Devo Exchange

Extend Your Security Team with Community-Based Content

SOLUTION BRIEF

SECURITY ORGANIZATIONS STRUGGLE TO STAY AHEAD OF THEIR ADVERSARIES

The threat landscape is constantly changing. New threats and attack techniques appear daily, and existing attacks evolve continuously. To stay ahead of their adversaries, security teams need access to up-to-date security content and threat intelligence to stay informed about the latest threats and trends. But how can security organizations stay on top of such a dynamic environment?

Moreover, even with current information on attacks and threats, analysts lack sufficient context to understand the impact and full scope of an attack. Analysts need content that will provide the information they need to assess the severity and potential consequences to their environment of an attack. And finally, analysts are buried under an avalanche of alerts, far too many are false positives. Security teams need information that will help them prioritize and investigate threats more efficiently.

Devo Exchange's Community-Driven Content Helps Security Teams

Improve security posture by quickly and easily identifying and closing coverage gaps.

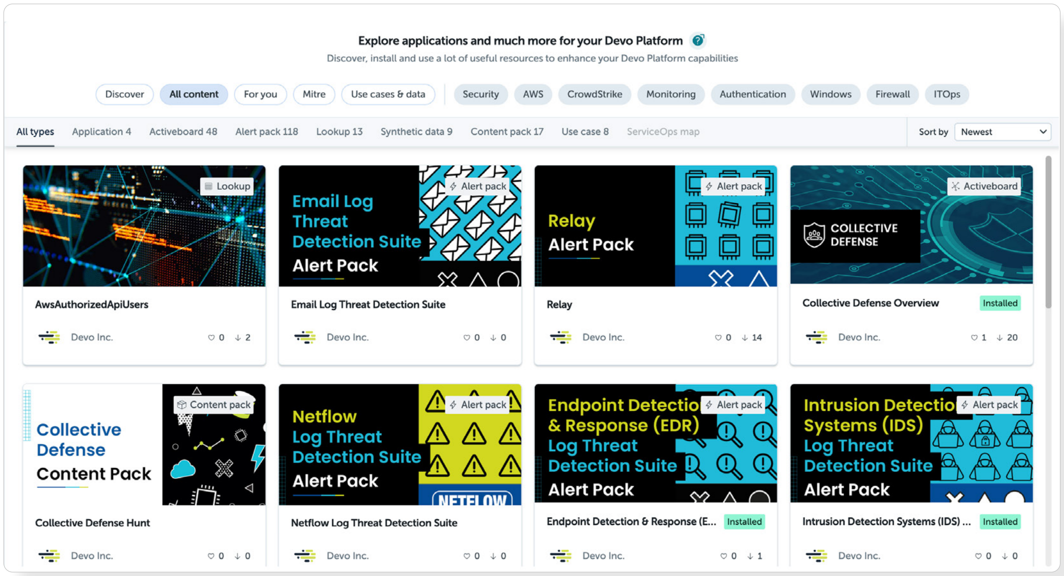
Outsmart attackers by protecting the organization from the techniques that threat actors commonly use.

Gain up-to-date knowledge of detection coverage across specific threat groups or across a collection of threat groups.

Deeply understand data across multiple platforms in a single location using Devo 360 apps and pre-built Activeboards, which are available for dozens of partners.

DEVO EXCHANGE LEVERAGES THE COMMUNITY TO HELP SECURITY TEAMS WORK FASTER – AND SMARTER

Devo Exchange, a key capability of the Devo Security Data Platform, is a comprehensive content marketplace for every Devo customer. It provides on-demand access to an ever-growing library of curated security content created by Devo, our partners, customers, and the greater security community. By leveraging relevant and vetted content, security teams accelerate the deployment of new use cases and detect malicious activity faster.



Explore applications and much more for your Devo Platform

Discover, install and use a lot of useful resources to enhance your Devo Platform capabilities

Devo Exchange provides access to curated security content.

WHAT CONTENT IS AVAILABLE IN DEVO EXCHANGE?

Expert-created security analytics: A collection of related alerts that enable customers to detect important signals within their data in real time.

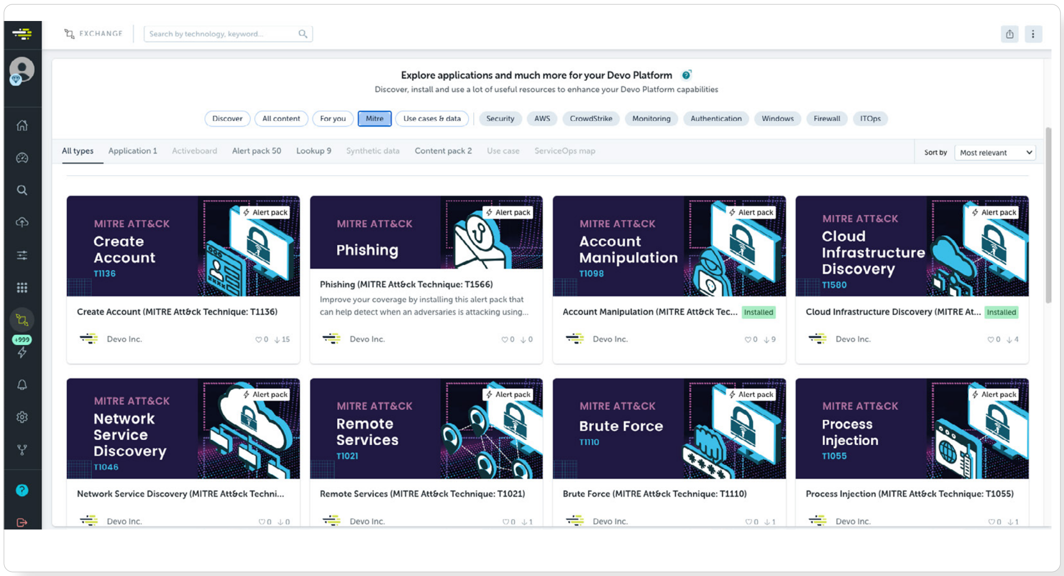
Dynamic visualizations: Devo Activeboards are intuitive, interactive dashboards that enable customers to visualize and explore their data easily.

Context enrichments: Provide real-time context to accelerate investigations and help analysts increase their understanding of threats in real time.

Content packs: Pre-packaged collections of related content centered around specific use cases, designed for quick and easy deployment to accelerate attack detection.

LEVERAGE ANALYTICS FOR WELL-KNOWN TECHNIQUES

Devo Exchange provides MITRE ATT&CK alert packs that can be directly installed into the user's Devo domain. Alert packs align with MITRE ATT&CK tactics and techniques, and technologies, so users can quickly identify security gaps in their workflow. Hundreds of alert packs are available, each with its own alerts, giving users complete control over how they deploy new alerts in their environment.



Explore applications and much more for your Devo Platform

Discover, install and use a lot of useful resources to enhance your Devo Platform capabilities

Create Account (MITRE Att&ck Technique: T1136) — Devo Inc. ♡0 ↓15

Phishing (MITRE Att&ck Technique: T1566) — Improve your coverage by installing this alert pack that can help detect when an adversaries is attacking using... — Devo Inc. ♡0 ↓0

Account Manipulation (MITRE Att&ck Tec... Installed — Devo Inc. ♡0 ↓9

Cloud Infrastructure Discovery (MITRE At... Installed — Devo Inc. ♡0 ↓4

Network Service Discovery (MITRE Att&ck Techni... — Devo Inc. ♡0 ↓0

Remote Services (MITRE Att&ck Technique: T1021) — Devo Inc. ♡0 ↓1

Brute Force (MITRE Att&ck Technique: T1110) — Devo Inc. ♡0 ↓1

Process Injection (MITRE Att&ck Technique: T1055) — Devo Inc. ♡0 ↓1

Devo Exchange provides alert packs for MITRE ATT&CK tactics and techniques.

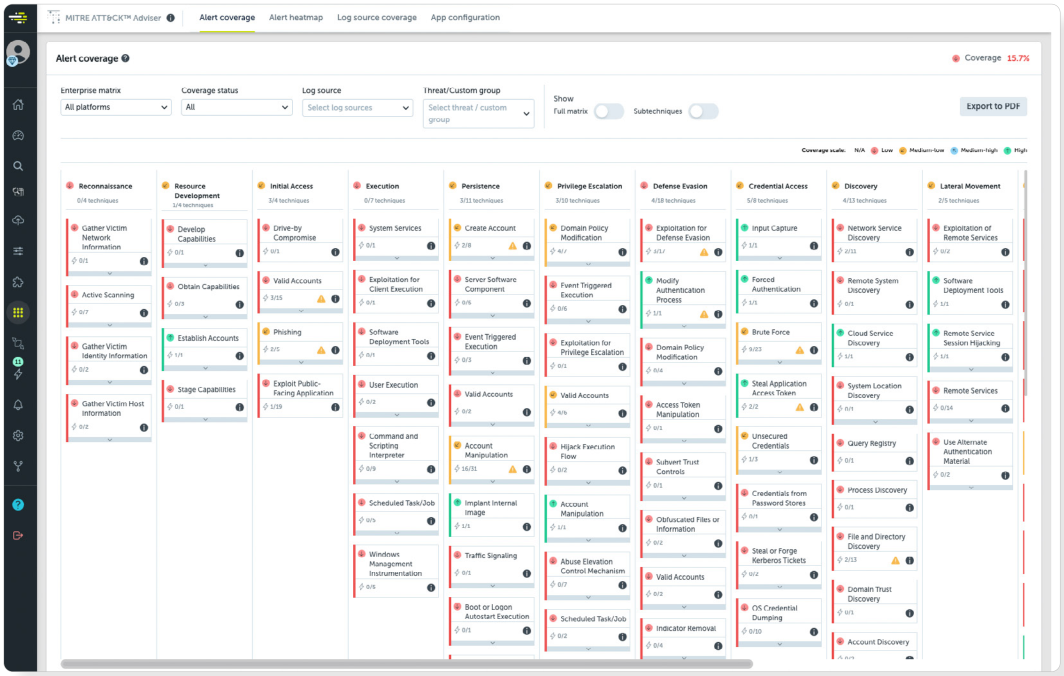
MAP ALERTS AND LOG SOURCES WITH THE MITRE ATT&CK ADVISER APP

The Devo MITRE ATT&CK Adviser application takes attack mitigation and security context enrichment one step further by correlating alerts and log sources with MITRE ATT&CK tactics and techniques:

Alert coverage map: Color-coded matrix maps alerts to specific MITRE ATT&CK techniques. Determining the coverage of alerts helps security teams identify gaps and vulnerabilities in their defenses.

Alert heatmap: The alert heatmap displays the concentration of triggered alerts per MITRE ATT&CK technique and tactic for a specific period of time. This dynamic view highlights the up-to-date activity and pinpoints the range of detection coverage while indicating which areas may be vulnerable to attacks.

Log source coverage: The MITRE ATT&CK app correlates the ingested log sources with the MITRE ATT&CK matrix, helping analysts maintain compliance and ensure a robust defense against threats.



MITRE ATT&CK™ Adviser — Alert coverage | Alert heatmap | Log source coverage | App configuration

Alert coverage Coverage 15.7%

Enterprise matrix: All platforms
Coverage status: All
Log source: Select log sources
Threat/Custom group: Select threat / custom group
Show: Full matrix ○ Subtechniques ○
Export to PDF

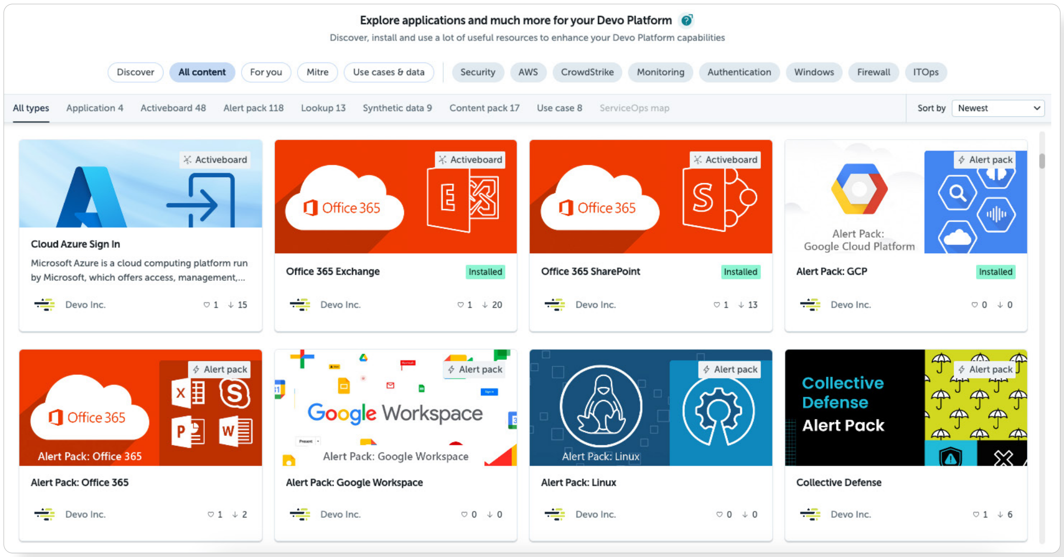
Coverage scale: N/A ● Low ● Medium-low ● Medium-high ● High

Reconnaissance 0/4 techniques	Resource Development 1/4 techniques	Initial Access 3/4 techniques	Execution 0/7 techniques	Persistence 3/11 techniques	Privilege Escalation 3/10 techniques	Defense Evasion 4/18 techniques	Credential Access 5/8 techniques	Discovery 4/13 techniques	Lateral Movement 2/5 techniques
Gather Victim Network Information 0/1	Develop Capabilities 0/1	Drive-by Compromise 0/1	System Services 0/1	Create Account 2/8	Domain Policy Modification 4/7	Exploitation for Defense Evasion 5/17	Input Capture 1/1	Network Service Discovery 2/11	Exploitation of Remote Services 0/2
Active Scanning 0/7	Obtain Capabilities 0/3	Valid Accounts 3/15	Exploitation for Client Execution 0/1	Server Software Component 0/5	Event Triggered Execution 0/6	Modify Authentication Process 1/1	Forced Authentication 1/1	Remote System Discovery 0/1	Software Deployment Tools 1/1
Gather Victim Identity Information 0/2	Establish Accounts 1/1	Phishing 2/5	Software Deployment Tools 0/1	Event Triggered Execution 0/3	Exploitation for Privilege Escalation 0/1	Domain Policy Modification 0/4	Brute Force 9/23	Cloud Service Discovery 1/1	Remote Service Session Hijacking 1/1
Gather Victim Host Information 0/2	Stage Capabilities 0/1	Exploit Public-Facing Application 1/19	User Execution 0/2	Valid Accounts 0/2	Valid Accounts 4/6	Access Token Manipulation 0/1	Steal Application Access Token 2/2	System Location Discovery 0/1	Remote Services 0/14
			Command and Scripting Interpreter 0/9	Account Manipulation 16/31	Hijack Execution Flow 0/2	Subvert Trust Controls 0/1	Unsecured Credentials 1/3	Query Registry 0/1	Use Alternate Authentication Material 0/2
			Scheduled Task/Job 0/5	Implant Internal Image 1/1	Account Manipulation 1/1	Obfuscated Files or Information 0/2	Credentials from Password Stores 0/1	Process Discovery 0/1	
			Windows Management Instrumentation 0/5	Traffic Signaling 0/1	Abuse Elevation Control Mechanism 0/7	Valid Accounts 0/2	Steal or Forge Kerberos Tickets 0/2	File and Directory Discovery 2/13	
				Boot or Logon Autostart Execution 0/1	Scheduled Task/Job 0/2	Indicator Removal 0/4	OS Credential Dumping 0/10	Domain Trust Discovery 0/1	
								Account Discovery 0/2	

The MITRE ATT&CK Adviser alert coverage map helps security teams identify gaps and vulnerabilities.

VISUALIZE AND INTERACT WITH YOUR SECURITY DATA

Devo Exchange provides visualizations and applications that are tailored for the key data sources that users ingest into the platform, including AWS, Crowdstrike, Palo Alto, Office365, GCP, Azure, Firewall, Proxy, G-Suite, and Linux.



Explore applications and much more for your Devo Platform

Discover, install and use a lot of useful resources to enhance your Devo Platform capabilities

Discover | All content | For you | Mitre | Use cases & data | Security | AWS | CrowdStrike | Monitoring | Authentication | Windows | Firewall | ITOps

All types | Application 4 | Activeboard 48 | Alert pack 118 | Lookup 13 | Synthetic data 9 | Content pack 17 | Use case 8 | ServiceOps map   Sort by: Newest

Type	Title	Description / Status	Publisher	Likes	Downloads
Activeboard	Cloud Azure Sign In	Microsoft Azure is a cloud computing platform run by Microsoft, which offers access, management,...	Devo Inc.	1	15
Activeboard	Office 365 Exchange	Installed	Devo Inc.	1	20
Activeboard	Office 365 SharePoint	Installed	Devo Inc.	1	13
Alert pack	Alert Pack: GCP	Installed	Devo Inc.	0	0
Alert pack	Alert Pack: Office 365		Devo Inc.	1	2
Alert pack	Alert Pack: Google Workspace		Devo Inc.	0	0
Alert pack	Alert Pack: Linux		Devo Inc.	0	0
Alert pack	Collective Defense		Devo Inc.	1	6

Office 365
Alert Pack: Google Cloud Platform
Alert Pack: Office 365
Google Workspace
Alert Pack: Google Workspace
Alert Pack: Linux
Collective Defense Alert Pack

Devo Exchange provides visualizations and applications that are tailored for key data sources.

These visualizations enable analysts, security engineers, and SOC managers to quickly:

Understand Security Data: Visualization helps analysts understand the security data coming from across your organization so they can ask valuable questions to improve security posture.

Correlate Disparate Sources: Gain a more comprehensive understanding of the threat environment by correlating data from internal and external sources to identify new threats and their impact on the organization.

Visualize Operational Flows: Measure operational workflows and improve MTTR using Activeboards to improve security processes.

Are you ready to learn more about Devo Exchange?

Contact your sales representative or visit Devo.com.

Devo
3 Center Plaza
Suite 302
Boston, MA 02108

Devo unleashes the power of the SOC. The Devo Security Data Platform, powered by our HyperStream technology, is purpose-built to provide the speed and scale, real-time analytics, and actionable intelligence global enterprises need to defend expanding attack surfaces. An ally in keeping your organization secure, Devo combines the power of people and AI to augment security teams, leading to better insights and faster outcomes. Learn more at **www.devo.com**.