CYBER INTEL MATRIX

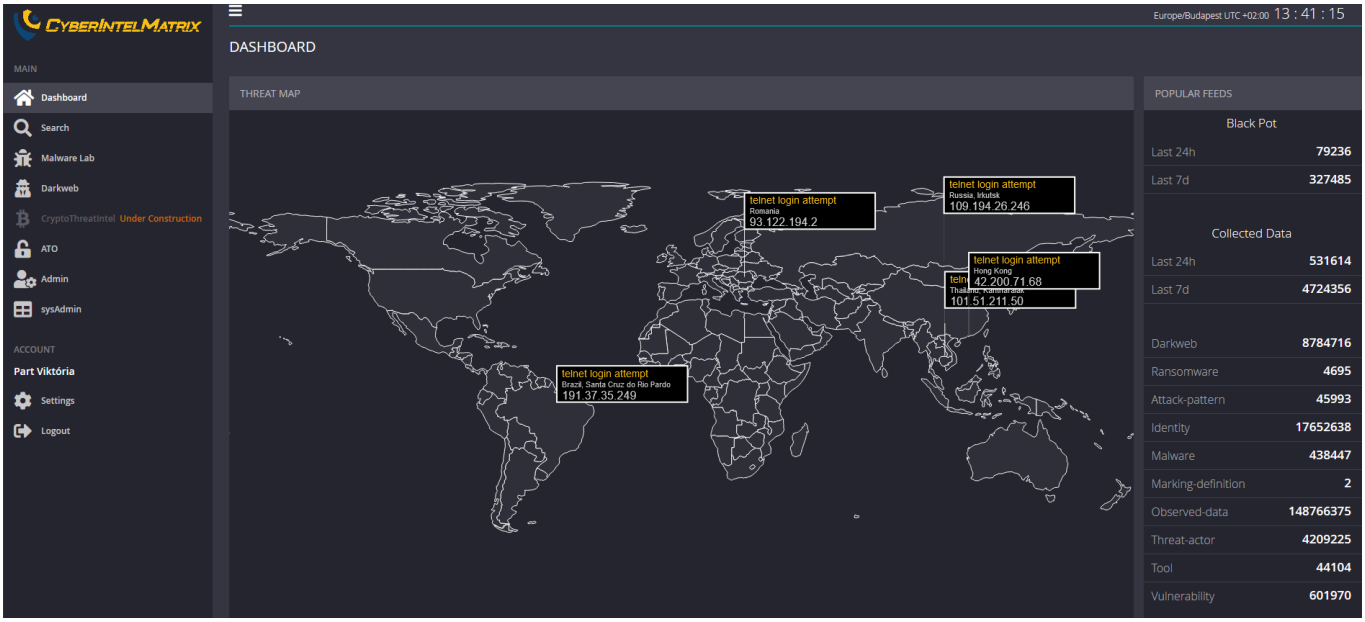
CYBER INTEL MATRIX FEED

Introduction

Manufacturing companies have become the primary targets of cyber-attacks against industrial control systems in recent years. Initially, almost no tools / systems were available to protect these devices, but more recently, the industry has begun to show a need to protect the integrity of automated manufacturing processes.

Periodically updated protection systems may not be sufficient to reduce exposure. In many cases, the protection devices used in the production control network only receive attack detection rules weeks or months later, enabling attackers to operate in the system unnoticed.

This is the reason CIM places a strong emphasis on attacks on ICS protocols / devices in addition to IT threat feeds.



STIX Structure

CIM gathers data and provides it to customers using data models based on the industry standard STIX structure.

The model has already proven its excellent applicability in connection with the transaction of general threat feeds, however it is also suitable for storing and securing threat data of industrial control systems.

More about the STIX 2.0 data structure and its object properties used by CIM here:
https://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html

CYBER INTEL MATRIX

Cyber Intel Matrix Feeds

Honeypot feeds

CIM's proprietary honeynet system is the most important source of its collections. Through it CIM provides first-hand information about attacks on both general IT infrastructure and the most common ICS protocols.

Honeypot networks operate on three distinct layers:

1. **Surface layer:** Its purpose is to capture open network scans and botnet attacks. The information obtained is the attacking IP and any payloads (e.g. username, password).
2. **Application layer:** In the case of real, prepared attackers, they find services in the honeynet that emulate real applications (e.g. Apache), the vulnerabilities of which can be exploited by known exploits
3. **Advanced layer:** Emulates live, complex applications that do not have known vulnerabilities. They are only sensitive to very complex attacks or zero-day exploits.

Emulated general protocols:

- ***HTTP / HTTPS:*** TTP information about the attacker is obtained through an emulated web application. If the attacker manages to get through the login interface, the application records all the actions of the actor (so-called Session-logging). The collected data is correlated with the IoC database of already registered vulnerabilities so that the attack method can be identified. If the system does not find a match, it registers it as a possible zero-day attack and submits it to the analyst for further investigation. Less complex attacks are also registered, providing information about possible botnets.
- ***Telnet:*** Simple telnet service with authentication. It primarily provides information about threat actors.
- ***FTP:*** A full-fledged file server to which an attacker can upload documents. After uploading a new file, the system automatically scans it with multiple antivirus programs and subjects it to dynamic analysis in the Cyber Intel Matrix Malware Lab.
- ***SSH:*** A shell with a reduced instruction set that logs commands issued by an attacker. Once collected, the system places it in context based on IoC rules.
- ***SNMP:*** Emulates a corporate network through which the attacker's attack target and methods can be identified.

In addition to general purpose honeypots, CIM also emulates industrial services. They respond as full-fledged devices, so they log all protocol-specific commands.

Emulated ICS protocols:

- DNP3
- Modbus
- S7comm
- EC 60870-5-104
- OPC

Due to the explosive spread of smart homes, CIM has incorporated protocols governing the communication of IoT devices as well. Services include the MQTT protocol implementation in CIM honeynet systems.

CYBER INTEL MATRIX

Cyber Intel Matrix Feeds

Enrichment Feeds

The data collected from honeypots is complemented by other self-developed, open-source and third-party information gathering services. These include some of CIM's proprietary crawlers that gather the latest threat results from more than 40 different sources (e.g. CVE descriptions, NVD entries).

1 Domain Information

If the system finds a publicly available domain name for the incoming attacker's IP, it assesses the registration and hosting information available from the DNS records using that host's surface enumeration.

Example of domain information collected:

{"name":"api.cyberintelmatrix.com","domain":"cyberintelmatrix.com","addresses":[{"ip":"92.249.148.164","cidr":"92.249.128.0/17","asn":20845,"desc":"DIGICABLE"}],"tag":"cert","source":"Crtsh"}

{"name":"cyberintelmatrix.com","domain":"cyberintelmatrix.com","addresses":[{"ip":"2a00:c760:83:def:aced:fff0:0:40db","cidr":"2a00:c760::/32","asn":47381,"desc":"DOCLERWEB-AS"},{"ip":"185.33.54.17","cidr":"185.33.52.0/22","asn":47381,"desc":"DOCLERWEB-AS"}],"tag":"cert","source":"CertSpotter"}

2 IP Feeds

Important information can be added to threat-actor objects by comparing their IP addresses with those found on automated scanners (e.g. Shodan). The additional data that can be deduced from this can help identify the operating system running on the attacking machine, open ports, and the services running on them.

3 Botnet Information

CIM's various automated scanners (self-developed and third-party) are able to determine if a host using the specified IP address is a member of a botnet and whether it sends information to an alleged C2 server. From this data, IP blacklists can be generated almost immediately, which can be integrated into firewalls to block large amounts of attacks.

4 Malware Info Feeds

By automatically hash-analyzing files uploaded to honeypots or collected by crawlers, the system instantly detects known malware on the system.

It is also possible to manually analyze files using the Cyber Intel Matrix platform.

5 Vulnerability Databases

CIM's crawlers collect the most recent published vulnerabilities and their indicators in real time. During the received attacks, the system defines the attack vector by correlational analysis and registers the found connections.

CYBER INTEL MATRIX

Cyber Intel Matrix Feed API

CIM Rest API

Cyber Intel Matrix feeds can be retrieved with HTTP requests via the REST API.

CIM provides data through two main API endpoints, one is a stream-type entry point that reports current attacks, and the other is a searchable, relational-centric entry point.

On the searchable API (Search feed), queries can be filtered with a JSON-based, self-developed query language called Cyber Intel Query LAnguage, CIQLA for short.

The data is only accessible with the knowledge of the API key (token).

Live Information Feed

Endpoint: https://api.cyberintelmatrix.com/api/feeds/live/get
Method: POST
Description: The endpoint was designed to provide recently registered honeypot alerts and crawled data in a descending list. Depending on the length of the requested time interval, the response may take more time (up to 1 minute). Due to the amount of the collected objects it is not recommended to set the interval longer than 1 day. To ensure the stability of the service, the number of hits in a response is limited to 5000 objects.
Object types retrieved from the service: observed-data, identity, threat-actor, vulnerability, malware
Request properties:

- ***Header properties:***
  - Auth: the service token to identify the requester
- ***Body properties:***
  - fromTime: The time after which the objects were registered. The required format is the following:YYYY-MM-ddTHH:mm:SS.f (eg. 2020-03-21T00:00:00.0)

Example HTTP request

```
POST
/api/feeds/live/get HTTP/1.1
Host: api.cyberintelmatrix.com
Auth: <token>
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundary7MA4YWxkTrZu0gW
----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="fromTime"
2020-03-21T00:00:00.0
----WebKitFormBoundary7MA4YWxkTrZu0gW
```

Example HTTP response

```
HTTP/1.1 200 OK
Date: Sun, 02 Aug 2020 15:27:18 GMT
Content-Type: application/json
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

{"status": "success", "hits": [{"_index": "stix-observed-data",
"_type": "observed-data", "_id": "observed-data--f90267f8-7f16-
4c2d-8a1e-0d9138330137", "_score": null, "_source": {"type":
"github", ...
```

CYBER INTEL MATRIX

Cyber Intel Matrix Feed API

Search Feed

Endpoint: https://api.cyberintelmatrix.com/api/ciqla/search
Method: POST
Description: For executing complex searches, the service accepts a CIQLA query and returns all the matching objects.
Object types retrieved from the service: observed-data, identity, threat-actor, vulnerability, malware, attack-pattern, relationship
Request properties:

- ***Header properties:***
  - Auth: the service token to identify the requester
- ***Body properties:***
  - ciqla: the query in the structure of the proprietary CIQLA format.

Example HTTP request

```
POST /api/ciqla/search HTTP/1.1
Content-Type: application/json
Auth: <token>
Accept: */*
Host: api.cyberintelmatrix.com
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 88
{"graph":"[]","ciqla":"[{\"_id\":\"indicator—6f70bc72-3818-4074-ae49-c5da7170daf3\"}]"}
```

Example HTTP response

```
HTTP/1.1 200 OK
Date: Mon, 03 Aug 2020 11:13:09 GMT
Access-Control-Allow-Origin: *
Content-Type: application/json
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
{"status": "success", "data":
"[{\"type\": \"relationship\", \"created\"...
```

Outputs

Due to the connection system between objects, CIM mainly supports STIX output, but outputs can also be queried in other formats.

The following formats are currently supported:
STIX, MISP, CSV