DATA COLLECTIONS

SAGA® data collections are expandable and user-friendly security resources that require a minimum of configuration from your side to start accelerating threat detection and investigation.

The collections are designed in close collaboration with our clients and partners and offer the widest and deepest possible range of collections. SAGA® "pay-as-you-use" modular approach allows you to receive high-quality and cost-effective intelligence delivered in real-time.

DARK WEB

The dark web has become a breeding ground for cybercriminals, where illicit activities thrive and digital vulnerabilities are exploited. SAGA® offers the industry's leading set of dark web data, offering the largest commercially available database of dark web content in the world. The dark web data collection is split up into several sub-sets, to ease use and improve precision/reduce signal-to-noise ratio.

Discussions: Dive into the depths of hacking forums, where conversations revolve around the misuse of digital assets, system abuse, and data breaches. Telegram groups and channels add another layer of intrigue to your exploration.
Datastores: Explore marketplaces

Paste Sites: Uncover the secrets of the Dark Web's anonymous platform – paste sites. These sites are a hub for sharing confidential materials, including hacking scripts and stolen information.
Chat Applications: Immerse yourself in three main chat applications: Telegram, Discord, and ICQ. Here, leaked credentials, financial frauds, and hacking-related content await your perusal.
Social Media: Traverse various alternative social Media sites such as Gab, MeWe, Reddit, Getter, Rumble, and Mastodon. Delve into discussions surrounding topics like terror, extremism, and disinformation.
Imageboards: Embark on a visual journey through imageboards, particularly on the open web and the i2p network. Engage in

offering compromised accounts and PII (Personal Identifiable Information), pilfered from computers infiltrated by log-stealer malware such as Redline and Raccoon.
Marketplaces: Journey into online marketplaces where you can unearth everything from illicit drugs to counterfeit goods, weapons, and even hacking tools.
Ransomware Sites: Gain exclusive access to official sites operated by ransomware gangs and their affiliates. Stay updated on their latest activities and announcements.

discussions accompanied by images, texts, and debates.

Explore solutions

Brand protection

Executive protection

Data breach protection

Domain Protection

Fraud prevention

Threat Intelligence

STEALERS & LEAKS

Malware stealer logs are created by a specific type of malware called a “stealer.” These logs collect and store data extracted from compromised systems, including sensitive personal and financial information.

Key targets of malware stealers include:

Login Credentials: These often comprise usernames and passwords for email, social Media, and online banking services, occasionally including additional authentication details.
Financial Data: Targets can include credit card numbers, bank account information, and transaction histories.
Personal Information: Stealers can capture personally identifiable information (PII) such as names, addresses, phone

Web Browsing History: These logs might document the websites visited by the user, complete with timestamps and URLs. **Keylogging Data:** Some stealers incorporate keyloggers to record all user keystrokes, capturing sensitive inputs like passwords. **Screenshots:** Certain malware stealers can take screenshots of the victim’s desktop or active windows for later retrieval by the attacker.

Explore solutions

Brand protection

Executive protection

Data breach protection

numbers, and social security numbers.
System Information: Logs may detail the infected system’s operating system, hardware specifications, and installed software.

Domain Protection

Fraud prevention

Threat Intelligence

CREDENTIAL LEAKS

A data leak is a dataset usually available on deep- and dark-web hacker forums. This dataset can include massive amounts of personal email, login and password combinations, or even sensitive additional personal data like Social Security numbers, and personal and medical information.

SAGA® guards your business against the most recent leaks with an automated engine that constantly discovers new sources of leaked data and includes up to 5 years of compromised history. SAGA® moves beyond the standard detection of compromised emails and passwords to include user IDs, CC, account names, SSNs, phone numbers, and many more.

Explore solutions

Executive protection

Data breach protection

DOMAIN & WHOIS DATA

Phishing attacks are one of the most common methods used to steal valuable personal information.

This collection arms your organization and VIPs against phishing and cybersquatting with intelligence around attempts to steal employee information or

SAGA® monitors exact matches, variations and common misspellings of your brand name and trademarks. It enables the search across all recently registered and deleted domain names and gets sets of domain names that contain terms that are specified by you.

compromise your assets. It monitors exact matches, variations, and common misspellings of domains, for example, to detect websites selling counterfeit products.

Explore solutions

Executive protection

Domain protection

EXPOSED SERVICES

Any device that is directly connected to the internet may contain publicly-available information. This information might be used by cybercriminals to gather information or attack companies and personal systems.

The Exposed Services data module scrapes the data of any possible vulnerable networks and devices connected to the internet: software, webcams, internet routers, security cameras, thermostats, water treatment facilities, yachts, medical devices, license plate readers, smart TVs, etc.

SAGA® helps mitigate such cyber threats as banner grabbing, firewall issues, unauthorized or vulnerable IoT devices, and outdated software that could significantly increase the chances of data leaks.

Explore solutions

Threat Intelligence

Executive protection

Brand Protection

SOCIALMEDIA

Social Media enables people to share and access real-time content easily and efficiently. At the same time, it is widely acknowledged that many social Media platforms are used to facilitate illegal transactions. This can include threats to

Facilitating ultra-scalable monitoring and evidence collection, SAGA®can save you up a massive number of man-hours. Develop cost-effective and efficient systems, going beyond conventional cybersecurity approaches..

VIP or public figures, counterfeit goods, or even drugs being sold in closed groups.

Explore solutions

Brand protection | Executive protection | Data breach protection | Domain protection | Fraud prevention | Threat Intelligence

GLOBALMEDIA

Monitoring of Media provides a global overview of various trends and news. Furthermore, it feeds raw data into analytics systems, providing an outline of hotspots and relations links.

This collection includes 170.000 global news sources across 150 languages. Beyond this, any existing news source or website news section can be monitored with SAGA®.

SAGAs® leading-edge technology can search and stream millions of news articles every day. You can granulate the content by preselecting certain countries, languages or Media types to ensure that you get precisely what you need.

Explore solutions

Brand protection | Executive protection | Data breach protection | Domain Protection | Fraud prevention | Threat Intelligence

AVOSEC
Software Distribution