. The Recorded Future Intelligence Platform delivers accurate and actionable real-time intelligence at scale. The modular platform combines automated analytics with human expertise to unite an unrivaled variety of open source, dark web, technical sources, and original research.

By dynamically categorizing, linking, and analyzing intelligence in real-time, the platform delivers the Aera Technology security team easy-to-consume insights for proactive and persistent risk mitigation. The Recorded Future Intelligence Platform scours an unrivaled quantity and variety of open, dark web, and technical sources in real-time.

That included access to intelligence within the web portal, integrations, a mobile app, and a browser extension. "Recorded Future was effortless to work with, and a key example is our ability to use our current procurement processes and purchase through AWS Marketplace, making it quick and easy to move forward," says Anghel.

The implementation went smoothly, and the team found it straightforward to quickly correlate intelligence with their current business-technology environment and security posture.

As Ungureanu explains, the team used Recorded Future's SIEM Integration to bring Recorded Future's intelligence into their SIEM. The team also integrated Recorded Future intelligence with their web application firewall from Signal Sciences so that IP addresses that have a substantial risk score can be automatically blocked.

"The integration worked flawlessly with our SIEM tool and our web application firewall," Ungureanu says. "When an alert comes in, we can look at it and swiftly prioritize our response based on Recorded Future's confidence level," adds Anghel.

The trusted intelligence coupled with Recorded Future's integrations mean the time previously spent chasing false-positive alerts (about 15 minutes per alert, with dozens of alerts daily) is slashed to zero. All of that time is now invested in much higher value security initiatives.

Automating, Prioritizing Response with Intelligence

The security team now responds more rapidly, if not automatically mitigates, the threats arriving within security alerts across the board. In addition to the automated web application firewall responses, the team also uses such information to prioritize their patch management efforts based on real-time intelligence.

"Recorded Future enables us to leverage threat intelligence within our day-by-day activities and makes it much easier to identify the right way to protect our organization and keep an effective security posture," Anghel says.

The need for intelligence never stops. Because attackers are constantly changing what they target and how they target enterprises, the stream of up-to-the-minute intelligence to security teams must be continuous. "We are always using threat intelligence to tune our security environment. Recorded Future provides us the visibility we need to maintain a strong security posture," Anghel says.

> Recorded Future enables us to leverage threat intelligence within our day-by-day activities and makes it much easier to identify the right way to protect our organization and keep an effective security posture,"
>
> Cosmin Anghel
> Security Operation Center Manager, Aera Technology