Devo and Recorded Future

Cloud-native logging and security analytics meets enterprise threat intelligence

SOLUTION BRIEF

DEVO

+

Recorded Future®

PROACTIVE USE OF THREAT INTELLIGENCE IS CRITICAL FOR ANTICIPATING AND RESPONDING TO THREATS

Today's Security Operations leaders struggle to anticipate and respond to threats in an evolving landscape. To combat this, threat intelligence within SOC tools to speed identification, investigation, and triage of threats has become a critical component of a security strategy. The ability to quickly correlate your internal data against threat intelligence to detect, validate and identify threats is essential.

EMPOWER YOUR TEAM WITH CONTEXT TO MAKE CONFIDENT TRIAGE DECISIONS AND ACCELERATE INVESTIGATIONS

Joint Devo and Recorded Future customers are able to leverage a powerful integration to empower their team with context. By ingesting Recorded Future Threat Intelligence into the Devo Platform, organizations can enrich their alerts with context, directly inside of Devo minimizing manual research needed to investigate potential threats. Organizations are leveraging this integration to blend Recorded Future's machine-readable intelligence on IOCs, including IP addresses, domains, and file hashes, and pair it with log data from systems on their own networks.

Taking advantage of this powerful integration enables security teams to prioritize alerts, uncover unknown threats, and accelerate investigations to reduce the dwell time of potential cyberattacks. Additionally, the Devo and Recorded Future integrated solution improves SOC productivity by leveraging automation to reduce the amount of time spent in manual investigations and reduces analysts' alert fatigue by helping analysts focus on the alerts that matter the most.

USE CASES

Threat Detection

Detect threats with Recorded Future risk lists and identify potential threats.

Threat Hunting

Hunt with context for threats across all data, streaming and historical, with Devo DeepTrace. Devo DeepTrace helps security teams autonomously investigate alerts and perform proactive threat hunting by using an AI engine to ask and answer over 100,000 questions for the analyst to fully generate attack chains for you.

Threat Prioritization

Find and stop threats before they impact the business.

Alert Triage

Enrich alerts with threat intelligence from Recorded Futures, ensuring analysts have all the information they need to reduce time to verdict.

Joint Win: Multinational Chain of Retail Convenience Stores

PROBLEM

After a large acquisition, this Multinational Retail chain decided to move off of their on-premises Splunk deployment in order to help them better scale and consolidate into one cloud-native SIEM solution. Already working with Recorded Future, this team sought a modern SIEM solution that would integrate well with their current tech stack and enrich their threat hunting

SOLUTION

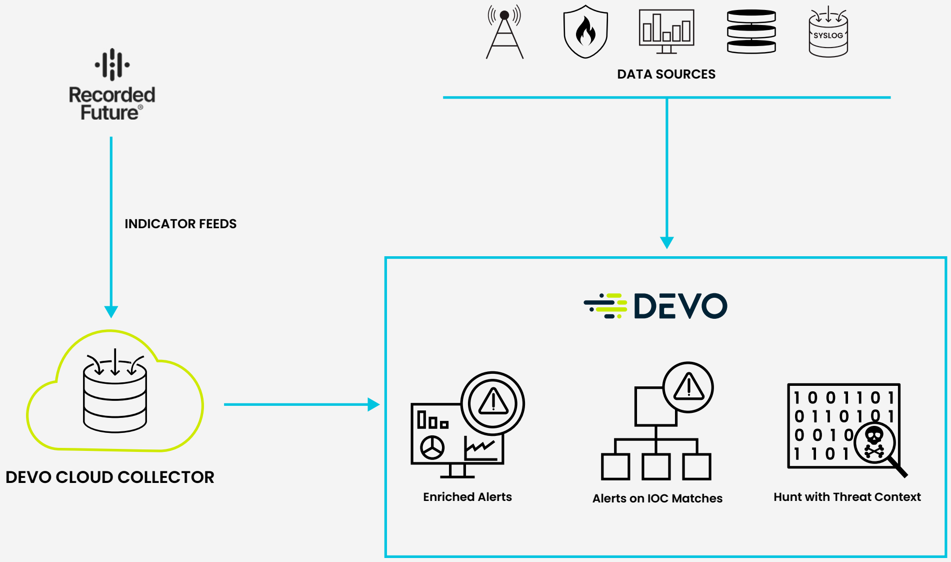
The customer selected Devo for the following reasons:

- Devo is a cloud-native solution that allowed the customer to make a seamless transition from on-premises to the cloud without compromising any of their preexisting data.
- Access to advanced alert triage. The Devo Platform is able to enrich alerts with Recorded Future intelligence to reduce time to verdict.
- The Devo Platform paired with Recorded Future's threat Intelligence provided the customer with a single pane of glass, consolidating multiple SIEMs to create a single source of truth and increase visibility across their teams.
- Access to a joint team from Recorded Future and Devo to help with anything they need during migration or deployment. Together, Devo and Recorded Future provide top tier support 24/7 to their joint customers.
- Devo and Recorded Future work together to provide the client with superior threat detection, detecting and gaining context on threats with real time external intelligence.

BOTTOM LINE

Devo and Recorded Future offer the client an advanced, modern SIEM solution with next level threat detection with the support they needed as they made the decision to migrate to the cloud.

ARCHITECTURE DIAGRAM



Devo customers with a valid Recorded Future license and API subscription can access this integration.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's Intelligence Cloud provides complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape. It empowers countries and organizations to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

THE BOTTOM LINE: WHY DEVO AND RECORDED FUTURE TOGETHER

This integration provides value across alerting and enrichment, enabling teams to reduce dwell time and mean time to respond through Recorded Future-provided intelligence.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.