

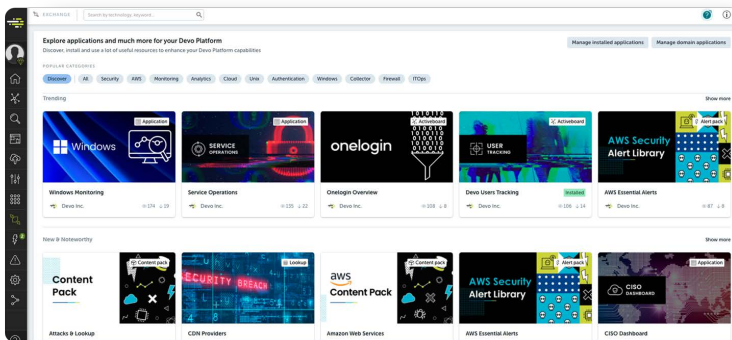
How a Financial Services Company Leverages Devo Exchange to Defend Their Organization



CASE STUDY

DEVO EXCHANGE

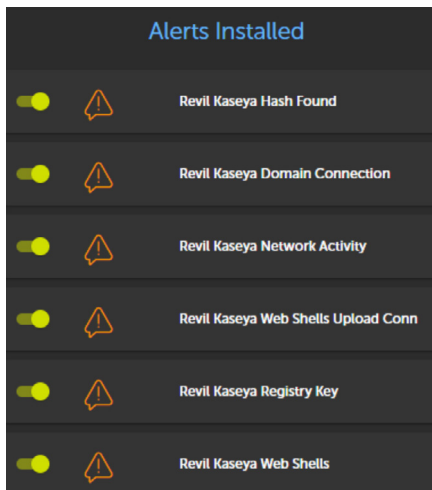
Devo Exchange, Devo's content marketplace, extends your security team capabilities by providing customers with valuable content. With Devo Exchange, customers can browse, install and manage a catalog of devo-curated content with push-button simplicity. Customers can access applications, alerts, Lookups, and Activeboards - all organized into convenient content packs. Devo Exchange is updated in real-time to help customers stay ahead of the latest threats.



Devo Exchange continuously delivers actionable security content

SUCCESS STORY: Devo Financial Services Customer

In response to the REvil Ransomware attack against Kaseya on July 3, 2021, Devo created a package of alerts and released them through Devo Exchange, proactively equipping our customers to detect indicators of compromise related to the attack.



Installed Kaseya alerts in Devo Security Operations

JULY 3, 2021

Kaseya detected a ransomware attack in its environment against the Virtual System Administrator (VSA)

JULY 8, 2021

Devo released six different alerts specific to the Kaseya attack through Devo Exchange

JULY 9, 2021 (a.m.)

Organization deploys alerts

JULY 9, 2021 AT 10:37 a.m. CENTRAL

Receives a hit from one of the alerts

“ One of the hardest things to do with a small team is balance everything that needs to be completed while also dealing with an ever-changing threat landscape. With Devo Exchange we can enable new alerts that help detect emerging threats with minimal impact on our analysts.

- Cybersecurity Operations Manager

Devo notifies customers when new alerts are available and this financial services organization took advantage of the notification. On the morning of July 9, 2021, the firm's cyber team deployed these alerts using Devo Exchange and **within a few hours** the team received a notification that one of the alerts fired. They quickly responded to the alert and remediated the threat.

"I see this as a massive win for our partnership with Devo," says the organization's cybersecurity operations manager. **"The ability to depend on Devo to produce alerts based on active threats is a great asset to the team. As a smaller team, it frees up our critical time and resources so we can focus on intelligence, hunting, and response."**

If the team had tried to create these alerts themselves, it would have taken multiple days to create, test, and tune them. The ability to seamlessly deploy these alerts via Devo Exchange saved the team days of work and multiple hours of analyst time. Instead, analysts were able to focus on other critical elements of their job.



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

© 2021 Devo All Rights Reserved

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.