SUCCESS STORY

SOKIGO
PART OF ADDNODE GROUP

flare

Sokigo Saves About 600 Hours Per Year with Threat Exposure Management and Executive Reporting

The Customer

- European software and services company working with clients mainly in the public sector
- About 250 employees
- Build digital solutions with the company's software

Whether working remotely or using a corporate wireless network, user credentials are more valuable than ever. To obtain these credentials, threat actors increasingly deploy info stealer malware, a malicious program that collects and packages up user data stored in:

- **Browsers**
- **Session cookies**
- **Browser history**
- **Host data**
- **Screenshots from the victim's screen**
- **Crypto wallet**

"Stealer logs have been the [sources] where we have seen the most actionable intelligence regarding leaked credentials."

- Victor Pettersson, CISO, Sokigo

Threat actors then sell the stolen data on the dark web or in illicit Telegram channels. When researching 50 companies whose data breaches were publicly available, **Flare** found that:

- **90% had previous corporate credentials leaked in a stealer log**
- **78% had corporate credentials leaked in a stealer log either six months before or after the identified breach**

For software companies, these breaches and the associated credential theft pose several risks:

- **Intellectual property theft or modification:** Malicious actors targeting software companies can either steal source code or compromise source code stored in development environments.
- **Customer data theft:** Malicious actors can steal customer data, like payment details, credentials used to access customer portals, or customer contact information to use for spear phishing campaigns.
- **Reputation:** Compromised software or customer records undermine digital brand reputation that can lead to customer churn.

With the rising threat of infostealer malware, Sokigo sought to gain insight into leaked credentials and infected devices that could impact their security, especially mentions of senior leadership. Also by monitoring the dark web and illicit Telegram channels, the security team hoped to understand whether the organization was targeted by hacktivist groups in Europe, which have been targeting commercial organizations.

Challenge: Manual Intelligence Gathering was Costly and Inefficient

In response to these risks, Sokigo sought to operationalize threat intelligence as part of its cybersecurity and digital risk management strategies. Unfortunately, the manual processes made gathering intelligence time-consuming and cost-prohibitive. The security team's processes involved:

- **Vendor-supplied documents**
- **Google alerts to monitor clear web chatter**
- **Limited, ad-hoc dark web monitoring**

The security team spent more time looking for information than acting on the threat intelligence. As Sokigo began researching threat exposure management technologies, the team knew they needed a solution that would:

- **Quickly and easily integrate into their environment**
- **Provide trustworthy insights and actionable suggestions**
- **Enable faster and more effective responses**

Implementation: Comprehensive and Smooth Free Trial to Proof of Concept Process

Sokigo leveraged Flare's free trial to test the value. Within a week, the customer had a working version of the Flare platform and began to realize value using the indexed data. During this time, the organization identified previous breaches and took appropriate actions quickly. Flare gave them near immediate insight into the sources, including:

- **A combo list dating back to 2014, with credentials that had already been rotated**
- **Stealer logs, gaining the most actionable intelligence for leaked credentials**

Sokigo moved through the free trial to the proof of concept (POC) in roughly a month. With the POC, multiple members of the security team evaluated the Flare platform adapted to their organization's needs.

Although Sokigo was in discussions with another vendor, they chose Flare because the platform offered:

- **More data sources which further reduced manual monitoring**
- **Transparency into sources for insight into threat monitoring scope**
- **Reporting that included email notification which reduced the time spent checking the platform**

The security team was able to save time immediately with Flare's actionable, prioritized alerts and clear threat intelligence scope.

> **"We're saving about 20-30 hours per month with threat exposure management and executive reporting. The biggest difference is how great we feel knowing that if our threat level would increase then we would be quickly informed about it and able to take proactive action."**
>
> - Victor Pettersson, CISO, Sokigo

Benefit: Saves 20-30 Hours Per Month with Confidence in Responding to Threats

Flare's onboarding process and intuitive user interface enables Sokigo to gain confidence in the alerts and their actionability within 1-2 months. Once they gained access to the platform, they rapidly:

- **Leveraged feedback on indicators to identify necessary tuning**
- **Identified trends in the large dataset to evaluate data's importance**
- **Removed data sources from monitoring to improve alert fidelity**

Since the client onboarded six months ago, the security team now:

- **Saves 20-30 hours per month with threat exposure management and executive reporting**
- **Has confidence in their ability to identify changes to their threat level**
- **Clearly understands the threat landscape to make data-driven, educated decisions about security investments**

In the next 6-12 months, Sokigo plans to expand the team's use of the platform so that they can extend the value further.