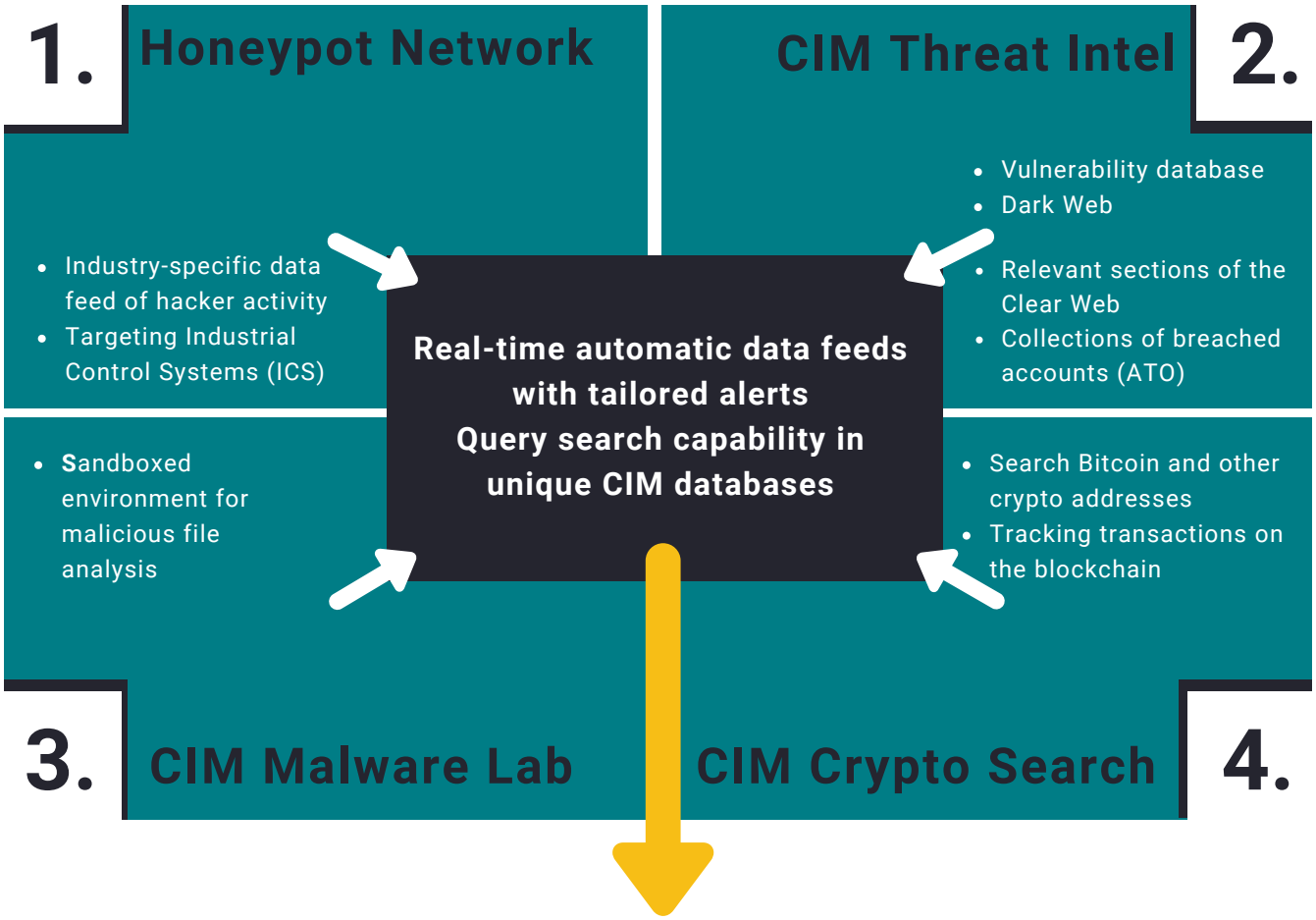
CYBER INTEL MATRIX

CYBER INTEL MATRIX (CIM)



CIM is a cyber defense threat intel tool that provides automated smart feeds and vulnerability alerts

1. **Protects fundamental IT infrastructure (software & hardware)**
2. **Protects OT infrastructure: industrial control systems (ICS) and connected smart devices**
3. **Protects intellectual property (IP) through industrial counter-espionage**
4. **Ensures cybersecurity compliance (CMMC, NIST SP 800-171, ISO 27001, PCI DSS, NATO, etc.)**

It also allows cyber analysts and law enforcement investigators to conduct in-depth background research on cyber criminals, including providing evidence in court

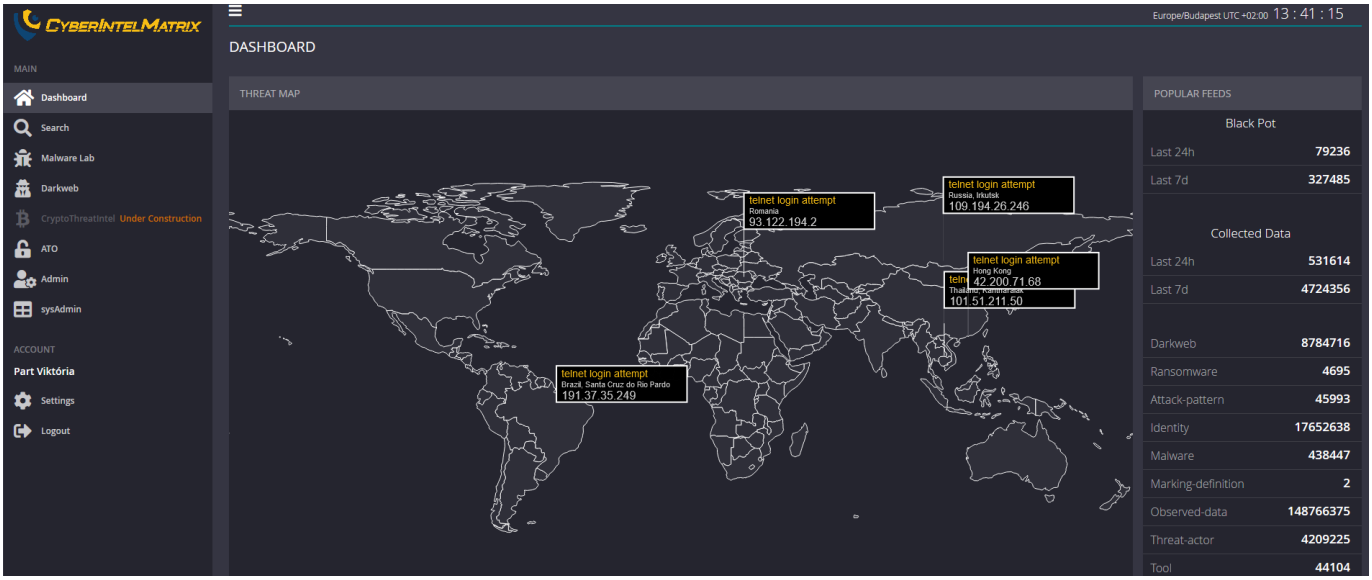
CYBER INTEL MATRIX

CYBER INTEL MATRIX (CIM)

CIM is a standalone platform

- Programmable to autopilot, easily customizable·
- Cyber analysts can also manually query targeted data in unique and public databases

At the same time, Cyber Threat Intel as a Service (CTIaaS) **enriched feeds can be integrated into** existing enterprise SIEM or SOC systems (e.g. IBM QRadar, Splunk, Zeek, Microsoft CyberX), adding unique data sources to existing subscriptions.



CIM Enriched Feeds

- Result: Higher level of protection
- Background checks for incidents detected in a SIEM can take place separately on the CIM Platform

Integration is made possible through the standard STIX graph format, but CIM also provides data in

- MISP (used by EU and NATO)
- General CSV formats

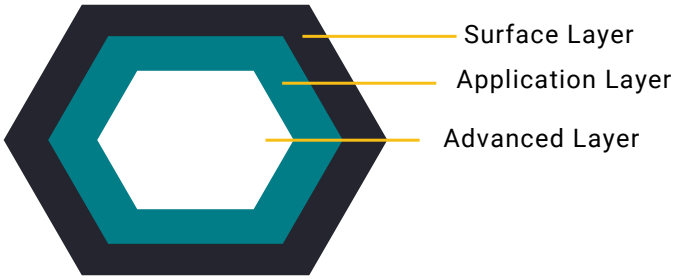
CIM uses the **MITRE standards** for defining threat actors, devices, attack patterns, contextualizing incidents, and displaying the relational matrix. Therefore, CIM can easily be integrated with 3rd-party Cyber Threat Intelligence (CTI), Security Operations Center (SOC), and Security Information and Event Management (SIEM) software, including proprietary solutions.

CYBER INTEL MATRIX

1. CIM Honeypot Network

Industry-specific feeds of Indicators of Compromise (IoC) and threat actors attacking Industrial Control Systems (ICS):

IP addresses; behavioral patterns (TTPs); time, frequency, coordination of attacks; types of malware, ports, attack type, common ICS protocols, username and password combinations used; and similar data are added to the CIM Blackpot™ database.



Suspicious IP addresses are identified, among other things, as

1. Automatic scanner programs (e.g. Shodan)
2. Part of an offensive botnet
3. IP blacklisted
4. C2 servers where attackers upload data.

2. CIM Threat Intel

Customer's integrity or infrastructure is not at risk when searching for sensitive content
CIM Crawlers constantly gather data on the dark web and sections of the clear web

Over 40 sources (among others):

- Known vulnerabilities by CVE code (MITRE Corporation)
- National Vulnerability Database, NVD (National Institute of Standards and Technology, NIST)
- Dark Web (Tor Project)
- Github developer community platform for open source projects
- Telegram encrypted chat app and group information sharing platform
- Twitter microblogging social media platform
- Reddit news aggregator and information sharing network
- ATO (Account Takeover) data dumps of compromised user accounts

3. CIM Malware Lab

Sandboxed environment for malicious file analysis
Malware evaluation does not take place on customer's devices
Malware can be automatically funneled from customer's IT network or the CIM honeypot network

- Known malware is spontaneously identified, categorized by severity
- Unknown malware is analyzed in multiple operating system environments and escalated for further action

4. CIM Crypto Search

Tracking transactions on public blockchains

Monitor crypto wallets based on transaction amount limits, participating trading houses and connected wallets, and timestamps

CYBER INTEL MATRIX

Additional features

1. Building a Custom Honeypot Network

Blackpot Honeynet™ is a network of Blackpots™ CIM builds a Blackpot™ Honeynet of IT tools and industrial controllers under the customer's IP domain, a virtual organization/facility around the real one.

Blackpot™ is a CIM honeypot
Blackpot Honeynet™ is a network of Blackpots™

- As the attacker spends time in the honeypot, CIM learns valuable information, resulting in customer's better preparedness
- In the event of a violent Denial of Service (DoS) attack, customer is informed in time
- Removes the pressure off the real firewall
- Double protection: Getting through the real firewall is made more difficult by the different security solution applied by the honeypot's firewall

Customer receives information of particular attackers specifically targeting them, not merely general industry-specific threat feeds.

Customer builds their own threat intel database to make the CIM software more targeted in effectively discovering pattern anomalies and reveal Advanced Persistent Threats (APTs) and specific hacker groups threatening them.

---

2. Entity Monitoring

In addition to the automatic configurations of the CIM Platform, additional services include regular enterprise vulnerability monitoring performed by active dedicated analysts regarding:

- Exposure of corporate intellectual property
- Vulnerability to blackmail
- Strategic liability indicators

Professional analysis of existing results and active systematic investigative research results in customer's higher level of exposure transparency.

---

3. Asset Mapping

- Bird's eye view, all in one place
- Essential assessment for planning future developments
- Inventory of assets ensuring business continuity with current status report and opportunities for expansion

---

4. Exposure Test

- Passive data collection
- Active attack
- Detailed analysis of the cybersecurity exposure of the organization from a hacker's perspective

Main Industries of Application

- *Industry, manufacturing*
- *Utility operators, power plants*
  - *Electric*
  - *Water*
  - *Gas*
- *Critical infrastructure*
- *Public transport*
- *Building engineering, smart buildings*
- *Healthcare*
- *Telekom*
- *Banking sector*

Certifications

- *NATO AQAP 2110:2016 compliant quality management system*
- *ISO/IEC 27001:2013*
- *BS EN ISO 9001:2015*
- *BLACK CERT by Carnegie Mellon University*
- *CEH, OSCP, OSCE*
- *CISSP, CISA, CISM*
- *Vendor competencies: Aruba, CyberArk, FireEye, Fortinet, IBM, Palo Alto Networks, Rapid7, Sophos, Tenable, Imperva, Microsoft Security*

Contact Us

BSS Unit Inc.

Andras Patkai
Sales Director
andras.patkai@cyberintelmatrix.com
202-321-2099

CYBER INTEL MATRIX