confluera

INTEGRATION BRIEF

Confluera CxDR and Devo for Rapid Threat Detection and Response

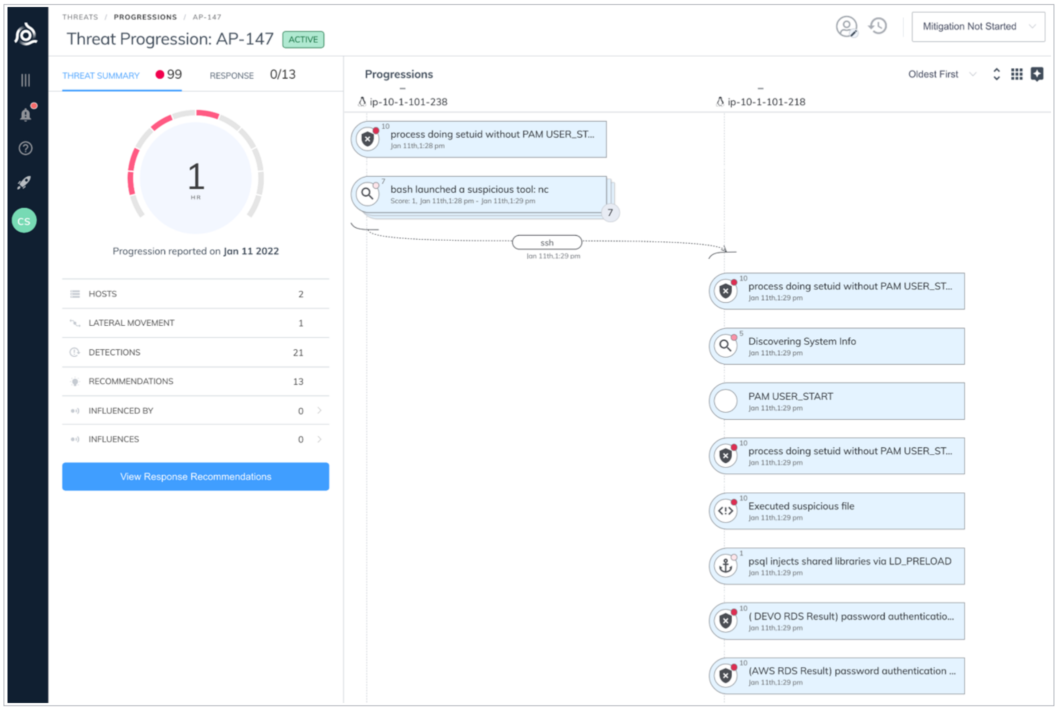
> Confluera CxDR integration with Devo's cloud-native logging solution enables organizations to expand Confluera CxDR's native security signals with external security signals for rapid threat detection, incident analysis, and response using Confluera's real-time threat storyboarding and observability capabilities for cloud workloads.

CHALLENGE: Devo's next-generation SIEM gives a centralized view of security events from multiple data sources by ingesting security events from a wide range of data sources such as Cloud logs, firewalls, EDRs, and other security tools. The security analysts, however, continue to struggle with manual and time-consuming investigations of security alerts. When investigating IOCs or multi-stage attacks with lateral movements, analysts are challenged to combine events across the different data sources quickly, and using a threat hunting approach becomes a time-consuming and tedious task.

SOLUTION: Confluera CxDR is a cloud-native detection and response platform built to protect VMs and container workloads in public and private cloud environments. It tracks threats progressing through your workload infrastructure in real-time, using its native signal collection. The integration with Devo's next-generation SIEM enables Confluera CxDR to ingest additional signals, automatically enriching its threat detection data. The result is more comprehensive context and visibility of activity sequences available in Confluera's threat storyboards.

Benefits:

- Speed up threat investigations
- Reduce false positives with enriched signals
- Minimize time-to-remediation
- Gain comprehensive context and visibility of activity sequences



THREATS / PROGRESSIONS / AP-147

Threat Progression: AP-147 ACTIVE

Mitigation Not Started

THREAT SUMMARY ● 99 RESPONSE 0/13

1 HR

Progression reported on **Jan 11 2022**

HOSTS	2
LATERAL MOVEMENT	1
DETECTIONS	21
RECOMMENDATIONS	13
INFLUENCED BY	0
INFLUENCES	0

View Response Recommendations

Progressions — Oldest First

ip-10-1-101-238

10 process doing setuid without PAM USER_ST... Jan 11th,1:28 pm

7 bash launched a suspicious tool: nc Score: 1, Jan 11th,1:28 pm - Jan 11th,1:29 pm (7)

ssh Jan 11th,1:29 pm

ip-10-1-101-218

10 process doing setuid without PAM USER_ST... Jan 11th,1:29 pm

5 Discovering System Info Jan 11th,1:29 pm

PAM USER_START Jan 11th,1:29 pm

10 process doing setuid without PAM USER_ST... Jan 11th,1:29 pm

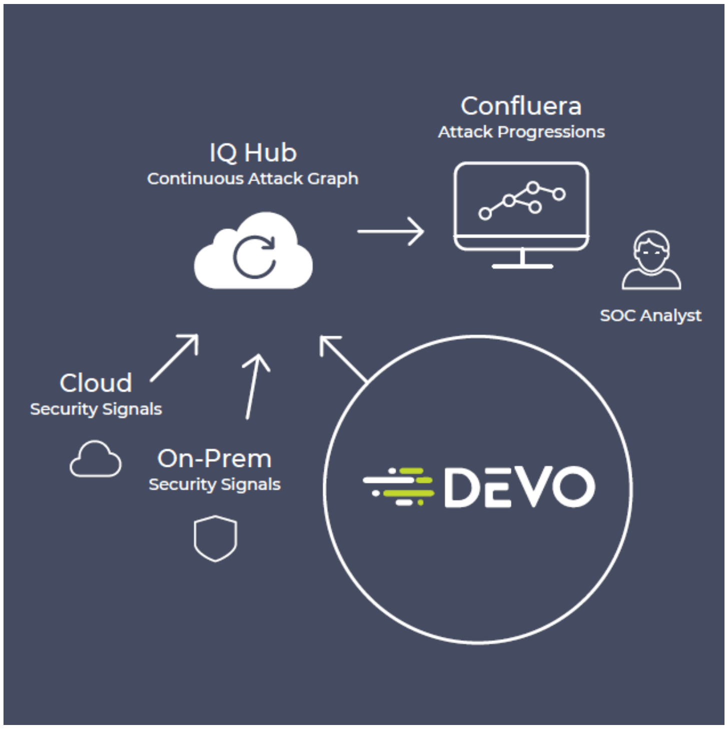
10 Executed suspicious file Jan 11th,1:29 pm

1 psql injects shared libraries via LD_PRELOAD Jan 11th,1:29 pm

10 (DEVO RDS Result) password authenticatio... Jan 11th,1:29 pm

10 (AWS RDS Result) password authentication ... Jan 11th,1:29 pm

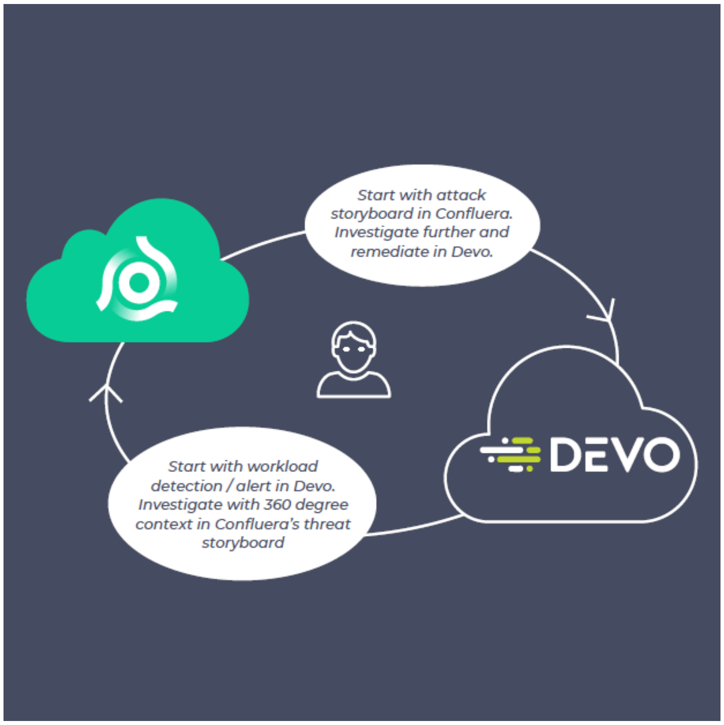
Simple Deployment



Devo's next-generation SIEM is configured as a signal source within Confluera CxDR. As Devo receives signals from the security tools, the signals are retrieved by Confluera's IQ Hub. The Confluera solution can be deployed as a SaaS service or on-premises.

Use Case

A security analyst can investigate alerts and events in Confluera's threat storyboards enriched with context from the ingested security signals from Devo. The threat storyboard enables the analyst to easily view the sequence of activities leading up to and following the event in real-time. No additional steps such as manual correlation are necessary. The security analyst continues to leverage existing processes put in place to carry out responses and remediation via Devo.


Start with attack storyboard in Confluera. Investigate further and remediate in Devo.
Start with workload detection / alert in Devo. Investigate with 360 degree context in Confluera's threat storyboard
DEVO

About Confluera Confluera is the only vendor that offers real-time sequencing of various attack steps found in modern cyberattacks. Confluera's patented machine learning technology automates the tedious and error-prone task of correlating events, removes the complexity of manual analysis of multiple systems, and provides a high degree of detection accuracy not previously possible. To learn more about Confluera's award-winning solution, visit www.confluera.com.