Devo + Detecteam: Engineering Confidence in Threat Detection

Automate detection engineering to stay ahead of evolving threats.

SOLUTION BRIEF

SECURITY OPERATIONS TEAMS CAN'T KEEP UP WITH EVOLVING THREATS

Security operations teams face an impossible task: creating, validating, and deploying threat detections to keep pace with rapidly evolving threats. Organizations struggle with the burden of manually managing outdated or poorly configured detections. Compounding the issue, scarce detection engineering expertise prevents teams from quickly operationalizng threat intelligence. As a result, they are unable to adapt to quickly emerging threats.

CASE STUDY

- **Industry:** MDR Provider, IoT/OT
- **Size:** 1000+ employees
- **Challenges:** New detections and defense validation took weeks to complete. The client needed a way to speed up the development, testing, and deployment of detections.
- **Outcomes:** Detecteam automated the detection engineering and validation process, reducing the time spent updating and testing per detection from hours to minutes.

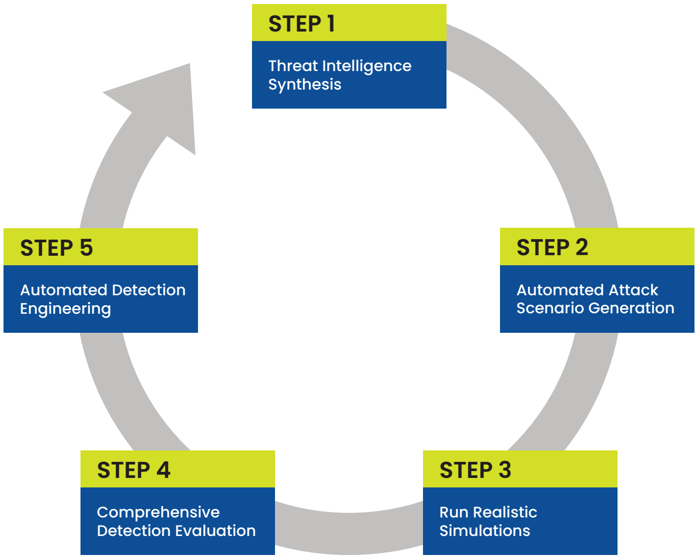
AUTOMATE DETECTION ENGINEERING WITH DEVO + DETECTEAM

Devo, the security data platform delivering real-time visibility for security operations, has partnered with Detecteam to revolutionize detection engineering. This integrated solution empowers analysts by:

- **Automating Detection Engineering** - Leverage AI to analyze threat data and produce new and improved detections.
- **Customizing scenarios to your ecosystem** - Ensure your threat detection is effective across each identity, network, and endpoint.
- **Rapidly deploying and validating new detections** - New detections are ready to deploy in hours, not weeks, and validation in as little as 15 minutes.

DEVO + DETECTEAM: HOW IT WORKS

1. Upload threat intelligence like advisories, CVEs or threat reports directly into Detecteam
2. Automatically turn the latest threat intelligence into customized attack scenarios.
3. Test your current detections against realistic attack simulations.
4. Validate defenses and identify gaps in detection with comprehensive detection evaluation.
5. Automatically generate new detections or improvements to existing ones based on identified gaps.



STEP 1
Threat Intelligence Synthesis

STEP 2
Automated Attack Scenario Generation

STEP 3
Run Realistic Simulations

STEP 4
Comprehensive Detection Evaluation

STEP 5
Automated Detection Engineering

UNLOCK ADVANCED THREAT DETECTION WITH DEVO + DETECTEAM

Experience a transformation in your security operations with these key benefits:

- **Proactive Threat Detection:** identify and remediate detection gaps before attackers can exploit them.
- **Continuous Validation:** Test detections against realistic attack scenarios to validate your defenses.
- **Rapid Threat Adaptation:** Turn the newest threat intelligence to validated detections in minutes, not weeks.
- **Close Expertise Gaps:** Automate detection engineering without needing specialized expertise.
- **Improve Security Metrics:** Improve MTTD/ MTTR and reduce breaches.

EMPOWER YOUR SECURITY TEAM WITH AUTOMATED DETECTION ENGINEERING

Devo and Detecteam partnered to create an integrated solution that automates detection engineering, continuously validates defenses against real-world attack scenarios, and proactively closes detection gaps. With Devo's real-time security insights and Detecteam's autonomic detection lifecycle, teams rapidly adapt to new threats, dramatically reduce detection deployment times, and measurably improve their security posture. Stay ahead of threats with validated, proactive, and continuously improving threat detection.

Don't let evolving threats leave you vulnerable. Schedule a demo today and discover how Devo + Detecteam can revolutionize your threat detection at devo.com/demo.

DEVO

Devo
3 Center Plaza
Suite 302
Boston, MA 02108

Devo Technology delivers a real-time security data platform that serves as the foundation of your security operations and includes data-powered threat detection, automated case management, autonomous investigations and threat hunting. AI and intelligent automation help your SOC work faster and smarter so your team can proactively make the right decisions in real time.