CYBER INTEL MATRIX

CIM-ISAC - Actionable, Industry Specific And Timely Cyber Intel For Humans And Machines

Cyber Threat Intelligence capabilities

Human Readable

The CIM-ISAC framework includes the basic ISAC functions that enable the sector or entity to act as a "virtual war room" defense communication platform in the event of a coordinated cyber attack.

Report an incident

Anonymity

The tab allows both anonymous and named incident reporting for authorized users. Anonymity is important because market competition within the sector can override information sharing making the whole crowdsourcing project ineffectual.

Ticketing

Incidents can be integrated with most ticketing tools (JIRA, SNOW, etc), and the platform can also send email and sms notifications directly.

Forum

The forum serves to share upcoming tasks, sector-specific problems and solutions.

Documents

The uploaded documents and their descriptions are collected under Documents. Various categories, file visibility, and permissions can be set individually.

News

The uploaded documents and their descriptions are collected under Documents. Various categories, file visibility, and permissions can be set individually.

Events

Reminders and announced events can be published (Exercises, Expos, conferences, TTX, Range / Drill, etc.,) The iCal function can be used to save the selected event to the user's calendar. Only the site administrator has permission to announce an event.

Site feed news

Information about the collected resources (TTPs, Tools, Campaigns, Alerts, IoC, etc.) as well as their distribution by type, is found on this page.

Executive summary

The importance of ISACs (Information Sharing and Analytics Centers) will increase with the rise of information technology, Industry 4.0 and 5.0. Their goal is to respond to the cyber security challenges generated within the industry by bringing the stakeholders together on a centralized platform. An ISAC must meet both human-to-human and machine-to-machine needs. Accordingly, traditionally accepted "human readable intel" functions are no longer sufficient.

The Cyber Intel Matrix (CIM) ISAC harmonizes knowledge that can be processed, shared, and distributed by both human and machine means, by hosting repository-based servers such as MISP or TAXII. This ability is not tomorrow's technology, but yesterday's competition, as we are now talking about machine-to-machine AI-based attacks and defense, where manual human interaction is not enough.

The Plone CMS was used for development because platform protection is critical. Plone is a free and open source content management system. High-profile public sector users include the U.S. Federal Bureau of Investigation, Brazilian Government, United Nations, City of Bern (Switzerland), New South Wales Government (Australia), and the European Environment Agency. Plone's proponents cite its security track record and its accessibility as reasons to choose Plone.

Incident response
If a dedicated CSIRT / CERT is available to the sector, then the entity's direct, dedicated contact details are displayed here.

Human Readable

Incident response
One of the goals of CIM-ISAC is to broadcast and spread the threat feed, which we achieve using integrated solutions such as MISP (Malware Information Sharing Platform), STIX (Structured Threat Information Expression) or TAXII (Trusted Automated Exchange of Intelligence Information). With the help of the technology, the organization and the entire sector can automate the detection of IoCs which were lost during threat hunting. Furthermore, stakeholders can jointly perform malware analysis.

The distribution of threat feeds is the privilege of the umbrella organization, and the platform includes licensing options to support this business model.

Threat feed
The CIM architecture employs a sector-specific deception-based intrusion detection infrastructure and places the incoming data in context (Domain info; IP info; Malware hash, Botnet Vulnerability Database, etc).

CIM is able to produce sector-specific feeds due to its customized decoy / honeynet infrastructure, for example:

- DNS Honeypot
- Honeytokens
- ICS honeypots
- Financial phishing intel