CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE
OF TECHNOLOGY

CÆSAIR - AN AIT SOLUTION FOR COMPREHENSIVE ANALYSIS OF CYBER THREAT INTELLIGENCE

CÆSAIR is a cyber threat intelligence solution designed to provide analytical support for security experts carrying out IT incident handling tasks on a local, national or international level.

Thanks to its powerful correlation capability, CÆSAIR provides analysts with the necessary support to handle reported incident information.

- It **aggregates and examines intelligence** acquired from numerous Open Source INTelligence (OSINT) feeds;
- it quickly identifies related threats and existing mitigation procedures;
- it allows to **establish cyber situational awareness** by keeping track of security incidents and threats affecting the monitored infrastructures over time.
- Visit the **CÆSAIR homepage** to get a detailed look! http://caesair.ait.ac.at

ADVANTAGES OF CÆSAIR

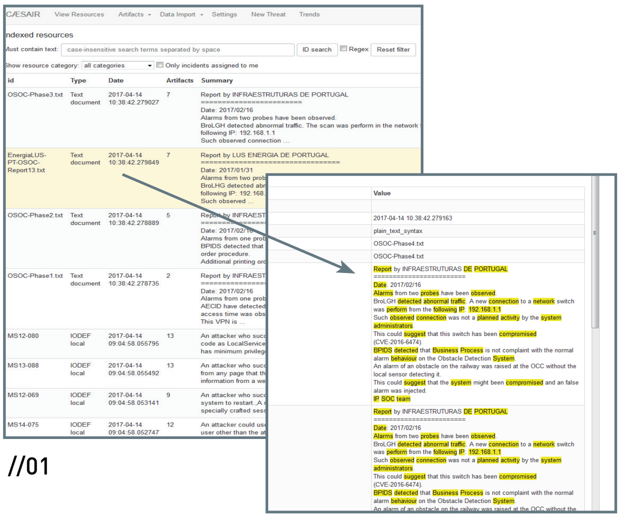
- **Reduced incident handling time**: from a multitude of imported security documents, CÆSAIR identifies the most relevant to a given one.
- **Reliable basis for decision making**: CÆSAIR explains how documents or events are connected to one another; it allows the analyst to select the most appropriate correlation method and to flexibly adjust relevance metrics.
- **Answers to strategic questions on threat landscape:**
  What software products are being targeted recently?
  Which attack patterns is the infrastructure most vulnerable to?
  Which vendors fix vulnerabilities faster?
- **Customizable import sources**: acquires organization's internal incident reports and a multitude of Open Source Intelligence (OSINT) feeds.
- **Interface** with existing security solutions by supporting widely adopted CTI standards: IODEF, STIX, TAXII, etc.

CÆSAIR APPLICATION CASES

IDENTIFY IMPLICIT RELATIONS BETWEEN DOCUMENTS OF DIFFERENT CATEGORIES:

- **Auto-tagging** of documents to identify their categories (e.g.: vulnerability, exploit, IoC) based on text content analysis.

- **Discovering relations** between documents from different classes: a vulnerability and its corresponding exploits; an exploit and the respective attack description; an attack and an advisory describing its possible mitigation.



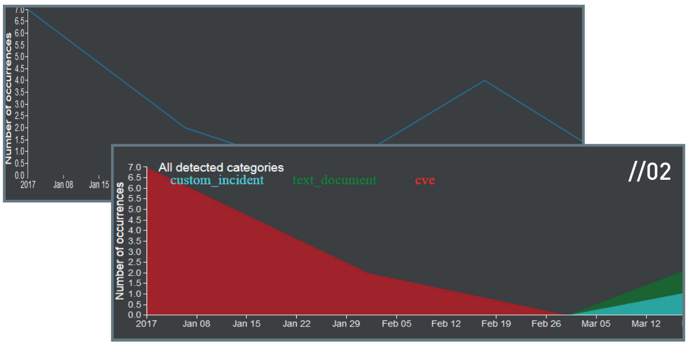
id	Type	Date	Artifacts	Summary
OSOC-Phase3.txt	Text document	2017-04-14 10:38:42.279027	7	Report by INFRAESTRUTURAS DE PORTUGAL ======================== Date: 2017/02/16 Alarms from two probes have been observed. BroLGH detected abnormal traffic. The scan was perform in the network following IP: 192.168.1.1 Such observed connection ...
EnergiaLUS-PT-OSOC-Report13.txt	Text document	2017-04-14 10:38:42.279849	7	Report by LUS ENERGIA DE PORTUGAL ================================ Date: 2017/01/31 Alarms from two prob BroLHG detected abn following IP: 192.168. Such observed ...
OSOC-Phase2.txt	Text document	2017-04-14 10:38:42.278889	5	Report by INFRAEST ============== Date: 2017/02/16 Alarms from one prob BPIDS detected that order procedure. Additional printing ord
OSOC-Phase1.txt	Text document	2017-04-14 10:38:42.278735	2	Report by INFRAEST ============== Date: 2017/02/16 Alarms from one prob AECID have detected access time was obs This VPN is ...
MS12-080	IODEF local	2017-04-14 09:04:58.055795	13	An attacker who succ code as LocalService has minimum privileg
MS13-088	IODEF local	2017-04-14 09:04:58.055492	13	An attacker who succ from any page that th information from a we
MS12-069	IODEF local	2017-04-14 09:04:58.053141	9	An attacker who succ system to restart.,A r specially crafted sess
MS14-075	IODEF local	2017-04-14 09:04:58.052747	12	An attacker could use user other than the at

	Value
	2017-04-14 10:38:42.279163
	plain_text_syntax
	OSOC-Phase4.txt
	OSOC-Phase4.txt
	Report by INFRAESTRUTURAS DE PORTUGAL ======================== Date: 2017/02/16 Alarms from two probes have been observed. BroLGH detected abnormal traffic. A new connection to a network switch was perform from the following IP: 192.168.1.1 Such observed connection was not a planned activity by the system administrators. This could suggest that this switch has been compromised (CVE-2016-6474). BPIDS detected that Business Process is not complaint with the normal alarm behaviour on the Obstacle Detection System. An alarm of an obstacle on the railway was raised at the OCC without the local sensor detecting it. This could suggest that the system might been compromised and an false alarm was injected. IP SOC team
	Report by INFRAESTRUTURAS DE PORTUGAL ======================== Date: 2017/02/16 Alarms from two probes have been observed. BroLGH detected abnormal traffic. A new connection to a network switch was perform from the following IP: 192.168.1.1 Such observed connection was not a planned activity by the system administrators. This could suggest that this switch has been compromised (CVE-2016-6474). BPIDS detected that Business Process is not complaint with the normal alarm behaviour on the Obstacle Detection System. An alarm of an obstacle on the railway was raised at the OCC without the

//01

TREND ANALYSIS – KEEP TRACK OF THE EVOLVEMENT OF THE IT SECURITY LANDSCAPE BY OBSERVING:

- How the vulnerability of a software & hardware product changes over time
- How timely a software vendor releases a fix after an exploit is disclosed
- Which products on the market are most exposed to security threats
- What are the „top 10" non-trivial frequently co-occurring topics in CTI



ASSISTANCE IN CREATION AND DISTRIBUTION OF ADVISORIES

CÆSAIR provides suggestions for generating warnings & advisories about:

- vulnerable software & hardware products
- potential counter-measures for a threat, found as related documents with the tag "patch/fix" or "course of action",
- recipients of the warning (based on assets information provided by end users). Warnings / advisories are sent out to the recipient list, or available on-demand (including the historic data).

INTERACTION WITH EXISTING SOLUTIONS FOR THREAT AND INCIDENT HANDLING

CÆSAIR's analytical functionality can be accessed through a **friendly graphical user interface**, as well as via APIs.

- deployed it as a **full-fledged standalone** installation **or**
- run it "**as a service**" on data collected from third-party solutions, such as threat sharing or incident handling solutions, and/or direct its output to such solutions. This allows the integration of CÆSAIR with open-source (such as IntelMQ and MISP) or commercial products.

//01 Identification of Related Documents: Users can expand a related document, observe its details, and compare them against the details of the selected document

//02 Trend Analysis: on top it shows the overall trend considering all categories; the stacked graph shows the portion of occurrences for each document category.

AIT AUSTRIAN INSITUTE OF TECHNOLOGY
Florian Skopik
Tel +43 50550 3116
Donau-City-Straße 1, 1220 Wien
florian.skopik@ait.ac.at
www.ait.ac.at