PROJECT

Multi-tenant cybersecurity operations centre designed as an open cloud service with machine learning elements

Supporting document for V4

Design and implementation of a threat intelligence process

Linked to work package KPB2 – Design of the SOCaaS service

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

1. Design and implementation of a threat intelligence process 3
2. Review of available tools and platforms for Threat Intelligence 4
2.1. ThreatConnect 4
2.2. Recorded Future 5
2.3. Anomali ThreatStream 6
2.4. Comparison of selected solutions 6
3. Selection of a suitable tool for the SOC 8
3.1. Test deployment of the Threat Intel module as part of the Filebeat agent ... 8
List of sources 10

Funded by the European Union NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

1. DESIGN AND IMPLEMENTATION OF A THREAT INTELLIGENCE PROCESS

The term Threat Intelligence, which in recent years has become an inseparable part of cybersecurity, where it also has the established abbreviation CTI (Cyber Threat Intelligence). According to Gartner: "*Threat Intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets. This information helps in making decisions about the appropriate response to these threats.*"

CTI should help obtain answers to the following questions:

- Who poses a threat to our organization and by what methods can they carry out an attack?
- How do attack vectors affect the security of our organization?
- What should our SOC team be monitoring?
- How can we reduce the risk of a cyberattack on our organization?

CTI is information that helps organizations better understand threats and take appropriate measures to mitigate them, and it is divided into three categories:

1. Strategic CTI
2. Operational CTI
3. Tactical CTI

Strategic CTI
It provides a broad view of the evolution of cyber threats over time, the identification of attackers' motivations and their historical patterns of behaviour. It helps to answer the questions "Who?" and "Why?" by analysing attack attribution, trends in threat activity and their relationship to geopolitical conflicts. It includes mapping attacks to global events, statistical overviews of security breaches, changes in attackers' TTPs (tactics, techniques and procedures) and the analysis of sector-specific threats. It makes it possible to assess technological and supply chains, identify the key areas in which the organization is under threat, and make better strategic decisions on cybersecurity and investment in it.

Operational CTI
It provides answers to the questions "How?" and "Where?" by analysing attackers' methodologies (TTPs) and identifying their activities in various environments. It includes brief written threat reports, profiles of victims and attack groups, and specific attack details such as tools, communication channels and techniques for persistence in systems. It helps analysts understand the method of attack and where it is carried out, thereby supporting better incident response and proactive hunting for unknown threats. It provides context for investigating cyberattacks and improving defence strategies.

Tactical CTI focuses on the identification and analysis of IOCs. It is used primarily for automated threat detection within systems. It can also be used to enrich security alerts, for example in SIEM systems, to provide more context for deciding which threats we can safely ignore and which require more detailed examination and the application of more comprehensive security measures. In this way it can help analysts, when analysing an incident, to find specific artefacts and document it better. To sum up, tactical CTI may contain, for example, file hashes, IP addresses, URLs and IOCs.

For a better understanding of the differences, we have compared them in the clear table Tab. 1 below.

Tab. 1 - Threat Intelligence categories

Type	Answers the questions	Focus	Output data
Strategic	Who? Why?	Non-technical	Extensive written reports, mapping of attacks and campaigns to conflicts, and more
Operational	How? Where?	Mixed	Brief written reports, profiles of victims and groups, description of TTPs, and more
Tactical	What?	Technical	Machine-readable indicators such as IP addresses, domains, IOCs (Indicators of compromise) and signatures
The data were obtained from the official website of Anomali [25].			

It follows from table Tab. 1 above that, for an environment where we want to implement technical measures to protect IT infrastructure against cyber threats, tactical Threat Intelligence is needed, as it is the only type that is also genuinely applicable in practice in our case.

2. REVIEW OF AVAILABLE TOOLS AND PLATFORMS FOR THREAT INTELLIGENCE

In this section we examine the available options for implementing tactical CTI. There are, of course, many CTI solutions, but it is not within the scope of this diploma thesis to examine absolutely all of them, and we therefore focus on the solutions selected in the thesis assignment.

2.1. ThreatConnect

The Threat Intelligence Platform (TIP) from ThreatConnect enables organizations to collect, enrich and analyse all sources on a single platform, thereby enabling prioritization of and response to the most critical threats. The platform harnesses the power of AI and automation to simplify and speed up threat detection and response, thereby increasing efficiency. In other words, this tool covers all three types of CTI, i.e. strategic, operational and tactical. However, since we are primarily interested in tactical CTI, we focus only on selected functions of this tool that are relevant to this area and that, in our opinion, could be useful in an academic environment.

Functionality:

1. **Unified threat intelligence source**
   It enables the automated collection, normalization and enrichment of various data sources. This eliminates the need for manual processing and unification of data from

different sources, which saves time and increases efficiency. The platform supports integration with a variety of sources, including commercial, open-source, community and internal sources, thereby ensuring a comprehensive and up-to-date overview of threats.

2. **Automation of analysts' work**
   This functionality includes:
   – **Automated playbooks**
     They enable rapid automation of custom processes using a simple drag-and-drop interface, thereby reducing the need for programming skills.
   – **AI and automation**
     The Collective Analytics Layer (CAL) Automated Threat Library (ATL) collects and analyses more than 60 authoritative open-source intelligence sources. Automatic detection of MITRE ATT&CK tactics and techniques, CVEs, indicators and AI-generated summaries saves analysts hours of manual work every day.
   – **Automated data enrichment**
     It uses third parties such as VirusTotal, Shodan, DomainTools and URLScan.io for automatic data enrichment, thereby providing analysts with actionable information without the need for manual intervention.

3. **Threat intelligence visualization**
   It helps analysts to examine attacker behaviour effectively, identify tactics and techniques, and improve team collaboration using the MITRE ATT&CK framework. However, it focuses on the tactical level of CTI, where it enables rapid detection of and response to specific threats.

2.2. Recorded Future

It enables organizations to identify, investigate and prioritize cyber threats. The platform uses advanced analytical tools and automation to simplify and speed up threat detection and response, thereby increasing efficiency. This tool also covers all three of the aforementioned CTI categories. As with the previous tool, we list here only the functions relevant to tactical CTI and to use in an academic environment.

Functionality:

1. **Strengthening threat elimination measures**
   It provides the detailed context needed to take effective measures. This includes IOCs, a customizable sandbox for testing and so-called "hunting packages", which help analysts in actively hunting for threats. Each package focuses on a specific threat actor, malware campaign or piece of malicious software. These packages contain YARA and SNORT rules, which allow them to be easily implemented in security solutions. It is therefore also a proactive approach to threats.
2. **Threat intelligence visualization**
   It makes it possible to respond faster and with greater confidence to alerts that are relevant to the organization.

The functionality of this tool is presented very specifically on the official website, and its interpretation is less clear and more difficult to understand than that of the previous tool.

2.3. Anomali ThreatStream

"It provides access to the largest global repository of curated threat intelligence. This platform enables the enrichment, contextualization and detection of known and emerging threats, tailored to the given organization." This tool also covers all three types of CTI. In line with the previous tools, for Anomali ThreatStream we also focus on the functions relevant to tactical CTI and its use in an academic environment.

Functionality:

1. **Extensive integrations**
   Access to an extensive ecosystem of third parties, including threat intelligence sources, enrichment data and tools, without duplicate or outdated data.
2. **Threat intelligence orchestration**
   They enable automated sharing of security data across firewalls, SIEM systems, proxy servers, DNS, endpoint protection platforms (EPP) and other solutions.

2.4. Comparison of the selected solutions

All the selected solutions look interesting; they collect threat information from various commercial as well as free sources and normalize it into a unified format. These commercial sources may differ between individual tools, but essentially it is only a matter of which partnerships the company behind the development of the tool has concluded. In addition, each of these tools can visualize this data nicely and plot various graphs. However, each interprets the information on the tool's functionality in its own way, which also complicates the subsequent comparison of the individual tools and finding one's way through the differences between them, if we do not take price into account. The real difference therefore apparently lies only in the additional functionality.

Recorded Future additionally includes an integrated customizable sandbox testing environment and the aforementioned so-called "hunting packages", in which we see significant potential for threat response. These two functionalities may be the reason why this tool ranks first in the Gartner rating in the Threat Intelligence products category, at least at the time of this project.

Anomali ThreatStream contains similar functionality, which, however, they describe in a slightly different way. Given that it was not possible to try these tools out in practice, the differences between their functionality are difficult to evaluate. ThreatConnect does not list these functionalities, but it provides automated playbooks and the integration of AI into automation processes, which can also be very beneficial in practice.

Finally, on the basis of functionality, the Gartner rating and the customers who rely on this solution, such as Microsoft, Amazon and Cisco, we would clearly choose Recorded Future, because its "hunting packages" can be a powerful tool for implementation in practice. In table Tab. 2 below we have compared the tools in terms of price and whether they include at least a limited free version.

Tab. 2 - Comparison of the selected Threat Intelligence solutions

	ThreatConnect	Recorded Future	Anomali ThreatStream
Free version	✓	✗	✗
Price	?	?	?
Tactical CTI coverage	✓	✓	✓
? Price available only on request.			

As we can see in table Tab. 2 above, all the tools also include tactical CTI, i.e. they meet our needs, but the price is available only on request, which suggests that it will be far from low and therefore certainly not friendly to the budget of a smaller organization. Of these tools, a free alternative was offered in the past by Anomali, and is currently offered only by ThreatConnect. The free tool called STAXX from Anomoli naturally has limited functionality and makes it possible to download data from various free threat sources using STIX/TAXII, which can be configured in it. It naturally also makes it possible to configure commercial threat sources, but this is where it currently ceases to be free. Apart from obtaining threat data, we can visualize it and search it manually in this tool, which, given the current capabilities of commercial tools, seems rather inefficient to us; moreover, its official support is ending and it will no longer receive updates, which is why we have stated that Anomali no longer offers a free solution.

As regards the free solution from ThreatConnect called Polarity Community Edition, compared with its paid version it naturally has limited functionality, but compared with Anomali STAXX it still brings added value even today. The function of this tool called Focus consists in the ability to define a specific area of the screen that interests us, such as the MD5 hash of a file or a security alert. Using the mouse cursor, the user marks the desired area, which is then captured in the form of a screenshot. This screenshot serves as the basis for an automated search for additional threat data. This is an interesting functionality, but manual work by the analyst, who reviews the data, for example from a SIEM system, is still necessary, and from our point of view the degree of automation here is low. As we stated at the beginning of the first chapter, tactical CTI primarily serves automated threat detection, which, in terms of this definition, is not fully achieved with such a solution.

3. SELECTION OF A SUITABLE TOOL FOR THE SOC CENTRE

Before selecting a specific solution, it is essential to understand the mechanisms by which the available CTI processing tools work and to analyse the processes that take place in the background. In the case of the free variants, threat information is obtained automatically from freely available sources, then normalized and made available for manual analysis or visualization. The exception is Polarity Community Edition, which enables semi-automated searching of this data.
Paid solutions naturally provide a considerably higher degree of automation. Paid tools also include commercial threat sources, thereby expanding the available data, and usually contain integrations with systems such as SIEM or a firewall, which can make further use of this data in automated threat detection. However, in smaller organizations it is important to minimize the costs of technological solutions, and in such a case only free threat sources are available to us, and advanced functionalities are also absent.
An important requirement for this project was to avoid paid tools. Unfortunately, of the selected solutions only ThreatConnect and its Polarity Community Edition solution meet this requirement, which, however, does not fully meet the requirement for a fully automated process.

3.1. Test deployment of the Threat Intel module as part of the Filebeat agent

With the aim of centralized processing and visualization of threat data, an implementation was designed using the Threat Intel module, which is part of the Filebeat agent. This module enables automated acquisition of data from various available sources, including free ones, while ensuring their immediate application in the form of security alerts. The CTI data processed include, for example, IP addresses, URLs and file hashes.

The module also provides the possibility of enriching already existing data and subsequently contextualizing it, which enables a better understanding of the context of the identified threats. Given the ability of such a solution to work over a wide range of data traffic, it was assessed as a suitable place for implementing the CTI process.
Implementing the Threat Intel module in the ELK environment ensures seamless integration of CTI, eliminates the need for additional data normalization and enables effective visualization of the data. Since Kibana is already part of the infrastructure, the visualization of threat data can be carried out directly in it, which simplifies the process and eliminates the need to use additional web interfaces.
Since most traffic nowadays is transmitted encrypted, without using the SSL inspection function it is difficult to detect malicious traffic, and so, for example, we can compare file hashes only with those transmitted over unencrypted traffic or obtained from devices on which we have auditbeat agents deployed.

The Threat Intel module makes it possible to collect threat data from the following sources:

- **Abuse.ch**: Provides community threat intelligence focused on fighting malware and botnets. Its key partner is **Spamhaus**, which provides support and cooperation in operation. 15,000 specialized researchers collaborate on this project.
- **Malware Bazaar:** A platform from abuse.ch and Spamhaus intended for sharing malware samples with the infosec community, antivirus vendors and threat intelligence providers.
- **MISP:** The Malware Information Sharing Platform (MISP) is an open-source threat information sharing platform, co-founded with the European Union. It enables organizations to collect, store, distribute and share IOCs. It supports automation, data visualization and integration with tools.
- **AlientVault OTX:** Open Threat Exchange (OTX) is a community-driven platform for sharing threat information. It provides access to more than 20 million IOCs daily, contributed by more than 200,000 participants from around the world.
- **Anomali Limo:** A free threat source used by Anomali's no longer supported STAXX tool.
- **Anomali ThreatStream:** This is an integration with this paid tool.
- **ThreatQuotient:** As in the previous point, this is an integration with a paid tool.

LIST OF SOURCES

1. **Gartner, Inc.,** *Definition: Threat Intelligence.* [online]. 10/4/2025. Available at: <https://www.gartner.com/en/documents/2487216>
2. **Anomali Inc.,** *What is threat intelligence?.* [online]. 10/4/2025. Available at: <https://www.anomali.com/resources/what-is-threat-intelligence>
3. **ThreatConnect,** *TI Ops: An Evolved Threat Intelligence Platform.* [online]. 10/4/2025. Available at: <https://threatconnect.com/threat-intelligence-platform/?>
4. **ThreatConnect,** *Unified Threat Library.* [online]. 10/4/2025. Available at: <https://threatconnect.com/solutions/unified-threat-library/>
5. **ThreatConnect,** *Unleash Efficiency Through Automation.* [online]. 10/4/2025. Available at: <https://threatconnect.com/solutions/automation/?>
6. **ThreatConnect,** *Understand the Attacker and Take Action.* [online]. 10/4/2025. Available at: <https://threatconnect.com/solutions/attck-visualizer/?>
7. **Recorded Future, Inc.,** *Identify, investigate, and prioritize cyber threats.* [online]. 10/4/2025. Available at: <https://www.recordedfuture.com/products/threat-intelligence>
8. **Recorded Future, Inc.,** *Special Delivery: Recorded Future Hunting Packages.* [online]. 10/4/2025. Available at: <https://www.recordedfuture.com/blog/threat-hunting-packages>
9. **Anomali Inc.,** *Harness the Power of Global Threat Intelligence.* [online]. 10/4/2025. Available at: <https://www.anomali.com/products/threatstream>
10. **Anomali Inc.,** *STAXX - Your Free STIX/TAXII Solution.* [online]. 10/4/2025. Available at: <https://www.anomali.com/resources/staxx>
11. **ThreatConnect,** *Get Started with Polarity Community Edition.* [online]. 10/4/2025. Available at: <https://threatconnect.com/polarity-community-edition>
12. **Abuse.ch,** *FIGHTING MALWARE AND BOTNETS.* [online]. 11/4/2025. Available at: <https://abuse.ch/>
13. **Abuse.ch,** *MalwareBazaar.* [online]. 11/4/2025. Available at: <https://bazaar.abuse.ch/>
14. **MISP project,** *Open Source Threat Intelligence and Sharing Platform.* [online]. 11/4/2025. Available at: <https://www.misp-project.org/>
15. **LevelBlue, Inc.,** *The World's First Truly Open Threat Intelligence Community.* [online]. 11/4/2025. Available at: <https://otx.alienvault.com/>
16. **Elasticsearch B.V.,** *Threat Intel module.* [online]. 11/4/2025. Available at: <https://www.elastic.co/docs/reference/beats/filebeat/filebeat-module-threatintel>
17. **Anomali,** *Download STAXX 3.4.* [online]. 11/4/2025. Available at: <https://www.anomali.com/resources/staxx/download-staxx>