revelstoke™

Recorded Future®

Revelstoke + Recorded Future

Recorded Future for Revelstoke SOAR

Empower security teams and radically simplify the SOC. Security teams rely on SOAR platforms, but most are inherently complex and stop teams from doing what's important — stopping actual threats. Revelstoke radically simplifies SOAR so security teams can work faster, smarter, and more effectively. Revelstoke is the first low-code SOAR platform built on a Unified Data Layer, enabling teams to automate anything, respond to incidents fast, and show value to their executives.

With this integration, your teams can:

- ✓ Automatically flag on risky IOCs from alerts in your environment with real-time context from the Recorded Future Intelligence Cloud.
- ✓ Use real-time threat intelligence to reduce alert triage time.
- ✓ Identify high-risk alerts using Recorded Future Risk Scores, minimizing the time it takes to identify threats in your environment and for you to act before they impact business.
- ✓ Automate your processes with pre-built integrations and a library of pre-built workflows for all of the most common use cases.
- ✓ Use drag-and-drop workflow builders to configure your own workflows with minimal code.
- ✓ Use robust reporting to show the business impact of your security team's work.

Features

- Intelligence Cards for informed incident response investigation
- Access to Recorded Future's Portal for further research
- Pre-built workflows for common use cases
- Generate intuitive, on-demand reports for executives and other key stakeholders
- Investigate and respond to incidents in minutes, not hours

Use Cases

- Alert Triage
- IOC Enrichment
- Threat Detection
- Threat Prevention

**How Recorded Future clients use Recorded Future for Revelstoke SOAR
to operationalize threat intelligence in their SIEM:**

EASE OF USE

Connect and orchestrate your entire security stack enhanced by Recorded Future's data, in just a few clicks. Low-code configurations let you customize to your needs, without more hassle and headache.

AUTOMATION

Revelstoke acts as a force multiplier for high-performing security teams wanting to do more, faster. Automate analysis, optimize workflows, scale your processes, and get to the root of incidents quickly and effectively.

METRICS

Revelstoke delivers actionable, real-time insight from Recorded Future across the entire team — from the SOC analyst to the CISO — with the information needed to make smarter decisions.

CASE MANAGEMENT

Revelstoke delivers dynamic incident response case management to give you total control over a security event from detection through remediation and beyond. Gain a clear chain of custody, improve collaboration, and streamline your investigation workflows.

ARCHITECTURE

Revelstoke is built differently, with a Unified Data layer that forms the tracks upon which all integrations run. This revolutionary cloud-native architecture is what creates the flexibility to integrate anything and automate everything.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most 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 and empowers clients 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 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.