

CHAOS

Cyber Health and Awareness Operational System

**Centro Nacional
de Cibersegurança**

1. Project Overview

CHAOS focuses on prevention and improvement of the health of Portuguese cyberspace through communications and alerts to reduce the cyber-attacks surface and support entities with the technical and procedures information.

Therefore, the CHAOS platform in National CyberSecurity Centre is being developed to prevent vulnerability exploits in Public Administration, Critical Infrastructures and important systems available in Portuguese cyberspace. The platform will support multiple tasks, like sending alerts of vulnerable systems detected in cyberspace and new found software and hardware vulnerabilities, recommendations to improve the security of systems and infrastructures, and monitoring the systems and networks in each entity to generate periodically a “reliability indicator” at a national, sector and entity level.

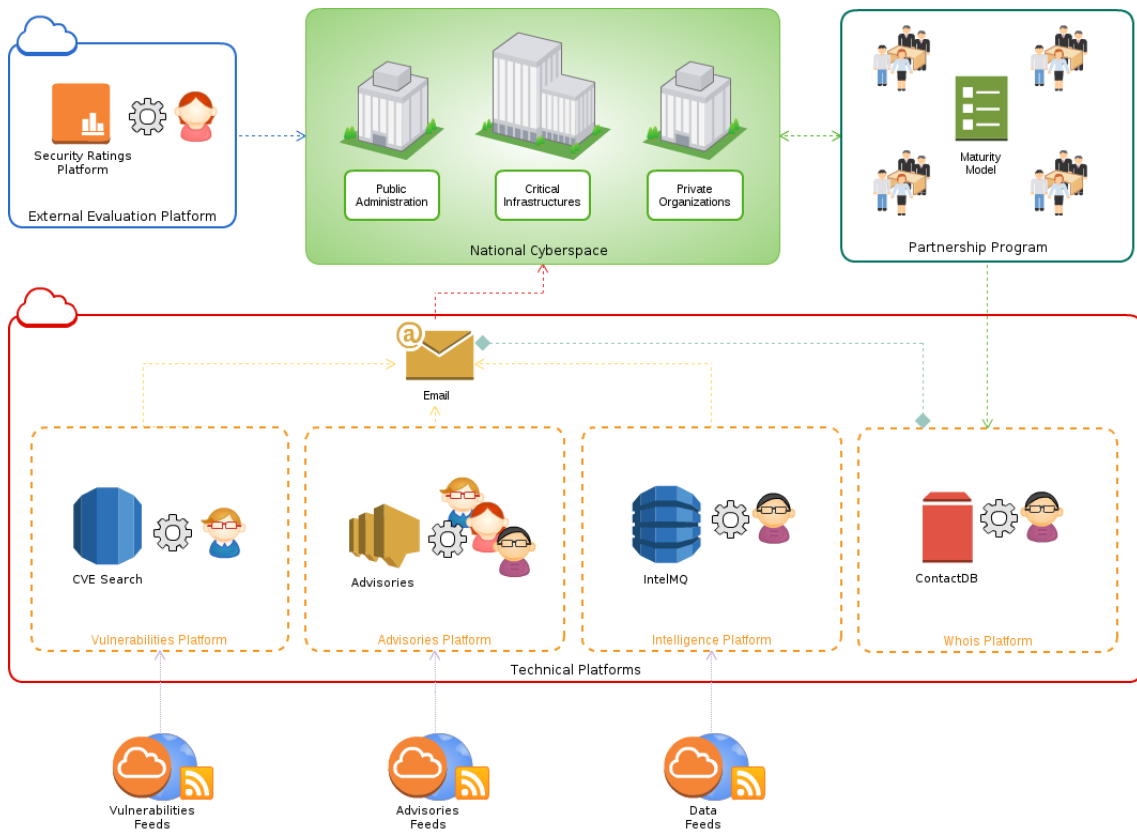
In order to achieve these goals, the project has the following steps:

1. Networks, domains and systems identification and map them to the correspondent entities. Insertion of collected information into an open-source tool named ContactDB;
2. Present and apply a “Maturity Model” to improve the reliability of technical teams responsible for monitor, prevent and respond to incidents at each entity. In this step, each entity should follow the model to achieve technical capabilities to correctly monitors and protect their networks and systems;
3. Collect and process data feeds (compromised systems, vulnerable systems, indicators of compromise) from multiple sources using an open-source tool named IntelMQ developed by CNCS;
4. Correlate information from step 1 and 3 and generate automated reports mentioning the possible vulnerable systems;
5. Based on found vulnerable systems, intersect vulnerabilities with CVE database using an open-source tool named CVE-Search to manually create reports and

recommendations with technical details to fix the vulnerability and prevent future systems compromise;

6. Monitor the “reliability indicator” generated by a commercial tool named Security Ratings Platform from BitSight Company to evaluate the effectiveness evolution of the project;
7. Generate “reliability indicator” evolution reports at a national, sector and entity level.

2. Architecture



3. Global Status

- Partnership Program
 - "Maturity Model" document: **completed**
 - Automated collection of technical information: **completed**
 - Verification of the technical information by organizations: **in process**
 - Meetings: **in process**
- Whois Platform: **under evaluation**
- Intelligence Platform:
 - Information collection process of vulnerable systems: **completed**
 - Alert process of vulnerable systems: **almost completed**
- Advisories Platform: **under evaluation**
- Vulnerabilities Platform: **under evaluation**
- External Evaluation Platform: **completed**

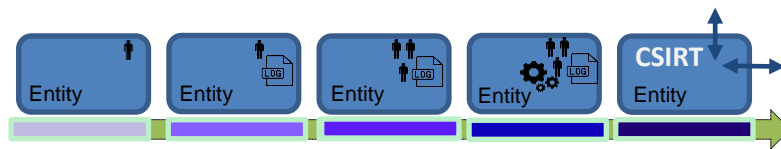
4. Partnership Program

i. "Maturity Model" document

Status: completed

Description: Maturity Model document has the guidelines for each organization to grow in terms of cybersecurity capabilities. In general, CNCS intends to develop and promote national capabilities such as:

- Human capabilities
- Technological capabilities
- Processes
- Prevention & Reaction



The document, available in the link below, is presented at meetings with all organizations that have technological systems connected to Portuguese cyberspace.

URL: <http://www.cncs.gov.pt/media/2015/06/Roadmap-Capacidades-Minimas.pdf>

ii. Automated collection of technical information

Status: completed

Description: Through RIPE Whois Client was possible to automatically collect all networks and related information in Portuguese cyberspace. Thus, CNCS starts generate a Whois-Database mapping the collected information with extra values like organization name, organization type (finance, governmental, ISP, etc), email contacts, etc. The main goal of this Whois-Database is to add support to the other parts of CHAOS project that needs, for example, the correspondence between IP addresses tagged as vulnerable systems and organization name and contacts.

iii. Verification of technical information by organizations

Status: in process

Description: Verification process is an import step to make sure that correct information goes to correct organization. In the last months, CNCS started to send official emails to official organization contacts to validate the technical information saved in Whois-Database.

Notification Example:

Caro(a) Senhor(a),

O Centro Nacional de Cibersegurança é um organismo da Administração Pública com a missão de contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional.

No âmbito de um projeto de validação e identificação das entidades responsáveis por cada gama de endereçamento IP público, o Centro Nacional de Cibersegurança, está a proceder ao levantamento dos pontos de contacto e responsáveis pela área de segurança dos SI/TIC das diversas entidades do Estado, operadores de Infraestruturas Críticas Nacionais e serviços vitais de informação. O resultado deste projecto, através do esforço conjunto de todas as entidades, permitirá caminharmos para um ciberespaço nacional mais seguro através da partilha informação relativa a alertas de segurança e notificações de incidentes de segurança.

Neste sentido, o Centro Nacional de Cibersegurança vem solicitar o preenchimento e validação de alguns dados relativos à sua entidade para facilitar a cooperação entre as duas entidades:

1) Preenchimento e validação das seguintes informações que serão usadas para comunicar incidentes de segurança detectados.

- Informações gerais da equipa/departamento de segurança e/ou informática da entidade

Entidade:

Telefone:

Telefone 24h:

Email:

- Informações relativas ao ECO (Elemento de Coordenação Operacional) da entidade

Nome:

Telemóvel:

Telefone:

Email:

2) Validação e confirmação de que as gamas de endereçamento público, seguidamente apresentadas, estão atribuídas à sua entidade. No caso de alguma gama de endereçamento pertencente à sua entidade não estar presente na lista, adicione a mesma à lista.

- Gamas de endereços IP:

<CIDRs>

Antecipadamente agradecemos a atenção que possa dispensar a este assunto, bem como a sua colaboração neste projeto.

Melhores cumprimentos,

iv. Meetings

Status: in process

Description: Schedule meetings aims to establish a trust relationship between Portuguese National CyberSecurity Center and organizations. At the meetings, CNCS takes the opportunity to present the Maturity Model and request technical information like networks and contacts which will be useful for alerts dissemination.

5. Whois Platform

Status: under evaluation

Description: The technical information automatically collected along with the information received from organizations is growing. CNCS is evaluating if ContactDB tool can handle correctly all these information and requests periodically organizations to validate the information related to them. Currently, all information is saved in CSV file.

Software

Name: ContactDB

Description: The ContactDB project was initiated to cover the need for a tool to maintain contacts for CSIRT teams. The first POC was designed based on specification of a few CERT team including CERT.at, CIRCL, CERT.PT and CERT.be.

Features:

- Secure implementation
- Easy and modular web interface
- Integration with 3rd party tools
- Support for GPG public key storage
- Delegation (an organization can keep his contact info up-to-date)

Link: <https://github.com/certtools/contactdb>

Screenshot:

A	B	C	D	E	F
org_name	org_email	whois_inetdescr	whois_inetname	isp_network	org_network
Banco Caixa Geral de Depósitos	@cgsd.pt	Caixa Geral Depósitos	CGD-PT	128.0/18	9.96/27
Banco Caixa Geral de Depósitos	@cgsd.pt	Caixa Geral Depósitos	CGD-PT	128.0/18	7.80/28
Banco Caixa Geral de Depósitos	@cgsd.pt	Caixa Geral Depósitos	CGD-PT	128.0/18	6.96/27
Banco Caixa Geral de Depósitos	@cgsd.pt	Caixa Geral Depósitos	CGD-PT	128.0/18	5.132/30
Banco Caixa Geral de Depósitos	@cgsd.pt	CAIXA GERAL DE DEPOSITOS, SA	CGDNET	4.134.0/24	34.0/24
EDP	@edp.pt	EDP Distribuição de Energia, SA	EDP	0.0/16	2.184/29
EDP	@edp.pt	EDP Energias de Portugal SA	EDP	0.0/16	14.32/29
EDP	@edp.pt	EDP Renováveis Europe S.L	EDPR	0.0/16	1.224/29
EDP	@edp.pt	EDP-Renovaveis	EDPRENOVAVEIS	0.0/16	3.184/29
EDP	@edp.pt	EDP - Energias de Portugal, S.A.	PTEDP-20140520	80.0/22	0/22
EDP	@edp.pt	EDP - Energias de Portugal, S.A.	PTEDP-20140520	040./29	0./29
Ministerio da Justica - IGFEJ	@igfej.mj.pt	Dir. Geral Servicos Informaticos	DGSI-PT	128.0/18	2.128/26
Ministerio da Justica - IGFEJ	@igfej.mj.pt	Min. Justica - Gabinete Estudos Planeamento	SEP	32.0/19	9.96/27
Ministerio da Justica - IGFEJ	@igfej.mj.pt	IJ	ITJ	5.64.0/19	4.224/27
Ministerio da Justica - IGFEJ	@igfej.mj.pt	Instituto das Tecnologias de Informacao na Justica - ITJ	ITJ	0.0/16	6.0/28
Ministerio da Justica - IGFEJ	@igfej.mj.pt	Instituto das Tecnologias de Informacao da Justica - P-ITJ	P-ITJ	28.0/18	1.144/29
Ministerio da Justica - IGFEJ	@igfej.mj.pt	Instituto das Tecnologias de Informacao da Justica - LP-ITJ	LP-ITJ	92.0/18	64/26
Ministerio da Justica - IGFEJ	@igfej.mj.pt	Ministerio da Justica	MJ	192.0/24	12.0/24
Banco Millennium BCP	@millenniumbcp.pt	Millennium BCP-Prestacao de Servicos ACE	PT.SERV/BANCA-01	22.0/24	0/24
Banco Millennium BCP	@millenniumbcp.pt	Millennium BCP-Prestacao de Servicos ACE - Rya AUP	PT.SERV/BANCA-01	0/16	0/25
Ministerio Administracao Interna	@sia.mai.gov.pt	Direccao Geral Infra Estr. e Equipamentos	DGIE	5.0/16	6.128/28
Ministerio Administracao Interna	@sia.mai.gov.pt	Direccao Geral Viacao	DGV	0.0/19	7.32/27
Ministerio Administracao Interna	@sia.mai.gov.pt	Ministerio Administracao Interna	MAI	0.0/16	6.64/26
Ministerio Administracao Interna	@sia.mai.gov.pt	MAI - Ministerio Administracao Interna	MAI	0.0/16	4.216/29
Ministerio Administracao Interna	@sia.mai.gov.pt	Secretaria-Geral do Ministerio da Administracao Inter	MAI-NET	28.0/18	64/26
Ministerio Administracao Interna	@sia.mai.gov.pt	Direccao Nacional da Policia de Seguranca Publica	PSP-PNET	92.0/18	224/28
Ministerio Administracao Interna	@sia.mai.gov.pt	Polica Seguranca Publica	PSPNET	64.0/18	9.96/27

6. Intelligence Platform

v. Information collection process of vulnerable systems

Status: completed

Description: CNCS is using IntelMQ tool to collect and process data feeds. The tool is in production since April and has been collecting thousands of security events regarding vulnerable systems in Portuguese cyberspace.

vi. Alert process of vulnerable systems

Status: almost completed

Description: CNCS is finishing the development of the tool named IntelMQ-Mailer which will be responsible to automatically send periodic email reports to organizations regarding vulnerable systems in each organization.

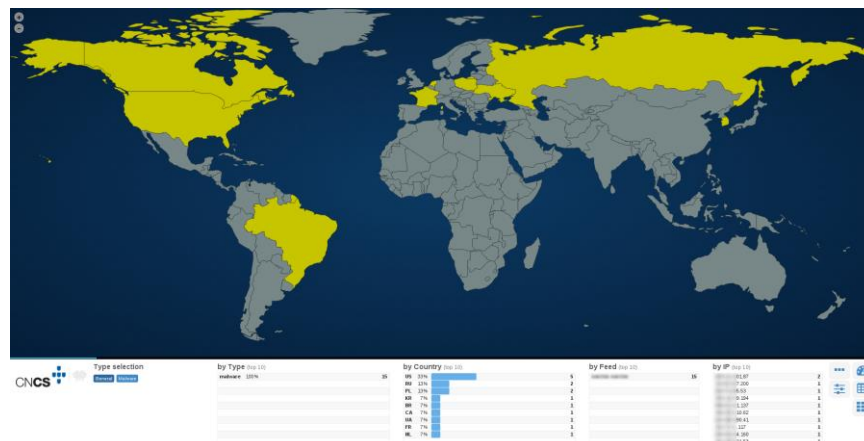
Software

Name: IntelMQ

Description: IntelMQ is a CERTs solution for collecting and processing security feeds, pastebins, tweets and log files using a message queuing protocol. It's a community driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs during several InfoSec events. Its main goal is to give to incident responders an easy way to collect & process threat intelligence thus improving the incident handling processes of CERTs.

Link: <https://github.com/certtools/intelmq>

Screenshot:



7. Advisories Platform

Status: under evaluation

Description: Advisories platform is under evaluation. The best solution until now is Taranis, a tool created by Dutch National Cyber Security Center.

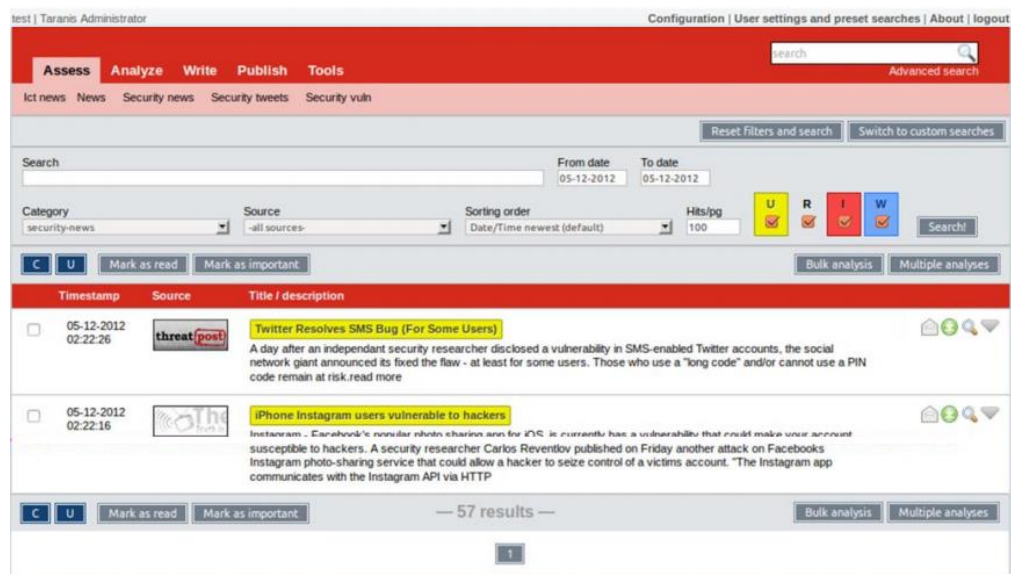
Software

Name: Taranis

Description: Taranis is a tool to collect, analyze and publish alerts regarding cyber-threats and vulnerabilities.

Link: <https://www.ncsc.nl/english/Incident+Response/monitoring/taranis.html>

Screenshot:



The screenshot displays the Taranis web interface. At the top, there is a navigation bar with tabs for 'Assess', 'Analyze', 'Write', 'Publish', and 'Tools'. Below this, there are search filters including 'From date' and 'To date' (both set to 05-12-2012), 'Category' (set to 'security-news'), 'Source' (set to '-all sources-'), and 'Sorting order' (set to 'Date/Time newest (default)'). There are also buttons for 'Mark as read' and 'Mark as important'. The main content area shows a list of search results with columns for 'Timestamp', 'Source', and 'Title / description'. Two results are visible: one from 'threatpost' titled 'Twitter Resolves SMS Bug (For Some Users)' and another from 'infosec' titled 'iPhone Instagram users vulnerable to hackers'. At the bottom, it indicates '57 results' and has buttons for 'Bulk analysis' and 'Multiple analyses'.

8. Vulnerabilities Platform

Status: under evaluation

Description: Vulnerabilities platform is under evaluation. After Taranis and CVE-Search final evaluation, CNCS will decide on keeping both platforms or if Taranis can handle all information in one place.

Software

Name: CVE-Search

Description: CVE-Search is a tool to import CVE (Common Vulnerabilities and Exposures) and CPE (Common Platform Enumeration) into a MongoDB to facilitate search and processing of CVEs. The main objective of the software is to avoid doing direct and public lookup into the public CVE databases. This is usually faster when doing local lookups and limits your sensitive queries via the Internet.

Link: <https://github.com/cve-search/cve-search>

9. External Evaluation Platform

Status: completed

Description: to evaluate the evolution of CHAOS project, Security Ratings Platform from BigSight is being used to monitor the risks and vulnerabilities of organizations. In order to get a better understanding of the maturity level of each organization, CNCS is periodically updating the networks associated to each organization based on technical information automatically collected and received from organizations.

Software

Name: Security Ratings Platform

Description: The BitSight Security Ratings Platform gathers terabytes of data on security outcomes from sensors deployed across the globe. From our data, we see indicators of compromise, infected machines, improper configuration and poor security hygiene. BitSight's sophisticated algorithms analyze the data for severity, frequency, duration, and confidence and then map it to a company's known networks, creating an overall rating of that organization's security performance. These objective ratings, based on externally accessible data, give visibility into a company's security posture over time.

Link: <https://www.bitsighttech.com/security-ratings-platform>

Screenshot:

