

## A Sneak Peek into Kovrr's Data Sources

Modeling impacts from cyber events requires extensive understanding of the cyber threat landscape. A core aspect of Kovrr's cyber risk modeling data pipeline combines unique data sources to better inform the data points taken into account when building out the frequency and severity of cyber events. Access to these data sources is derived via partnerships reserved for Kovrr's use exclusively for modeling purposes, developed among others with Israeli cybersecurity emerging vendors which continuously bring new exciting data and create a unique ecosystem.

### Hudson Rock

Hudson Rock is a cybercrime intelligence startup with a database composed of millions of machines compromised in global malware spreading campaigns. The data is augmented monthly with tens of thousands, to hundreds of thousands of new compromised machines. Data includes Info Stealers, ransomware bots and other types of malware. Hudson's high-fidelity data help protect employees, partners, customers, and digital assets with unprecedented granularity of threat vectors including Ransomware, Business Espionage, Breaches & Network Overtakes.


#### How Kovrr uses this data

Kovrr has extended capabilities to recognize ransomware trends and emerging techniques. This information is crucial for formulating accurate attack distributions. Kovrr leverages the data in order to enrich different parameters of its datasets. We can improve our understanding of the target audience profile by applying additional analytics on the data, Kovrr can deduce the entities who have suffered from the breach, this information may include location, job description and company. We also have extended information on the attack vector. Kovrr uses metadata regarding the attack to understand the attack vector used to install the malware, which is critical to understanding attack and exploitation patterns.

### Cynerio

Medical and IoT devices in healthcare environments grow more numerous and vulnerable every day, and mitigating their risk is becoming more complex. The Cynerio platform uses a granular inventory classification taxonomy which tracks device types, functions, vendors, models, serial numbers, firmware/OS, MAC, and IP+ methods of medical devices. Drilldowns into VLANs, ports, kernels, HW, services, browsers, and FDA class, classification, and recalls are also provided. Cynerio then leverages this data to monitor, verify, and reduce the risk





of IoT and IoMT device vulnerabilities through direct communication with vendors, third-party solution providers, and cybersecurity governance organizations.

### **How Kovrr uses this data**

Kovrr has secured unique cyber information sources per industry to have more detailed data reflecting the cyber risk landscape. Kovrr receives aggregated data on compromised medical IoT devices and relevant vulnerabilities, corresponding to companies' geographic location, size and industry that shows instances of potential attack per type of device. For this specific source, Kovrr's extended insights surrounding healthcare cybersecurity feeds into the industry exposure database. In turn this provides more accurate data on the frequency and severity of events affecting organizations in the healthcare industry and assists in better analysis of understanding a company's cyber resilience.

## **Sedric.me**

Sedric integrates into all communication systems of organizations and provides cyber risk management teams with a solution to securely store company interactions with internal and external users. By monitoring a wide range of interactions, Sedric uses AI to detect intentions related to regulatory, compliance, and company misconduct without the need for explicit exact phrase or rule matches. The platform securely cleans, encrypts and stores data associated with GDPR, PCI, PHI, and other violations before it enters a company's system.

### **How Kovrr uses this data**

Kovrr receives aggregated data of sensitive data records corresponding to companies' geographic location, size and industry that shows instances of misconduct per type of violation. The data is used to understand the distribution of data types in an organization, and further understand the likelihood of a data type to be involved in an incident. This enables Kovrr to better predict the regulation and compliance impacts on cyber attacks that affect organizational data.

There is a belief among some in the insurance industry that there isn't enough historical cyber data to properly inform risk modeling. But the data is out there and just needs to be captured, fused and expertly applied within the right modeling framework. Kovrr continues to be the leader in developing these exclusive data partnerships and building continuously updated models to support our customers.