CIM INTEL SERVICES

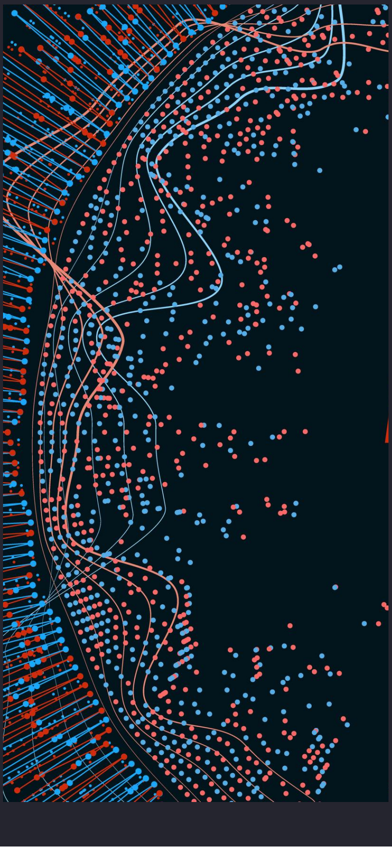
Although CIM's activities are primarily focused on ***industrial-network cyber security***, the true depth of this can only be mapped with an Intelligence approach and competence, which has therefore become one of the major pillars of CIM's cyber security services and has by now grown into a stand-alone service. The Intel service CIM represents is mostly based on OSINT, primarily ***Open Source Intelligence***. In addition, however, it leverages a number of competencies, from SOCMINT to IMINT to the increasingly emerging VHUMINT (***Virtual Human Intelligence***) capabilities. Thus, CIM's primary interest is in cyber security, but naturally it also includes the protection of the right to security and reputation, or up-to-date market information and knowledge of competitors. In practice, CIM leverages ***Intel***'s capability in two areas:

Threat Hunting

Threat Hunting does not address vulnerabilities that are already known, but focuses primarily on ***zero-day*** hacks, looking for pervasive practices that compromise the security of a family of software or a device or protocol used in industry. In addition, CIM automatically searches the Dark Web for malicious ***program code*** threatening industrial devices. However, corporate software families, third-party solutions, and medical devices that store and transmit sensitive data that are frequently used in business, are also vulnerable to malicious attacks. It is common for attackers to disassemble or reverse engineer a PLC or medical diagnostic tool to reveal vulnerabilities that could cause direct harm to corporate or everyday users of the device. CIM finds examples of this almost daily by analyzing the Dark Web forums, and it is also typical that CIM first learns about larger ***Data Breaches*** on the Dark Web, including corporate trade secrets that are often for sale (authentication keys, login passwords, corporate email system passwords), and, in many cases, data disclosing a company’s network architecture. These data sources can be used directly by SOC Analysts, as the Dark Web and Hacking forums can be used to check for traces left behind by possible cyber-attacks, which can provide relevant information about the perpetrator and the method of perpetration.

Related services:

- Manufacturer- or technology-specific Cyber Threat Hunting on the Dark Web and Clear Web Hacking Forums
- Vulnerability Monitor for Industry-Specific IIoT Devices, Industrial Controllers, and Software Vulnerability
- General Industrial or Corporate Threat Alerting about recent vulnerabilities



Competitive Intelligence

CIM's general ***Competitive Intelligence*** capability is based on daily press monitoring across three continents (Europe, Asia, North America), complemented by the bulk of the English-language IT and security / defense press, and continuously expanded with professional feeds from sectors such as telecommunications, financial technology, automotive industry, robotics, medical technology, and AI research. In addition, CIM closely follows the publications of information technology universities and research groups, especially in the field of Cybersecurity and AI research. In these resources CIM can monitor a brand or a special technology, software manufacturer at regular intervals, while also using tools such as NLP, Sentiment Analysis, Named Entity Recognition, Entity Profiling, Face Recognition, Social Media Monitoring (Facebook, Instagram, Twitter).

Targeted Competitive Intelligence measures what a full background check can show about a group of companies or individuals, in a single report or with repeated alerts: looking for data and relationships that may pose an external or internal digital threat or weaken the business positions or reputation of those affected. The service consists of the customer's own brand monitoring. The other part of the service is called passive reconnaissance, i.e. searching for security vulnerabilities, such as checking all the email addresses we know about in our Account Takeover database of hacked private and corporate emails and the entire Dark Web, along with data such as bank account numbers, social media identifiers, names of executives and partner companies, and any other potentially identifiable data. CIM also uses resources such as international business registers, government tenders and published tender results, international patent registrations, social media platforms, and other online databases to map the network of contacts.

Related services:

- Customizable, industry-specific news monitoring
- Multi-level competitor monitoring
- Passive Reconnaissance
- Continuous, Background-check-depth ***Brand Monitoring*** and ***Identity Theft Monitoring***
- ***Open Source Intelligence Analyst*** competency that supports and integrates all of the above activities