flare

AI Driven Threat Exposure Management

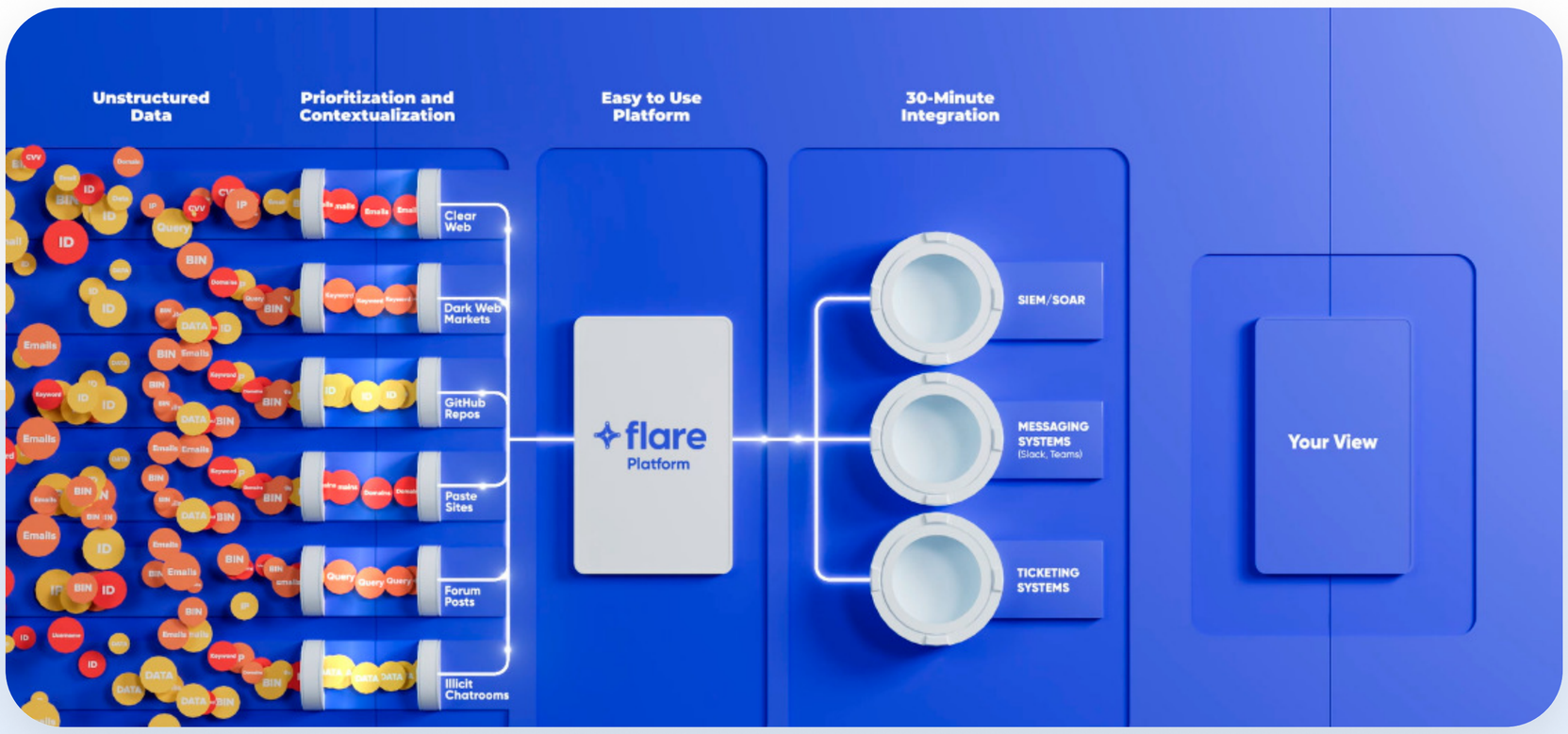
Flare's intuitive threat exposure management platform provides actionable intelligence from across the clear & dark web, and integrates into your security program in 30 minutes.

Today's visionary CISOs are embracing **threat driven cybersecurity programs**. Companies that successfully integrate real-time, actionable, threat exposure data are dramatically reducing the risk of major data breaches. According to Gartner, companies that base their security processes around continuous threat exposure management **will reduce breach risks up to 66% by 2026.**

> **What used to take about 1,500 hours to complete can now be done in one week.**
>
> -Senior Security Specialist
> North American MSSP

Continuous Detection and Remediation at Scale

Flare is transforming the cybersecurity landscape by delivering high-value, actionable threat exposure management tailored to your organization. Flare leverages AI to automate collection, structuring, analysis, contextualization, and remediation for events across hundreds of dark web forums and markets, thousands of Telegram sources, and millions of sources of risk across the clear web.



Flare's threat exposure management platform takes unstructured data points on the clear & dark web and illicit Telegram channels to provide your team with actionable alerts.

Unlike legacy CTI tools, Flare focuses on providing the **minimum viable information with maximum context — to focus analysts time on events that create real business risk**. This reduces the burden of excessive noise and helps your security teams make quick, informed decisions that directly protect your business.

Automate Cybercrime Monitoring

Flare monitors thousands of cybercrime channels across sources as diverse as Telegram, the traditional dark web (Tor) and I2P. Our platform automatically collects, analyzes, structures, and contextualizes dark web data to provide our customers with high-value intelligence specific to their organization. This includes six years of archived cybercrime data from Tor such as:

- Stolen credentials
- Corporate IP for sale (code or other IP)
- Brand & executive mentions (names, surnames, PII)
- Infected devices for sale on the Russian, Genesis, and Telegram Markets
- Targeted cyberattacks & fraud

Monitor for Data Exposure Due to Human Error

86% of security incidents are caused by human error. Monitoring clear web sources like paste sites, Bitbucket, Google, and other sites for data leaks is critical to building an effective information security posture. Flare's AI driven platform automatically scans millions of clear web sources of risk, enabling detection for PII & PHI leaks, leaky cloud buckets, developer secrets leakage, and a range of other threats.

Monitor Public GitHub Repositories for Leaked Secrets

Modern development teams are distributed and remote, in many cases with contractors and overseas developers providing crucial talent. Flare enables companies to rapidly detect leaked API keys, credentials, and other sensitive information leaked onto public GitHub environments. Flare monitors the GitHub Firehose and when it sees a commit email matching the identifier, it will clone the repository automatically and use a secret detection engine that goes through the entire repository to identify any secrets that are being exposed.

> **Whereas other solutions would present us with thousands of potential leaks which were impossible to work with for our small team, Flare was the only one that could successfully filter and prioritize data leaks with their 5-point scoring system. It allowed us to quickly cut incident response costs by 95%.**
>
> -CTI Director
> Large North American Bank

Key Features & Benefits

- Rapidly detect data leaks, stolen credentials, public GitHub secrets leakage, IOCs related to infected device markets, and other high-risk external exposure in a single unified platform with 30 minute integrations into leading SIEM/ticketing providers.
- Reduce noise and enable analysts to focus on threats that matter with Flare's AI driven prioritization engine.
- Automate takedowns across lookalike domains & public GitHub disclosures with the click of a button.
- Reduce mean time to detection (MTTD) and mean time to response (MTTR) by 90%+ with Flare's easy to use events feed.
- Proactively detect & remediate many of the most common vectors leading to data breaches, ransomware attacks, and third-party exposures.

Flare's Monitoring by the Numbers

4,000
Cybercrime Forums & Channels

1 Million
New Stealer Logs per Week

8 Billion
Data Points

28 Million
Public GitHub Repositories

Learn more about our solution

Sign Up for a Free Trial

flare

flare.io

hello@flare.io