flare

Press
Media Kit

flare

Press Media Kit

Cybersecurity as an industry is struggling. Data breach costs and cybersecurity spend continue to increase exponentially while security leaders struggle with talent shortages, tool integration, and disjunctive shifts in risk.

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.

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.

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.

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

Headquarters

Montréal, Québec

Team Size

50-75

Press Contact

press@flare.io

Date Launched

2017

Top Regions

US

Canada

Europe

Types of Organizations

MSSPs

Mid Market Companies

Large Enterprises

Serving Customers Across the Following Industries (and More)

Financial Industries

Healthcare

Technology

Retail & Hospitality

Government

Flare's Top Use Cases

Automate Cybercrime Monitoring

Flare monitors thousands of cybercrime channels across sources as diverse as Telegram and 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 Markets and Telegram
- Targeted cyberattacks & fraud

Monitor for Data Exposure Due to Human Error

85% 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.

Key Features

- 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 respond (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

Leadership

Norman Menz | CEO

Norman joined the company in 2021. Earlier in his career, Norman developed a number of information security and IT risk programs but decided to focus his attention on the biggest information security risk to organizations; which is the loss of data due to third-party relationships. Norman is a thought leader on third party and external information security risk and regularly speaks at industry events on the importance of understanding and mitigating risk associated with third parties. He is a Certified Third Party Risk Professional (CTPRP) and a contributor to the Shared Assessment's Risk Assessment Body of Knowledge.

Norman received his university degree in Business Management and has been pursuing entrepreneurial activities in technology since before becoming a Seton Hall University Pirate.

Mathieu Lavoie | Co-Founder and CTO

Mathieu Lavoie initially cofounded Flare back in 2017. With an extensive background in the industry, Mathieu started working in cybersecurity even before he obtained his B.Eng. from the L'École de Technologie Supérieure (ÉTS) in Montreal, Canada. He started his career working for a large financial institution where he was promoted to Manager of the Offensive Security Team and while at the organization, Mathieu was also a strategic advisor for senior executives on cybersecurity and blockchain.

He has been a guest speaker at security conferences such as HOPE, Hackfest, and NorthSec. In addition to cofounding Flare, Mathieu has also co-developed BitCluster, an open-source forensic tool for bitcoin transactions.

Israël Hallé | Co-Founder and Chief Architect

Israël earned a B.Eng. from ETS in 2016 and was involved in multiple cybersecurity clubs at the same time. He has since developed sought-after expertise in computer security and software engineering. His work experience spans working with the Merchant Protection and Checkout team at Shopify where he deployed a two-factor authentication system into the platform. Israël was also a malware analyst and a reverse engineer at Google where he hunted down new malware threats and introduced automation operations through big data analysis. Israël is deeply involved in the computer security ecosystem, is a sought-after presenter, and holds executive roles in multiple conferences and competitions.

Yohan Trépanier Montpetit | Co-Founder and CPO

For over 10 years, Yohan has led technical teams to reach ambitious goals on innovative projects. As Co-Founder and Chief Product Officer at Flare, he brings a broad technological background to develop innovative Cyber Threat Intelligence and Digital Risk Protection solutions to solve real-world business challenges. Yohan has a B.Eng. from ETS in software engineering.