SUCCESS STORY

flare

Global Manufacturing Company Closes Security Gaps by Discovering Unknown Organizational and Third-Party Security Risks

The Customer

- Global transit-packaging provider with over $2B in revenue
- Almost 10,000 employees across six continents and 100 facilities
- Serving customers in industries such as metal manufacturing, pharmaceutical, food and beverage, construction, e-commerce, and engineering

This global manufacturing company provides protective packaging internationally across multiple industries, so that their customers' valuable goods stay safe and intact in transit.

Challenge: Missing Visibility Into External Threats, Especially from Third-Parties

The company's cybersecurity team had built a solid foundation with endpoint protection, firewalls, and identity-based threat management. However, as they conducted a comprehensive review of their threat model after the SOC manager stepped into his role, a critical gap emerged: they lacked visibility into external threats, dark web activity, and leaked credentials that could serve as entry points for threat actors.

The security team was operating with limited external threat intelligence capabilities. While they had supplier risk management tools that provided insights into vendor compromises, these solutions had significant limitations:

- **Inaccurate lookalike domain detection:** Alerts for suspicious domains often came too late, with domains already inactive by the time the team could investigate
- **No dark web monitoring:** No visibility into credential leaks, ransomware data dumps, or underground marketplace discussions targeting their organization
- **Fragmented vendor assessment:** Difficulty connecting the dots between vendor security incidents and potential risks to their own environment
- **Reactive posture:** Seeing login failures in logs but unable to understand why credentials were being targeted

The team knew they needed a solution that could provide comprehensive Threat Exposure Management and dark web monitoring to further mature their security program.

Implementation: Eye-Opening Results from Day One

The team evaluated several solutions, ultimately choosing Flare for its transparency, customization capabilities, and hands-on approach. Unlike competing platforms that relied on email notifications and black-box processes, Flare provided direct access to data through an intuitive dashboard and robust API integration.

Proof of Concept: Immediate Value Discovery

During the 30-day proof of concept, the team uncovered critical security issues that had been hiding in plain sight:

- **Mysterious login failures:** Connected dots between log-in failure alerts and leaked credentials, understanding why specific accounts were being targeted
- **Weak password practices:** Identified users who incremented numbers in their passwords (password1, password2, password3), then implemented a more robust password change policy and proactive security awareness training
- **Unknown infrastructure:** Uncovered old login portals without MFA protection that had been forgotten by IT teams
- **GitHub exposure:** Discovered a GitHub repository with sensitive information publicly accessible
- **Vendor risks:** Found that a major vendor had RDP-exposed devices before their data breach announcement, enabling proactive vendor assessment discussions
- **Lookalike domains:** Identified domains impersonating the company and even found one legitimate company domain that nobody knew existed

> **The results spoke for themselves. During the POC, we found leaked credentials, unsecured portals, and vendor risks that we never would have discovered otherwise. That was all the proof leadership needed.**
>
> **– SOC Manager, Global Manufacturing Company**

Flare Differentiators

The team chose Flare over competitors for several key reasons:

- **Transparent data sources:** Unlike competitors that keep sources secret, Flare openly shares where data comes from
- **Hands-on control:** Direct access to customize indicators and filters rather than relying on a third-party to manage everything via email
- **SIEM integration:** Ability to ingest logs directly into Microsoft Sentinel for unified threat detection
- **Trust and transparency:** One competitor was disqualified after leaking other customers' information in document metadata

Shortly after implementation, a third-party vendor suffered a significant ransomware breach that exposed customer data. Because of Flare's monitoring capabilities, the security team was able to retrieve it and its parent company's data from the breach before the vendor notified them. This proactive discovery caught the attention of upper management and demonstrated clear ROI.

Benefits: Ongoing Operational Improvements

Since implementation, the security team has been:

- **Reducing false positives:** Credential browser with password policy filters automatically eliminates alerts for credentials that don't match organizational standards
- **Remediating in bulk:** Mark multiple old credentials as remediated at once, preventing duplicate alerts
- **Enhancing daily operations:** Threat Flow AI-powered search provides relevant updates for daily standup meetings
- **Consolidating feeds:** All threat intelligence feeds into Microsoft Sentinel alongside other security data
- **Assessing vendor risk:** Continuous monitoring of vendor security posture informs procurement decisions
- **Detecting "unknown unknowns:"** Ongoing discovery of exposed IP addresses, forgotten assets, and brand impersonation attempts, which fills a critical gap of securing what they didn't know they had

> **We use Threat Flow as part of our daily standup meeting so that we are informed of the most relevant actionable intelligence. It saves us time and makes sure we stay informed on the right information.**
>
> **- SOC Manager, Global Manufacturing Company**

Supporting a Vendor in Mitigating Risk from a Ransomware Attack

When a vendor suffered a ransomware attack and couldn't determine the entry point, the SOC manager searched Flare and found multiple leaked credentials with associated URLs, some of which still worked despite the vendor's claim that all passwords had been reset. A single vendor's exposure can quickly become an organization's risk, and gaining visibility into third-party threats is a critical part of any security program.

Forward Look: Data Security

For this global manufacturing company, the path from limited external visibility to comprehensive Threat Exposure Management fundamentally changed how the security team operates. What started as a 30-day proof of concept quickly surfaced leaked credentials, forgotten infrastructure, and vendor risks that had gone undetected, turning "unknown unknowns" into actionable intelligence. Today, the manufacturing company has gained visibility into threats across the clear and dark web, the team has shifted from a reactive posture to one where they consistently identify and address exposures before they become incidents, including discovering a major vendor breach before the vendor itself disclosed it.

As the organization turns its focus toward data security and sensitive file protection, Flare will continue to play a role in expanding that visibility into leaked files with specific sensitivity classifications.