Recorded Future®

JOINT SOLUTION BRIEF

Recorded Future and Devo

DEVO

ABOUT

Devo, the cloud-native logging and security analytics company, enables security and operations teams to realize the full potential of all their data to empower bold, confident action when it matters most.

Product Overview

Devo is a cloud-native logging and security analytics platform used to monitor and protect organizations, minus the complexity, performance and cost challenges.

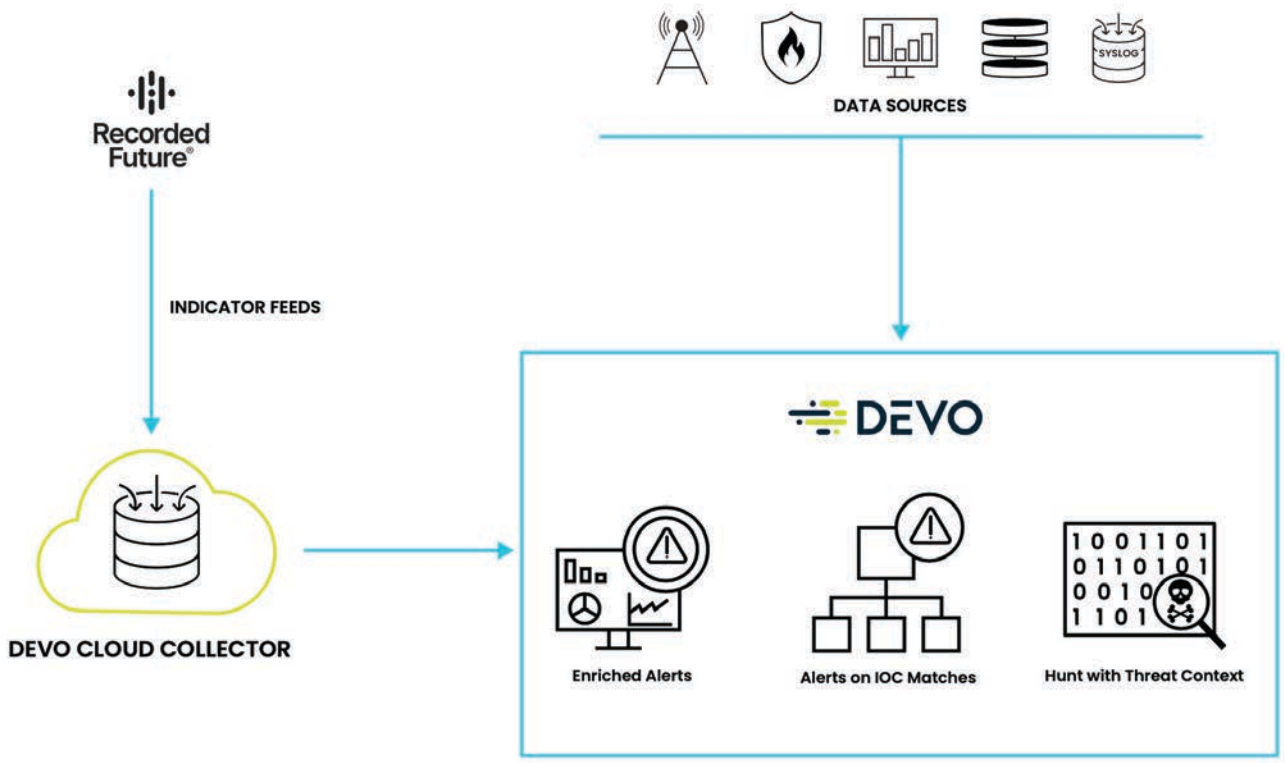
The Devo Platform enables security and operations teams to address common use cases including centralized logging, SIEM, compliance, fraud detection, and more. The Platform includes tightly integrated applications for security and IT teams.

Joint Integration Description

As the attack surface grows, security teams are seeing more and more events each day. However, with too little time and not enough context on the activity in their cloud environment, there's no way to connect the dots between data in their SIEM and the external risk of any detected threats. This slows responses and potentially enables relevant threats to slip through the cracks.

Our integration with Devo helps joint customers make informed decisions based on context from Recorded Future, through the use of Threat Lists containing enrichment information. This information is added to Lookup Tables inside of Devo, which includes IP Address, Domain, and File Hash entities, enabling:

- **Alerting:** The Recorded Future threat lists and resulting Devo lookup tables can be used to detect and alert on potential security threats through correlation with other data types ingested into Devo, for example, firewall, proxy, or EDR logs.
- **Alert Enrichment:** Threat lists also include additional contextual data about each entity enabling enrichment of security alerts.



Results

- **Reduce Dwell Time:** Correlation of Recorded Future Threat Intelligence and machine generated data from systems in the network security teams uncovers threats they would otherwise not know about and therefore reduce the dwell time of potential cyber attacks.
- **Reduce Mean-Time-To-Respond:** Joint clients get enriched alerts, helping to reduce the time required to complete triage and investigation of the alert in order to mitigate threats.

Use Cases

- **Threat Detection:** Detect and gain context on threats with real-time external intelligence
- **Threat Prevention:** Proactively block threats before they impact the business
- **Alert Triage:** Enrich with Recorded Future intelligence to reduce time to verdict

ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

www.recordedfuture.com @RecordedFuture