

Devo Collective Defense

Identify and respond to emerging threats with community-based threat intelligence

SOLUTION BRIEF



ANALYSTS STRUGGLE TO UNCOVER BROADER THREAT TRENDS

In addition to the expanding threat landscape and the increased sophistication of attacks, analysts confront unique difficulties. They must not only contend with the overwhelming volume of threat data but also grapple with the uncertainty of knowing if what they observe is part of a broader threat trend. As a result, analysts often bear the burden of understanding the significance of isolated incidents within the ever-evolving threat landscape. They need a threat intelligence solution that provides superior threat context so they can take action with decisive confidence.

STRENGTHEN SECURITY WITH COMMUNITY-BASED THREAT INTELLIGENCE

Devo Collective Defense is a community-based intelligence-sharing program that provides knowledge of threat activity and trends exclusively to Devo customers and partners.



**SECURELY ANALYZES
ALERT DATA**



**IDENTIFIES
EMERGING THREATS**



**DELIVERS A HIGH-VALUE
INTELLIGENCE FEED**

Devo Collective Defense helps organizations detect emerging threats.

A capability of the Devo Platform, Collective Defense analyzes alert data from across the Devo community and identifies insights, trends, and Indicators of Compromise (IOCs) that analysts can act upon immediately.

- **Securely analyzes alert data** to rapidly identify actionable intelligence, trending threats, and IOCs.
- **Identifies emerging threats** by aggregating alerts, investigations, and contained threats, helping security teams better understand the evolving threat environment.
- **Delivers a high-value intelligence feed** to Devo users, providing information about emerging threats and vulnerabilities, minimizing the potential impact of breaches.
- **Enhances threat context** by providing Devo users with contextual information about the Tactics, Techniques, and Procedures (TTPs) employed by threat actors.

LEVERAGE REAL-TIME THREAT INTELLIGENCE FOR DATA-DRIVEN PROTECTION

Collective Defense automatically aggregates alerts, investigations, and contained threats across the Devo user community. Collective Defense provides users with a unique combination of up-to-date threat intelligence and pre-built content that helps security teams make data-driven decisions to effectively investigate and respond to threats.

Integrated threat intelligence feed

The Collective Defense threat intelligence feed is automatically updated with emerging signals seen across the Devo community. Relevant IOCs are automatically flagged based on their frequency across the Devo user community.

eventdate	entity_sourceIP	entity_sourceAccount	Workload	Operation	cd_hit
2023-09-25 12:15:00.000	101.206.109.159	bdabinett1@vital.com	AzureActiveDirectory	UserLoggedIn	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	101.206.109.159	bdabinett1@vital.com	OneDrive	FileDeleted	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	101.206.109.159	bdabinett1@vital.com	OneDrive	FileModified	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	101.206.109.159	bdabinett1@vital.com	SharePoint	FileAccessed	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	103.87.33.55	rtallant2@vital.com	AzureActiveDirectory	UserLoggedIn	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	103.87.33.55	rtallant2@vital.com	AzureActiveDirectory	UserLoginFailed	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	103.87.33.55	rtallant2@vital.com	OneDrive	FileAccessed	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	103.87.33.55	rtallant2@vital.com	SharePoint	FileAccessed	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	104.246.244.28	paspling1m@vital.com	AzureActiveDirectory	UserLoggedIn	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	104.246.244.28	paspling1m@vital.com	OneDrive	FileAccessed	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	104.246.244.28	paspling1m@vital.com	OneDrive	FileModified	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122
2023-09-25 12:15:00.000	104.246.244.28	paspling1m@vital.com	OneDrive	FileUploaded	{'sectors': ['Industrial'], 'Technology': ['']; entity': '109.122

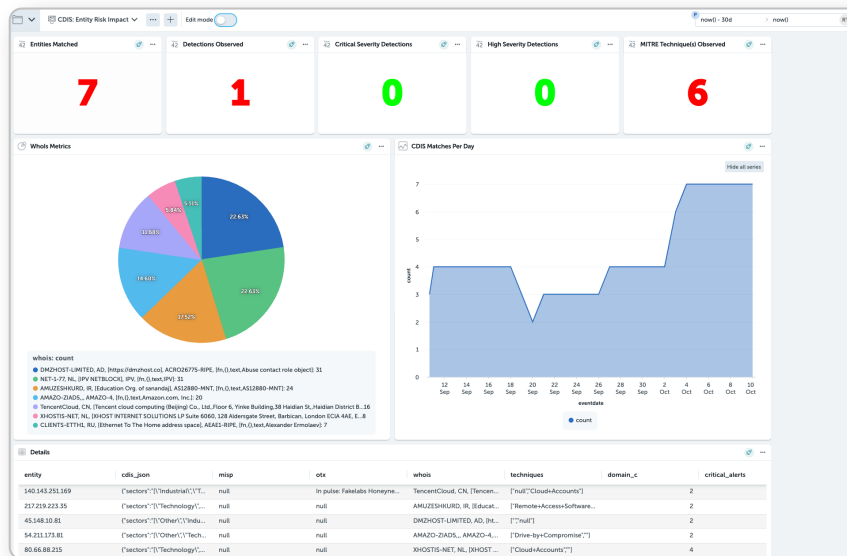
Collective Defense reports IOCs (filtered and aggregated to remove private data) based on community activity.

Collective Defense updates and communicates the latest threat intelligence to Devo users every six hours.

Out-of-the-box content

With Collective Defense, Devo users can identify emerging threats before they become significant incidents using pre-built content.

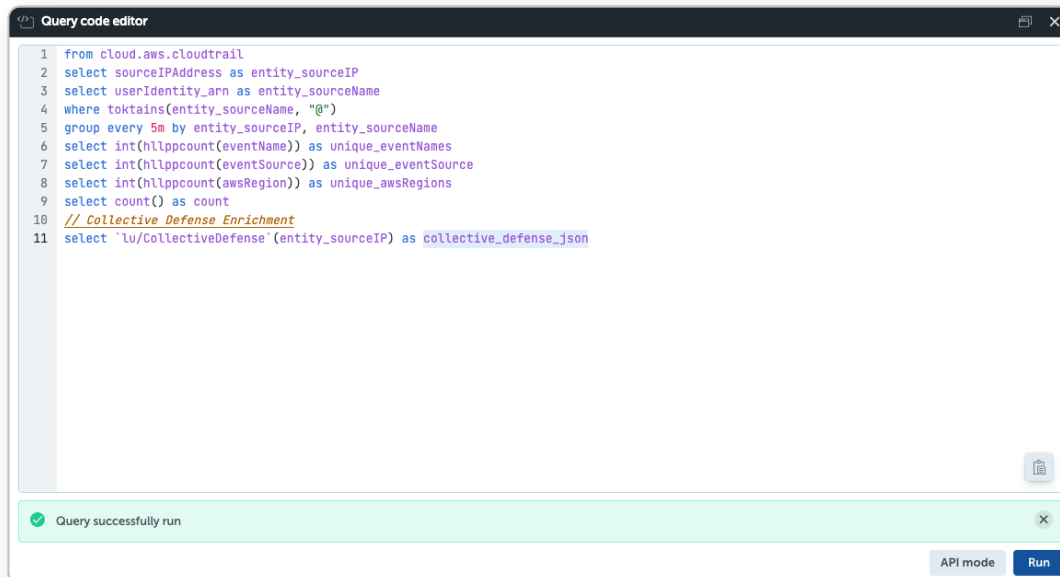
- **Alerts:** Collective Defense alerts detect malicious IOCs and identify risky entities within your organization.
- **Activeboards:** Devo Activeboards are intuitive, interactive dashboards that enable users to visualize, analyze, and explore data easily. Collective Defense Activeboards provide insights, patterns, anomalies, trends, threat hits, and findings.



Collective Defense Activeboards display insights so analysts can quickly track anomalous behavior.

Alert enrichment

Collective Defense includes a new multi-lookup that enables analysts to correlate entity data (i.e., IP, domain, URL, hostname, and file hash) against the Collective Defense feed to identify complex attacks.



```
1 from cloud.aws.cloudtrail
2 select sourceIPAddress as entity_sourceIP
3 select userIdentity_arn as entity_sourceName
4 where toktains(entity_sourceName, "@")
5 group every 5m by entity_sourceIP, entity_sourceName
6 select int(hllppcount(eventName)) as unique_eventNames
7 select int(hllppcount(eventSource)) as unique_eventSource
8 select int(hllppcount(awsRegion)) as unique_awsRegions
9 select count() as count
10 // Collective Defense Enrichment
11 select `lu/CollectiveDefense`(entity_sourceIP) as collective_defense_json
```

Query successfully run

API mode Run

Collective Defense context can be added to any Devo alert.

Devo users can enrich existing alerts to leverage information obtained by Collective Defense through these multi-lookups. For instance, analysts can quickly determine if Collective Defense has identified a known threat indicator by searching the IP address in a threat investigation.

REALIZE THE BENEFITS OF COMMUNITY-DRIVEN THREAT INTELLIGENCE

Collective Defense provides the Devo user community with an unprecedented collaborative intelligence program that improves their cybersecurity defenses and enhances expertise and efficiency within the organization. In turn, Collective Defense strengthens the security community as a whole, helping organizations survive and thrive amidst the ever-evolving threat landscape.

Are you ready to learn more about Devo Collective Defense?
Contact your sales representative to schedule a demo or visit devo.com



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

© 2023 Devo All Rights Reserved

Devo is the only cloud-native security analytics platform that combines the power of people and intelligent automation to confidently defend expanding attack surfaces. An ally in keeping your organization secure, Devo augments security teams with AI — enabling you to continuously scale SOC efficiency, increase the speed of threat detection and response, and gain greater clarity to empower bold action, minimize risk, and maximize outcomes. Learn more at www.devo.com.