Recorded Future®

CASE STUDY

# Recorded Future® Provides Daimler the Trusted Intelligence They Need to Effectively Manage Risk

Daimler leverages threat intelligence to reduce risk and improve security operations.

DAIMLER

### USE CASE

- Improve threat intelligence capabilities to help offensive and defensive security teams, security architects, and identity and access management teams make better risk-based decisions.

### CHALLENGE

- Previous threat intelligence did not provide sufficient context to enable security teams to make decisions quickly and with confidence.

### SOLUTION

- Threat Intelligence
- Brand Intelligence
- SecOps Intelligence
- Vulnerability Intelligence
- Splunk Integration

### OUTCOMES

- Meaningful, trusted threat intelligence
- Unique natural language processing capabilities
- Efficient, rapid onboarding
- Seamless integration with the existing security stack
- Shift to proactive, more efficient threat hunting
- Reduction of false-positives
- Continuous monitoring for third-party cybersecurity risks
- Proactive defense against ongoing campaigns by integrating with Splunk

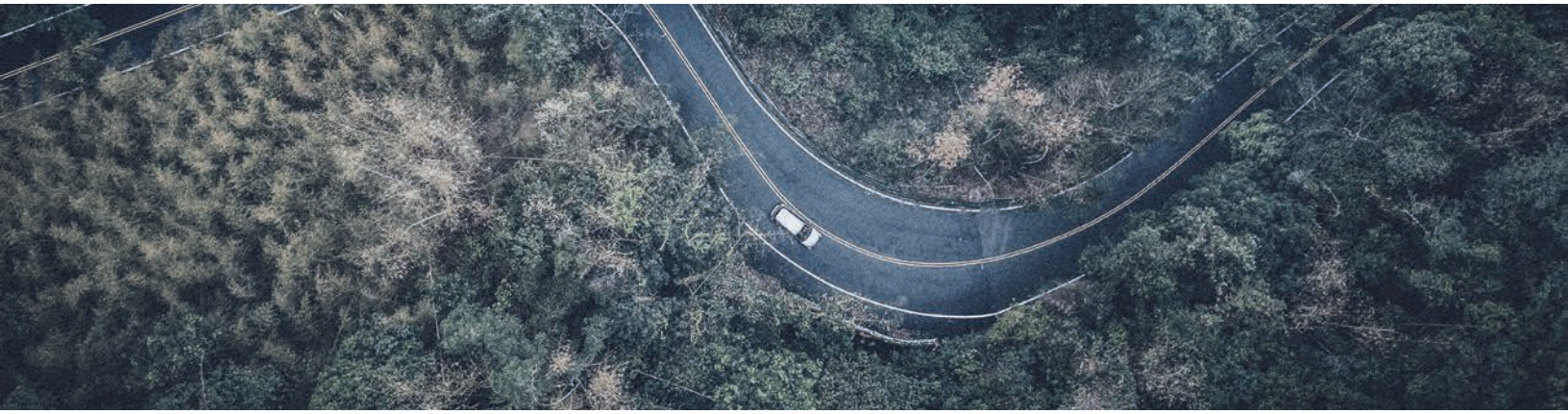
With 290,000 employees, annual revenue of €154.3 billion, and a product footprint in nearly every nation in the world, few companies have a global presence — and a digital attack surface — as big as automotive giant Daimler AG. Daimler has dedicated security teams based in Germany, Israel, the Asia-Pacific (APAC) region, and Canada to protect its data, systems, and brand.

As general manager of the APAC Cybersecurity Hub, Terence Lau leads cybersecurity for Daimler's APAC region. Recently, Lau set out to improve the cybersecurity threat intelligence capabilities in his region. "We are steadfast in improving our threat intelligence gathering and contextualizing that intelligence because our threat landscape is vast," says Lau. Lau turned to Recorded Future to get the contextualized threat intelligence Daimler needed.

Recorded Future's threat intelligence is used to help guide all of Daimler's security teams, including its blue team, red team, and security architects, and to help inform its identity and access management efforts. "Recorded Future's contextualized threat intelligence is critical across the security organization," adds Lau.

## Why Daimler Chose Recorded Future—Expertise, Context, and Customization

Lau relied upon Recorded Future at a previous employer and was familiar and impressed with the capabilities of Recorded Future's Intelligence Platform. "I knew Recorded Future could help us obtain meaningful threat intelligence. They have experts that will accurately place the raw indicators of compromise (IOCs) into context," Lau explains. Lau adds that Recorded Future provides natural language processing capabilities he couldn't find elsewhere. "We want to make sure that, for instance, any threat that is articulated in Farsi, in Hebrew, in Chinese, can be contextualized for our environment. Recorded Future does that," he says.



Lau selected Recorded Future not only because its threat intelligence would improve their overall security posture, but also provide deep and comprehensive access to the dark web and criminal underground, and straightforward integration with their existing tools and workflows. "Recorded Future's capabilities to look into the deepest corners of the internet help us to substantiate our internal team's threat intelligence and even enhance their proactive threat hunting capabilities," he explains.

Further, Recorded Future shares its internal repository for Daimler to customize to their needs. "Typically, intelligence companies keep their internal repositories confidential and don't share with customers. Recorded Future not only provides finished intelligence but also the raw intelligence," Lau says. "That is very important to us. Our stakeholders have lots of different concerns, and not everything in the raw intelligence may make it into the finished intelligence. But with the internal repository, we can make that decision for ourselves," he adds.

## Seamless Integrations and Efficient Processes Lead to Rapid, Straightforward Implementation

The onboarding process was fast and smooth for Daimler. Recorded Future ensured that Lau and the team had access to all of the functionality they needed and the knowledge to use it. "Recorded Future excelled at getting our program established. That's not an easy task. Daimler has a lot of stakeholders who all have a lot of requests. But even before the deal was closed, Recorded Future was very active in supporting us and ensuring our needs were met," Lau says.

One of the main reasons the deployment went so efficiently, explains Lau, is Recorded Future's established processes for onboarding new customers. "Their team helped us ensure we were using Recorded Future's intelligence in the best possible way, including suggesting what we should monitor so that we covered more entities," he explains.

Recorded Future integrates seamlessly with Daimler's existing systems; Lau and the security team were able to put that intelligence to work within their environment straight away. Recorded Future's APIs make it straightforward for Daimler to automate their intelligence with their most essential security applications. That includes their security information and event management system, security orchestration, automation and response platform, endpoint response applications, analysis tools, and more.

The combination of relevant threat intelligence, IOCs with accurate context, extensive dark web access and seamless integration with the company's security tech stack, enabled Daimler to proactively improve their security posture in an effective manner.

## Proactive, More Efficient Threat Hunting

Recorded Future provides the context Daimler requires to make decisions quickly and with confidence. "Recorded Future arms our analysts with the intelligence they need to understand threats, such as when given an indicator they also see a corresponding risk score," he explains.

Lau's team also integrates the intelligence with analysis tools, such as Splunk, to enable even more context and clarity for threat detection and swifter response — as well as the ability to dismiss false positives. "The API helped us contextualize a lot of things within Splunk, and additionally set up monitoring rules of Recorded Future's internal repository," he says.

Recorded Future provides the context that enables Daimler to quickly and confidently eliminate false positive alerts. Lau explains. "The reduction or the elimination of false positives is very critical. When tools produce a high number of false positives, they must all be investigated. That means real pressing incidents may be overlooked."

Lau and the team quickly appreciated Record Future's dynamic, evidence-based risk scoring of IOCs. Other vendors claim to have millions of IOCs, but their risk evaluation of the IOCs remains stagnant. "One's indicators change daily. Recorded Future is the company that provides a reliable risk matrix, with a very comprehensive indicator aging policy because it reflects the current situation and risk," Lau says.

Furthermore, Recorded Future's Threat Hunting Packages make it easy for the security team to perform proactive threat-hunting in their own environment. Lau explains that the team can use Recorded Future's hunting packages in combination with their Splunk monitoring to ensure that the new IOCs are not present in their environment. "This enables us to defend against ongoing campaigns more proactively and shortens the typical dwell time of advanced persistent threat actors," he says.

## Risk-Based Decision-Making Even Outside the Organization

Recorded Future also helps Daimler to monitor third-party cybersecurity risks. Lau explains, "The team uses Recorded Future to monitor the cyber risk scores of our critical third parties. This enables us to identify threats and mitigate risk in a timely manner."

Finally, Recorded Future has enabled Daimler's security operations to shift into being proactive and intelligence-led, rather than only reacting to alerts as they arrive. "Intelligence plays a heavy role in what we can do as an organization with our defensive and offensive operations and also help our stakeholders to contextualize and make smart, risk-based business decisions," Lau says.