

# Cloudforce One

Сбор и анализ информации об угрозах

## Получите беспрецедентную видимость угроз и экспертные знания

Сбор и анализ информации об угрозах имеет решающее значение для организаций, чтобы опережать возникающие риски, но сегодняшние команды часто сталкиваются с перегруженностью и нехваткой ресурсов.

Cloudforce One использует глобальные возможности Cloudflare по отслеживанию угроз, чтобы предоставить мощный пакет сбора и анализа информации об угрозах и экспертных знаний, который поможет вашей организации оптимизировать принятие решений, повысить скорость реагирования и уровень безопасности.

## Сбор и анализ информации об угрозах, созданный для действий

Cloudforce One помогает быстрее расследовать инциденты, реагировать на угрозы и уменьшать их число, предоставляя:

- **Доступ в реальном времени к информации о глобальных угрозах.** Получите доступ к тщательно отобранному данным об угрозах из глобальной сети Cloudflare, включая домены, IP, инфраструктуру Фишинга и запись DNS, каждое из которых сопоставлено с тактиками, техниками и процедурами (TTP) злоумышленников.
- **Индивидуальные исследования угроз.** Отправляйте собственные RFI аналитикам Cloudforce One для получения структурированных отчетов об атакующих, инфраструктуре, вредоносном ПО и т. д.
- **Встроенные операционные инструменты.** Изучайте индикаторы, отслеживайте злоупотребления брендом и принимайте меры непосредственно на панели управления Cloudflare для устранения угроз.



### Данные об угрозах в огромном масштабе

Около 20 % интернет-трафика проходит через Cloudflare, что обеспечивает уникальную возможность отслеживания триллионов сигналов об угрозах и позволяет выявлять атаки на самых ранних стадиях.



### Проверенный опыт в области защиты от угроз

Аналитики Cloudforce One обладают обширным опытом в анализе вредоносного ПО, отслеживании инфраструктуры и пресечении деятельности государственных и киберпреступных группировок.



### Превратите анализ в действие

Интеллектуальные функции изначально встроены в решения безопасности Cloudflare. Обнаружение угроз осуществляется посредством API-каналов, которые интегрируются с существующими рабочими процессами SOC и продуктами безопасности.

# Данные об угрозах, анализ и распространение

## Источники данных



## Платформа событий, связанных с угрозами

Cloudforce One преобразует большие объемы данных об атаках, обнаруженных в сети Cloudflare, в события, атрибутированные злоумышленникам и происходящие в реальном времени, которые важны для вашей организации.

- **Отслеживайте действия злоумышленников в масштабе** — включая инфраструктуру APT, группы киберпреступников, скомпрометированные устройства и объемную DDoS-активность.
- **Просматривайте подробные контекстные события** — включая интерактивные временные шкалы и подробные события, привязанные к тактикам злоумышленников, регионам и атакуемым вертикалям.
- **Внедряйте быстрее** — благодаря расширенным IoC, информации об объединениях злоумышленников и экспортируемому данным, которые можно использовать в рабочих процессах и инструментах.

Security Center  
**Cloudforce One Threat Intelligence**  
Observe threat intelligence data gathered by Cloudflare's global network and access critical intelligence from Cloudflare analysts.

Threat Events **New** Priority Intelligence Requirements Requests for Information

Threat Events **1**

Access and analyze threat intelligence data with this comprehensive, real-time view of cyber threats to protect your assets and respond to emerging threats.

Filter by: Attacker Attacker Country Target Country Target Industry TLP Indicator Type Dataset Kill Chain Tags

Event Category Date range Clear all

Date	Attacker	Indicator	TLP	Kill Chain	ATT&K Category	Attacker Country	Target Country	Target Industry	Event Summary
Jun 29, 2025 6:27 AM		141.11.107.191	●	1	RESEARCHED VULNERABILITY	IR	XX	-	Actor Researched
Jun 27, 2025 12:49 PM		141.11.107.191	●	1	RESEARCHED VULNERABILITY	IR	XX	-	Actor researched
Jun 25, 2025 8:46 AM		nato-summit...	●	2	ADDED DOMAIN	RU	XX	Government	Actor added the domain
Jun 24, 2025 8:48 AM		216.252.238...	●	2	DOMAIN RESOLUTION	RU	XX	Government	Domain resolves to
Jun 24, 2025 8:42 AM		nato-summit...	●	2	ADDED DOMAIN	RU	XX	Government	Actor added the domain
Jun 23, 2025 1:32 PM		216.252.238.9	●	2	DOMAIN RESOLUTION	RU	XX	Government	Domain resolves to