Cyber security sensor solution

Open. Fast. Scalable. Transparent.

OUR APPROACH

This blog is about building our next generation cyber sensor platform. First we must let you in on a little secret, our approach may be based on yours. We have a long experience in developing cyber security sensor technology for a national early warning system protecting the critical infrastructure and enterprises. At the inception of SensorFleet, we set out to re-imagine cyber security monitoring in order to solve the pain points from the field. Four key principles guided our work.

1: OPEN PLATFORM

We wanted to make deploying new cyber detection and protection tools easy for the end users. Our answer was to develop SensorFleet as an open platform that can host detection-, protection- and scanning tools. We call these tools Instruments and they can come from 3rd parties, whether commercial, free open source or inhouse. Today, power of ecosystems enable end users to flexibly deploy tools - or applications - based on the evolving requirements. The best known are the application ecosystems that enabled smartphones to become ubiquitous devices they are today. You can think of SensorFleet both as a platform and a distribution for cyber tools. There is no vendor lock-in for a specific capability and you can leverage the hive mind. Another obvious benefit is the speed to react when new tools come available. Having a unified and controlled way to deploy tools in potentially complex environments can be a life saver.

Openness is carried over to the other fundamental design decisions of SensorFleet: You own your data, you have a full visibility on sensor communication and what Instruments do and can do is plenty, transparent and contained.

2: YOU OWN AND CONTROL YOUR DATA

We won't ask for your network data in exchange for providing the security solution for you. While controlled data sharing, such as IoC exchange, is undeniably beneficial for the ecosystem at large, we believe any sharing should be transparent and under your full control. Another aspect is that too detailed, too duplicated or too long-term data increases exposure. Therefore our preferred approach is a network of lightweight sensors placed into network locations where data is being produced, instead of a single large number cruncher. Rather than raking everything into a huge haystack and then looking for a needle, look for a needle from smaller bales. Just to be clear, there are legitimate reasons for collecting and storing the network data and that's supported by SensorFleet, just not the default mode on which overall functionality of sensor network depends. Moreover, we give you full control over data collection and retention. We also help you to make sure that collected data is retained exactly for as long as required or allowed.

3: FULL VISIBILITY ON SENSOR COMMUNICATION

Many technically oriented people are familiar with a startling feeling of observing number of connections, both inbound and outbound, that the modern applications and devices create. Since a sealed box wouldn't be a very efficient sensor, SensorFleet will also need to communicate with the outside world. What we strive for is to be clear on what each of the interfaces and connections are used for. This enables users to audit Sensor and Instruments based on security policies of network segments they're protecting.

4: INSTRUMENTS ARE EASY TO ADD, TRANSPARENT AND CONTAINED

Smartphones have made it easy for us to get the tooling we need in different situations. Visit to a new city starts with installing an application for local transport, new home appliance installation comes with remote control application and so forth. SensorFleet has been designed with the same principle in mind, making it easy to add and remove Instruments as the monitoring requirements evolve. Maybe, for example, your day-to-day use case involves asset tracking or threat detection with the IDS, but when a new vulnerability emerges, you'd need to run vulnerability scanning within the perimeter of network segments you operate. Having SensorFleet platform in those segments enables you to quickly run a vulnerability scanner as an Instrument without extra network configuration changes or manual work for retrieving the results. Furthermore, instruments have clear technical contracts on what they can access and it is enforced by the platform. In a nutshell

You will own your data. SensorFleet is transparent on what happens under the hood. Open platform will help you to react faster, to deploy easier and to embrace the open source. We help you to take the detection close to the source and to find the needle easier by making the haystack smaller. With SensorFleet, potentially radioactive security monitoring data will be an asset, not a liability. We hope you will enjoy SensorFleet as much as we enjoy developing it.

contact@sensorfleet.com