

SECURITY TEAMS ARE DROWNING IN ALERTS AND STRUGGLING TO RESPOND

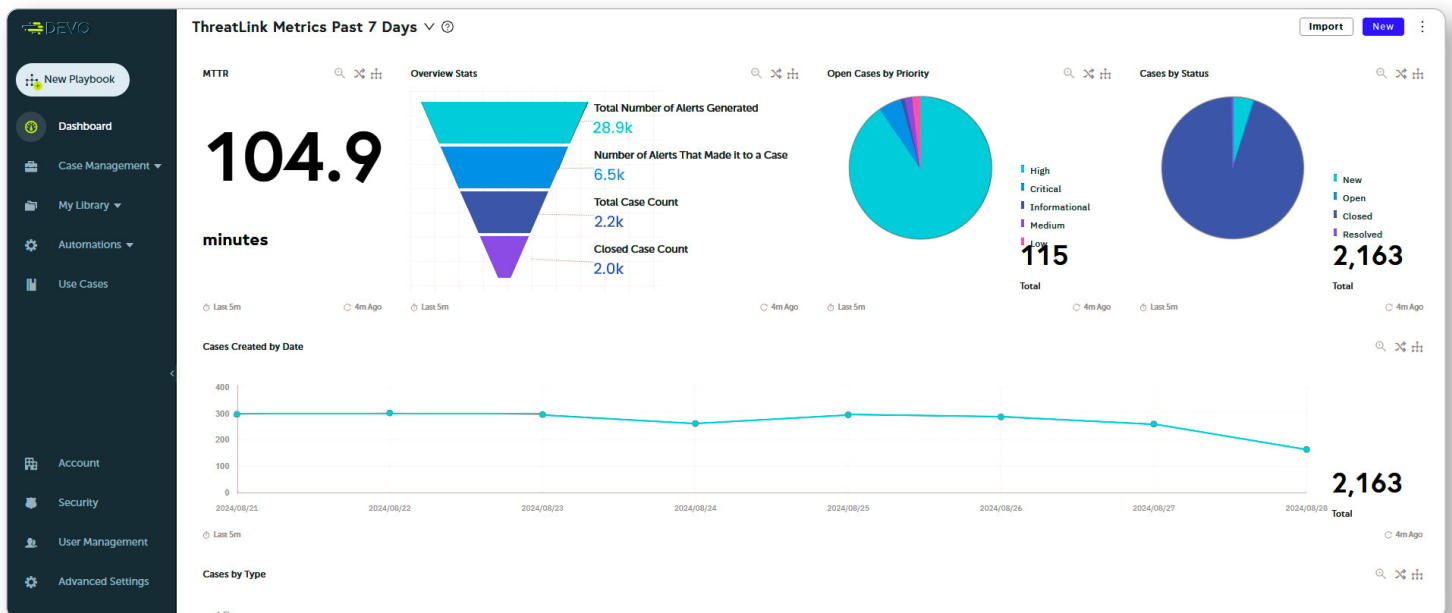
Security teams are drowning in a relentless deluge of security alerts, making it increasingly difficult to pinpoint and address critical threats. Manual alert triage and investigation processes consume valuable time and are prone to errors, resulting in missed threats and extended incident response times. Collaboration and knowledge sharing are often hindered by siloed tools and communication gaps, further complicating effective incident response. Moreover, the absence of clear performance metrics makes it difficult to document SOC effectiveness to stakeholders, impacting the ability to perform data-driven decision-making.

“ Since deploying Devo ThreatLink, our security team has seen a significant reduction in irrelevant alerts, enabling them to focus their time and energy on the threats that matter. ”

- Duane Hopkins,
Head of Global Cybersecurity, Carhatt

AUTOMATE CASE MANAGEMENT AND ALERT TRIAGE WITH DEVO THREATLINK

Devo ThreatLink is a centralized, automated case management solution that empowers security teams to efficiently navigate the complexities of incident response. A key element of the Devo Security Data Platform, ThreatLink automates alert triage, correlation, and enrichment, intelligently transforming a chaotic influx of alerts into manageable, high-fidelity cases. This significantly reduces analyst workload, enabling them to focus on critical threats. ThreatLink’s extensible automation streamlines workflows, facilitating swift and effective response actions. Additionally, its collaborative workspace fosters teamwork, while in-depth reporting provides valuable insights into SOC performance.



Devo ThreatLink empowers security teams with automated case management to combat alert overload and streamline incident response.

BOOST ANALYST EFFICIENCY WITH UNIQUE CAPABILITIES

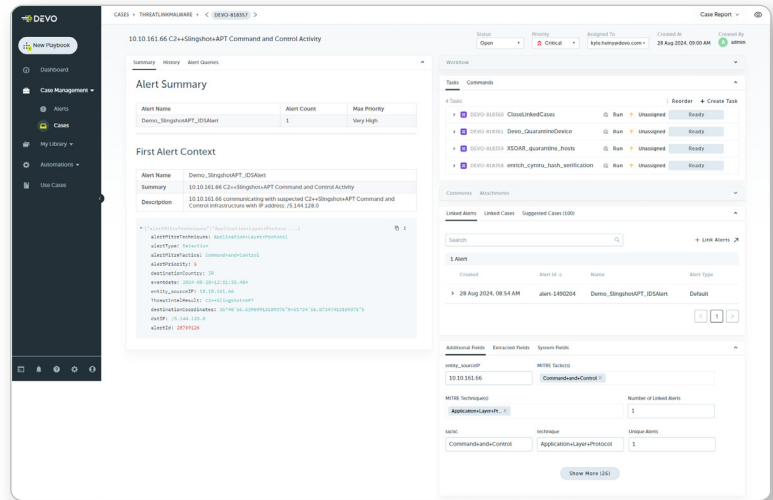
Devo ThreatLink equips security teams with the tools they need to efficiently manage and respond to security incidents:

Automated Alert Triage: Intelligently correlates and enriches alerts to generate high-fidelity cases, dramatically reducing analyst workload.

Extensible Automation: Integrates with existing security and IT tools to streamline workflows and enable swift response actions.

Collaborative Workspace: Provides a centralized platform for seamless team communication and knowledge sharing during investigations.

In-Depth Reporting: Documents incident response actions to quantify SOC performance and demonstrate value to stakeholders.



ThreatLink intelligently correlates and enriches alerts to generate high-fidelity cases, dramatically reducing analyst workload.

UNLOCK SECURITY OPERATIONS EFFICIENCY WITH THE DEVO THREATLINK ADVANTAGE

Experience a transformative impact on your security operations with the key benefits of Devo ThreatLink:

Reduced Level 1 Analyst Workload: Eliminate manual triage efforts and prioritize true threats.

Accelerated Threat Response: Reduce MTTR through automated actions and team collaboration.

Extensible Case Management: Seamlessly integrate with hundreds of existing IT and security tools.

Demonstrated SOC Effectiveness: Measure and document SOC performance to inform key stakeholders.

EMPOWER YOUR SECURITY TEAM AND EMBRACE THE FUTURE OF INCIDENT RESPONSE

Devo ThreatLink isn't just another tool in your security arsenal; it's a transformative automation that improves operational efficiency and threat response. By automating case management and improving collaboration, ThreatLink empowers your security team to rise above the alert noise and focus on what truly matters – safeguarding your organization.

Don't let alert fatigue hold your team back. **Schedule a demo today** and discover how Devo ThreatLink can revolutionize your security operations.



Devo
3 Center Plaza
Suite 302
Boston, MA 02108

© 2024 Devo All Rights Reserved

Devo replaces traditional SIEMs with a real-time security data platform. Devo's integrated platform serves as the foundation of your security operations and includes data-powered SIEM, SOAR, and UEBA. AI and intelligent automation help your SOC work faster and smarter so you can make the right decisions in real time.

Learn more at www.devo.com.