D5.2

CS-AWARE User and Usage Guidelines

Grant Agreement number:	740723
Project acronym:	CS-AWARE
Project title:	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis
Principal author:	Thomas Schaberreiter, University of Vienna, thomas.schaberreiter@univie.ac.at
Co-author(s)	John Forrester, Cesviter Consulting Massimo Della Valentina, Cesviter Consulting
Internal reviewers:	Christian Wieser, University of Oulu Alex Papanikolaou, InnoSec
Document version:	1.0

Table of Contents

Revision History

Version	Changes
1.0	Submitted to the European Commission

Executive Summary

The CS-AWARE deliverable 5.2 is concerned with providing material to be used by new CS-AWARE users in order to better understand the user interface (UI) options and interactions. In this context, two main topics have been identified that are addressed in this deliverable:

- User guides that are concerned with introducing the available interfaces and interface options to the user
- Usage guidelines that are concerned with detailing the possible user interactions with the different interfaces according to day-to-day usage scenarios

The user guides presented in this deliverable are grouped around three objectives: Give a quick overview of the CS-AWARE functionalities, introduce the main interfaces used in fulfilling CS-AWARE tasks, and give a detailed overview of the CS-AWARE user and content configuration options. Those three objectives have been addressed in three separate user guides, each one building on the previous one and providing more context with respect to the objective that is to be addressed. The user guides are based on the initial user guides published in CS-AWARE deliverable D4.4, updated according to user input and feedback from CS-AWARE piloting, and accounting for UI changes that resulted from this input.

The usage guidelines presented in this deliverable detail the possible user interactions with the CS-AWARE interface according to four scenarios that cover the main functionalities of the CS-AWARE system: cybersecurity awareness, self-healing and information sharing. The scenarios are grouped around how a user would resolve a threat detected by the CS-AWARE system (with and without self-healing available), how general security warnings from social media can be configured and monitored in the system, and how information can be shared with experts or communities outside the organization.

1 Introduction

The user material presented in this deliverable is concerned with two main aspects: to introduce the user to the UI elements available in the technical implementation of the CS-AWARE system (user guide), and to show the user how those elements are used in a dynamic way in day-to-day operation (usage guidelines). The user and usage guidelines presented in this document assume a readily configured and instantiated CS-AWARE instance, according to the system and dependency analysis guidelines presented in CS-AWARE deliverable D2.5.

The aim with these manuals is to help general users understand the issues and options presented to them via the CS-AWARE interface, and how to interact with them in day-to-day operation. The user manuals are presented in three different documents, introducing to the CS-AWARE system on 3 different levels of depth and expertise: The *CS-AWARE user manual reading guidelines*, the *CS-AWARE quick user guidelines* and the *CS-AWARE extended user manual*. The extended user manual contains more technical documentation regarding the initial installation and configuration (assuming the system and dependency analysis according to D5.2 has been completed). The quick user guidelines aim at giving a rapid introduction to the CS-AWARE system. The quick reading guide is intended to give a reader a quick reference guide to the system and its various components.

In addition, a set of four usage scenarios in the context of providing usage guidelines are presented in this deliverable. Those scenarios describe how the user interacts with different UI elements presented in the user guides in day-to-day operation. The presented scenarios reflect the most common usage scenarios, as observed during CS-AWARE piloting, and cover all main functionalities available in CS-AWARE. Scenarios 1 and 2 describes how a user reacts to a threat detected by CS-AWARE (including the possibility of self-healing, if available). The difference between Scenarios 1 and 2 is the difference in operation between small/ medium sized organizations and large organizations, which is reflected in the way how tasks relating to a detected threat are distributed among employees. Scenario 3 describes how a user would define and monitor general security warnings via social media, and Scenario 4 describes how information about a detected threat can be shared with security experts and communities outside the organizational context.

The CS-AWARE user guides are introduced in Section 2, with the actual content attached to this document in Annex 1 (CS-AWARE user manual reading guidelines), Annex 2 (CS-AWARE quick user guidelines) and Annex 3 (CS-AWARE extended user manual). The CS-AWARE usage guidelines in form of usage scenarios are presented in Section 3.

2 CS-AWARE user guide

The CS-AWARE user guides presented in this document are updated versions of the user guides originally presented in deliverable D4.4, with the updates accounting for user feedback and system implementation changes that were encountered during CS-AWARE piloting. The CS-AWARE user guides are presented on three different levels: An overview of the CS-AWARE interface presented in the CS-AWARE user manual reading guidelines in Annex 1, an introduction to the end-user facing interface options in the CS-AWARE quick user guidelines presented in Annex 2, and detailed descriptions of the interface and configuration options in the CS-AWARE extended user manual presented in Annex 3.

The idea of this “Quick User Guide” is to provide the inexperienced user with a simple, quick introduction to the CS-AWARE system and its various modules. More detailed information about the CS-AWARE system (especially user and content configuration options) is outlined in the extended version of the user manual. If users are just starting with the CS-AWARE system, it would be best to start with the “Quick User Guide” to gain a quick overview of the

system and use the "User Manual Reading Guide" as a quick refresher about the CS-AWARE system and its various components.

3 CS-AWARE usage guidelines

In this Section the possible interactions with the CS-AWARE system are presented in 4 illustrative common usage scenarios. The interactions are illustrated in the form of activity diagrams of possible actions after an event was initiated, with each action detailed in screen shots of the CS-AWARE interface. This document assumes a deployed CS-AWARE system, according to the requirements defined in the guidelines and procedures for the system and dependency analysis in CS-AWARE deliverable D2.5. The 4 scenarios cover the possible interactions with the CS-AWARE system for:

Scenario 1: A threat event detected by the CS-AWARE system is resolved by a single Person/ system administrator in a municipality. This is expected to be a typical scenario in small to medium sized municipalities that handle their IT in-house or have a service contract with a single supplier.

Scenario 2: Several persons/departments/external suppliers are involved in resolving a threat which requires coordination of their actions. This is expected to be a typical scenario in large and metropolitan municipalities.

Scenario 3: Describes the interactions with the CS-AWARE system for monitoring of general security warnings based on per-asset based keywords. The scenario includes the definition of custom keywords and the handling of such events detected by the CS-AWARE system.

Scenario 4: Describes the activities involved in sharing cyber threat intelligence with external cyber security communities, based on threat information from events detected by the CS-AWARE system.

The usage scenarios have been defined in response to a recommendation given in the context of the second CS-AWARE review, to supplement the CS-AWARE training plan presented in Section "10.1 Appendix 1 – Training Plan" of deliverable D4.4 with "situational exercises" to be able to train the operational aspects of the CS-AWARE interface. It was assessed that the main user group benefiting from this kind of exercises will be the system administrator and technical manager user group, which is the expected user group to interact with the CS-AWARE interface in an operational capacity.

As can be seen in Table 1, the training plan originally presented in Section 10.3.3 of deliverable D4.4 has been updated to include training according to the usage scenarios presented in this Section. Relevant changes have been marked in green.

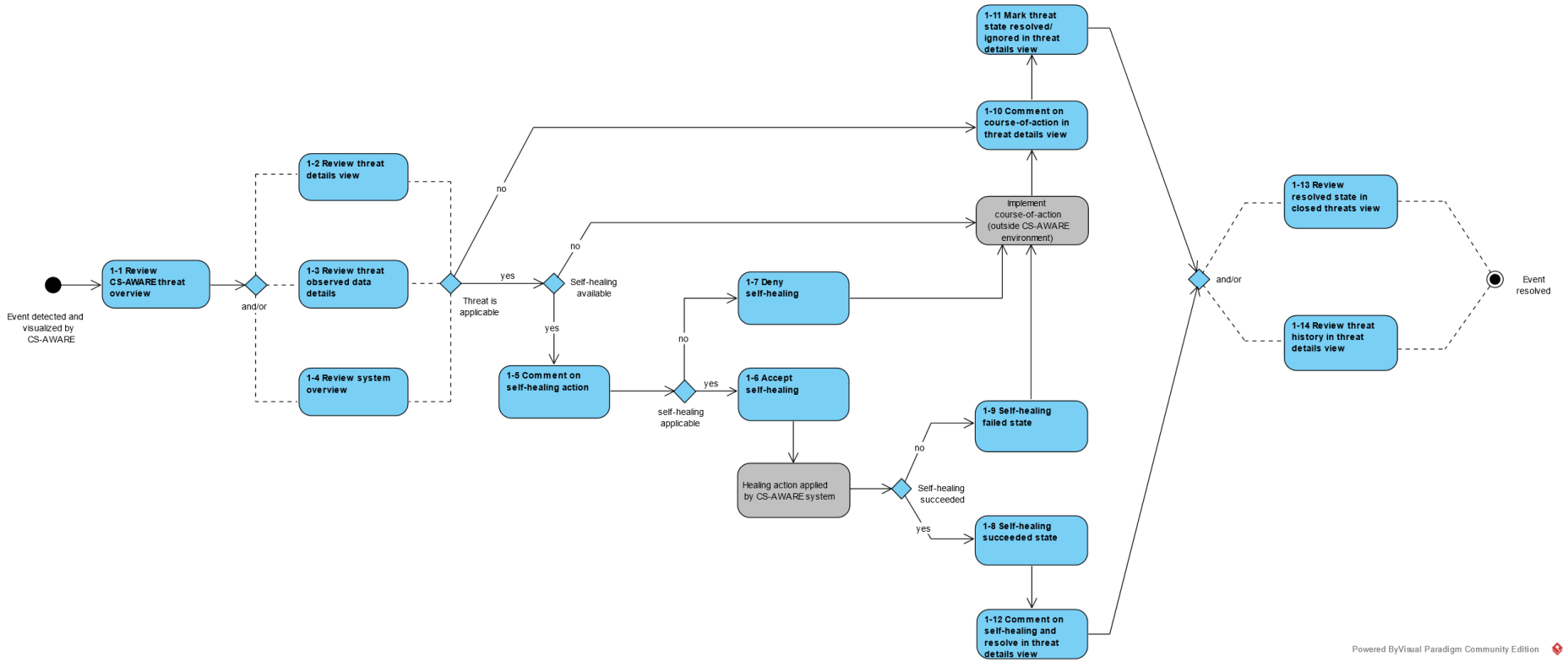
Table 1: Updated technical training plan (originally published in CS-AWARE deliverable D4.4)

Training phases detail	Topics and Products	Sessions (1/2 or full day)	Roles/Skills Associated

Setup virtual environments of reference	• General introduction to CS-AWARE System architecture	First session of Transfer of Technical know-how	• IT Architect • System Integrator • Db Admin. • Security specialist • Network Specialist
Release of documentation Products (analysis of solutions, specific technical and functional)	• Introduction to CS-AWARE technical documentation and operational manuals	Second session of Transfer Technical know-how	• IT Architect • System Integrator • Db Admin. • Security specialist • Network Specialist
Overview of reference environments and deployment infrastructure components	• Architectural model • Integration of components • Installation and configuration of the system • Usage scenarios covering use of CS-AWARE system	First session regarding system components and their relative deployment	• IT Architect • System Integrator • Security specialist • Network Specialist
Specific training for Integration of software components including issues relating to operation and maintenance	• Maintenance and Helpdesk issues • Integration with other systems	Second session regarding system components and specific aspects of CS-AWARE	• System Integrator • Db Admin. • Security specialist

	• Possible evolution of components • Further work on usage scenarios regarding CS-AWARE system		• Network Specialist

3.1 Usage scenario 1: Threat handling (small to medium sized organizational structure)



Scenario 1 represents a common usage example that guides through the different path available within the CS-AWARE interface for resolving an event detected by CS-AWARE. This scenario includes the usage path of an event that has a self-healing option available or not available.

The scenario starts by reviewing the events in the CS-AWARE threat overview in step 1-1 (Section 3.1.1). The user has the option to review details about the incident in the threat details view in step 1-2 (Section 3.1.2 for the view without self-healing and Section 3.1.3 for the view of an event with self-healing available), the incident's observed data view in step 1-3 (Section 3.1.4) and the system overview in step 1-4 (Section 3.1.5).

In case the user decides, based on the provided awareness information that the event is not relevant, the user can provide additional information as to why the event is considered irrelevant in step 1-10 (Section 3.1.11), and close the event with the state set to "ignored" in step 1-11 (Section 3.1.14).

If the event is relevant and no self-healing option is available, the user will implement a course-of-action outside the CS-AWARE environment, aided by the additional information provided by CS-AWARE. Once the course-of-action has been implemented satisfactory, the user is able to comment on how the threat has been resolved for future record in step 1-10 (Section 3.1.11) and mark the event state "resolved" in step 1-11 (Section 3.1.13).

If a self-healing option is available for the event, the user can decide, based on the review of the event information steps 1-1, 1-2, 1-3 have provided, to accept the self-healing action in step 1-6 (Section 3.1.7) or deny the self-healing action in step 1-7 (Section 3.1.8). In both cases, the user can provide additional information or context about the self-healing for later record in step 1-5 (Section 3.1.6). Following states are possible if a self-healing option is available:

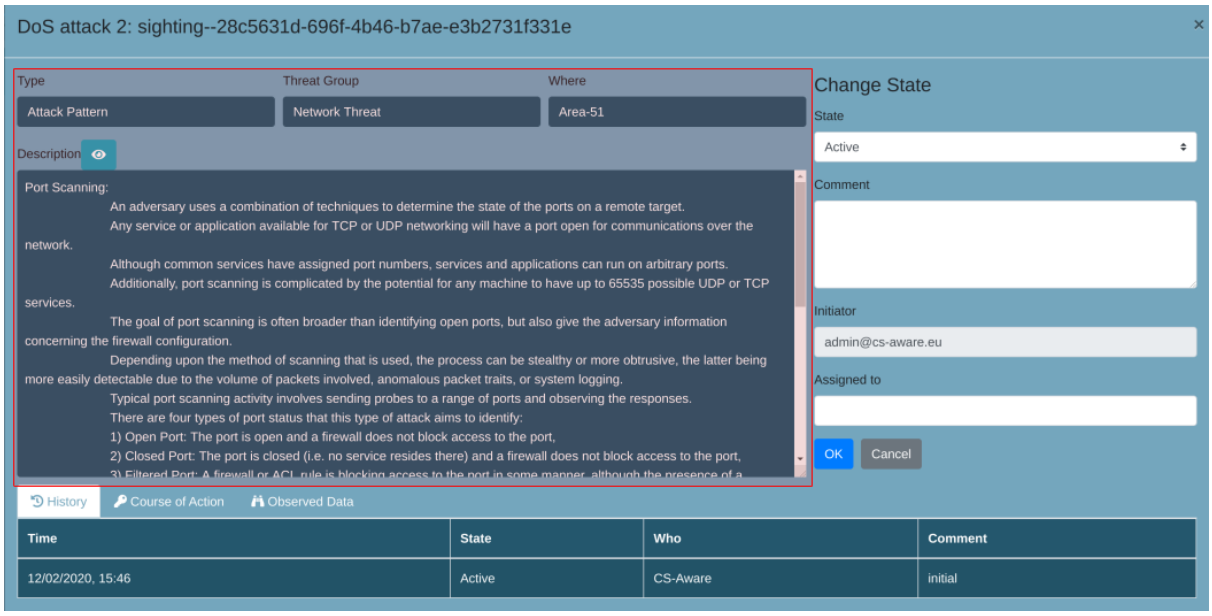
- In case self-healing is denied, the user has the option to resolve the event outside the CS-AWARE environment and resolve or ignore the event according to steps 1-10 and 1-11.
- In case the self-healing action is accepted, the CS-AWARE system gives visual feedback in the CS-AWARE threat overview about the success in step 1-8 (Section 3.1.9) or failure in step 1-9 (Section 3.1.10) of applying the self-healing action.
- In case self-healing failed, the event can be resolved outside the CS-AWARE environment and resolved/ignored according to steps 1-10 (Section 3.1.12) and 1-11 (Section 3.1.13).
- In case self-healing succeeded, the user has the option to comment and resolve the event in step 1-12 (Section 3.1.15).

After events have been resolved, the event state can be reviewed in the closed threats view in step 1-13 (Section 3.1.16) and the individual threat history in the threat details view in step 1-14 (Section 3.1.17 as an example of an event without self-healing, and Section 3.1.18 as an example of an event with self-healing).

3.1.1 Review CS-AWARE threat overview (Step 1-1)

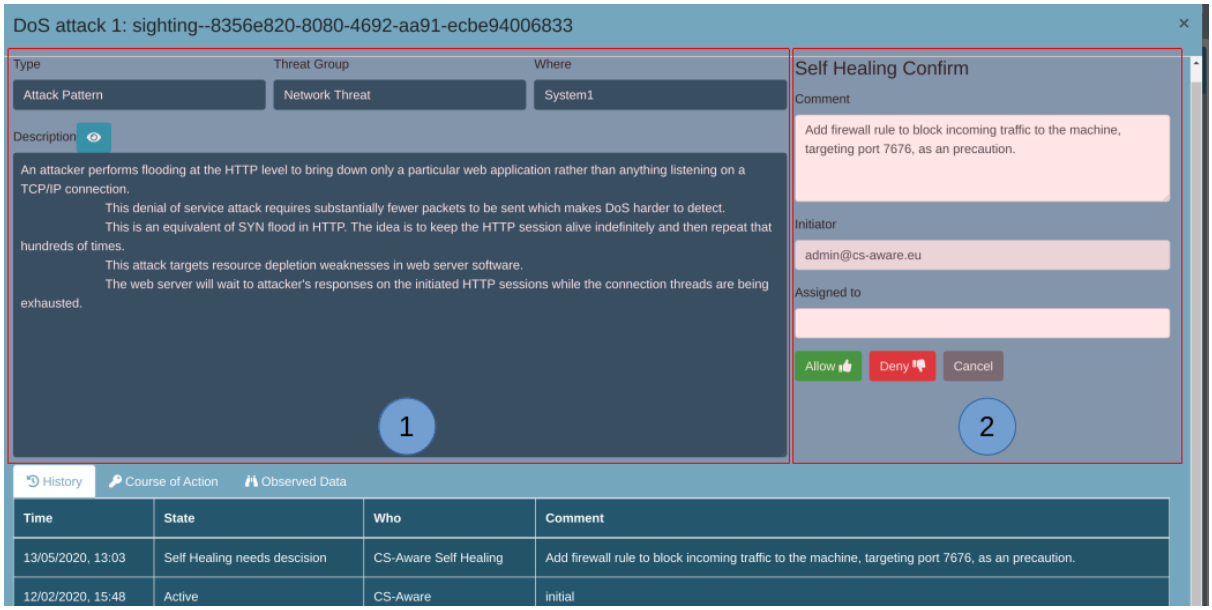
The CS-AWARE threat overview contains a visual representation of the existing events according to their threat classification and severity in the dart board on the left side. On the right side a list of existing events is listed, giving information about the severity state, date, person assigned to the event, threat classification, location of the event within the system and threat name. The shield symbol seen in the third event in the list indicates that a self-healing option is available.

3.1.2 Review threat details (without self-healing) (Step 1-2)



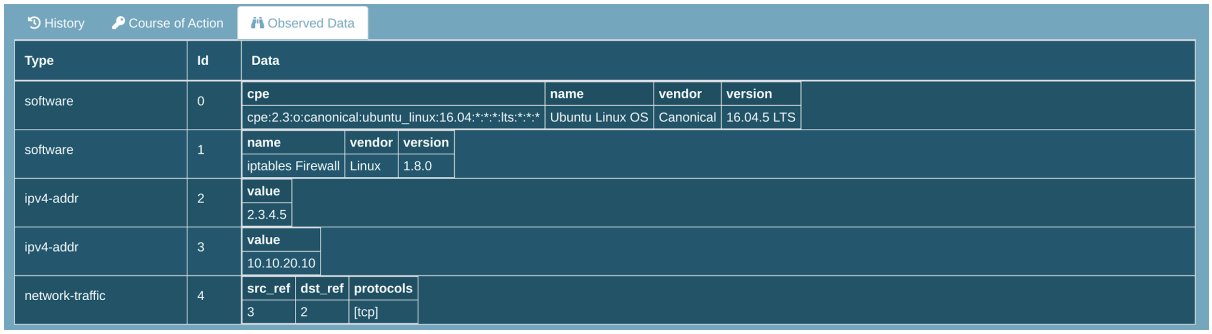
Each threat event has a detailed view that is accessible by clicking on the event in the CS-AWARE threat overview. The information given in this view includes the type of threat, the general threat group, the location within the system and a detailed description that can contain context as well as potential mitigation options to address the threat.

3.1.3 Review threat details view (with self-healing) (Step 1-2)



If self-healing is available for a specific threat event, the detailed threats view contains, in addition to the information provided in (1) and described in Section 3.1.2, information relating to the self-healing action provided (2). This includes a description of the self-healing option in the "comments" section, and the option to allow/deny the self-healing action.

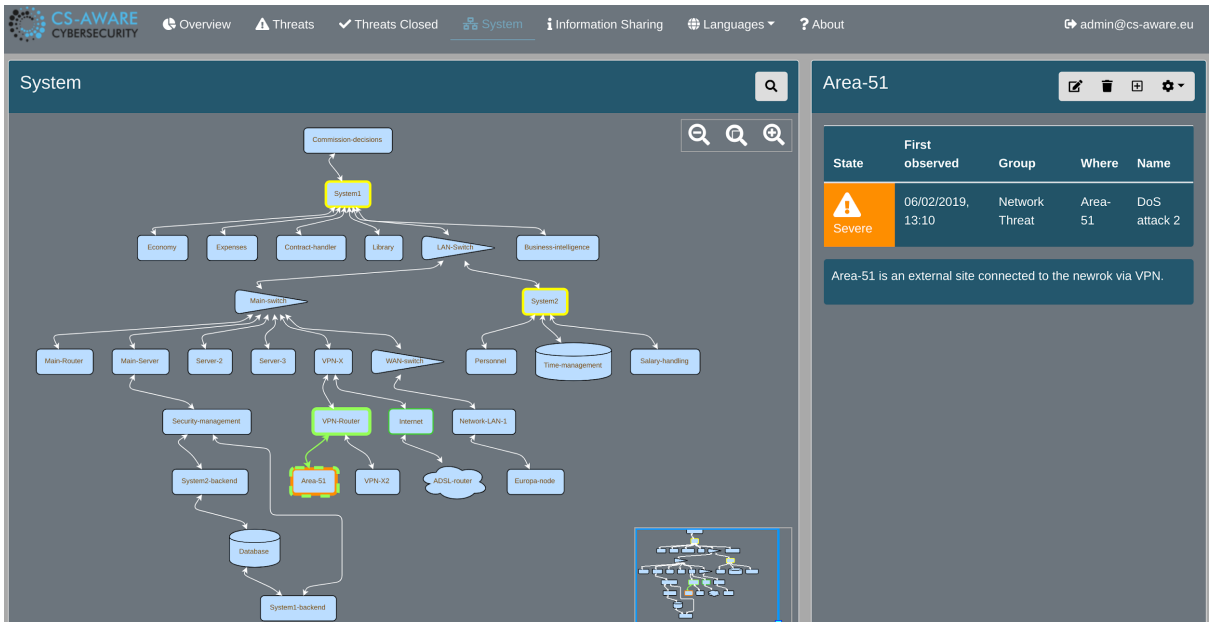
3.1.4 Review threat observed data details (Step 1-3)



Each threat event has a detailed accounting of the parameters that were used to detect and compile the event in the "Observed Data" tab. The concrete content of this tab is highly

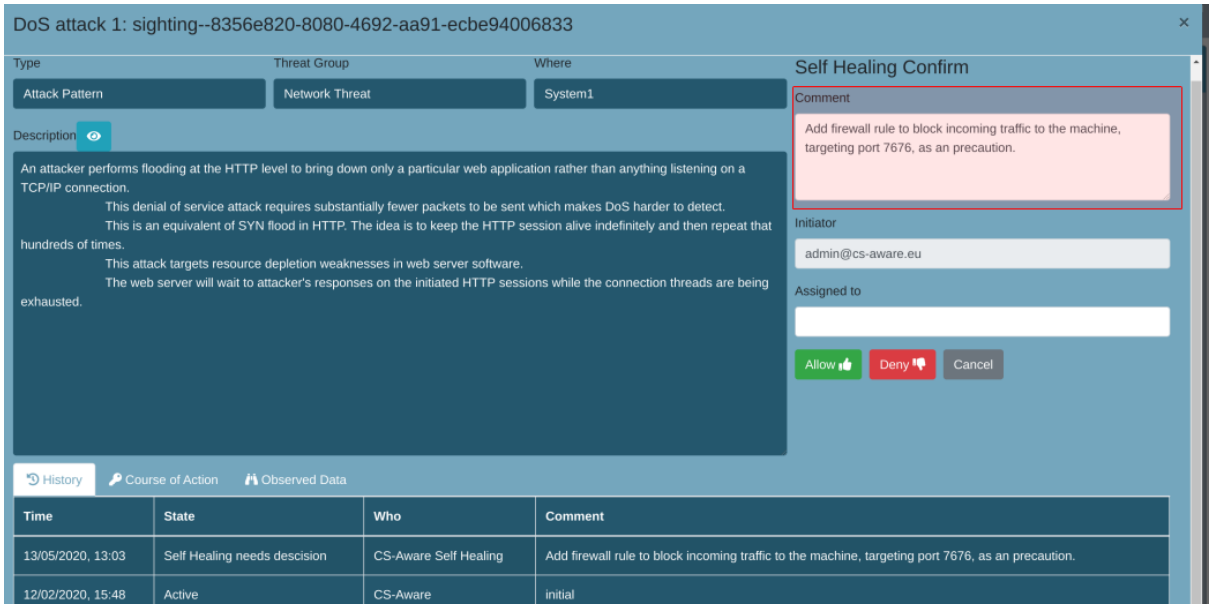
dependent on the defined monitoring pattern and the information sources that are utilized by those patterns.

3.1.5 Review system overview (Step 1-4)



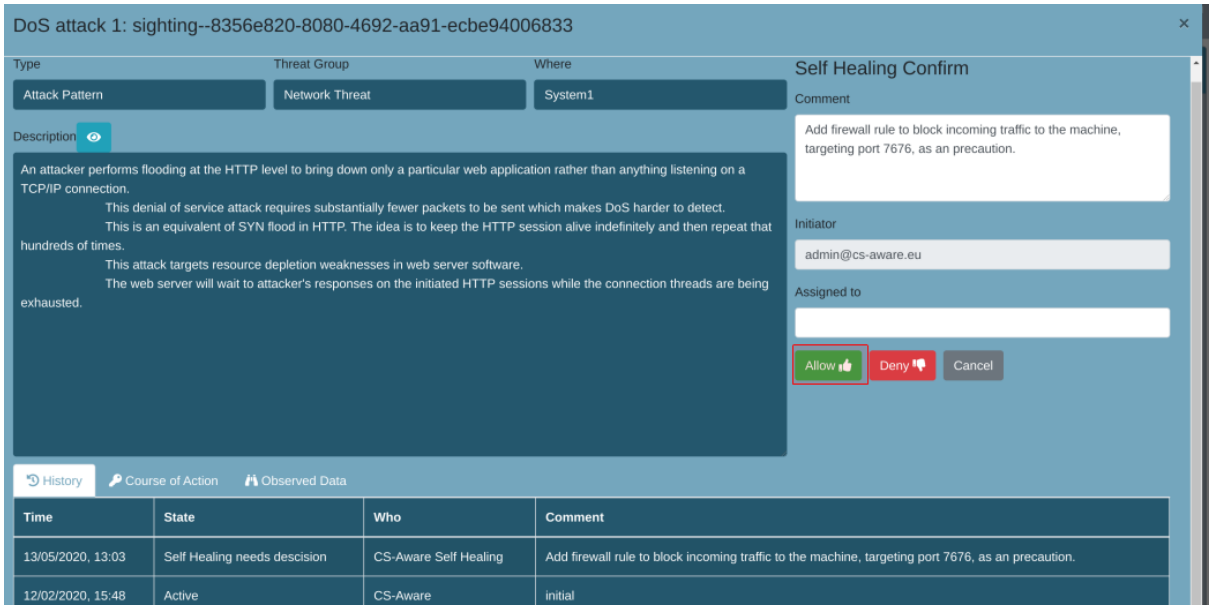
The system overview depicts the asset and dependency graph of the systems that are monitored. Threat events are visualized in this view at the location they were detected in, the severity is indicated by the different coloured borders of each node. The right side contains a description and other context information about each asset, as well as the list of threats that are associated to the asset.

3.1.6 Comment on self-healing action (Step 1-5)



The CS-AWARE system allows to give additional context to a self-healing action before allowing or denying the action in the "Comment" field. A description of the self-healing action is automatically provided by the CS-AWARE system, and can be modified/amended with additional information if necessary.

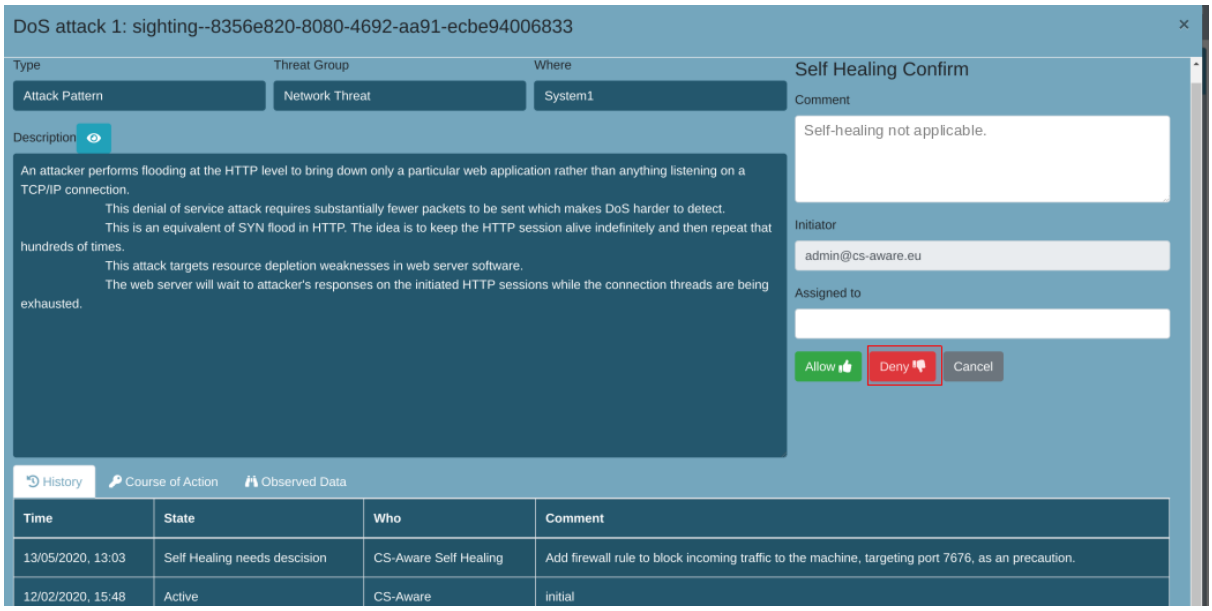
3.1.7 Accept self-healing (Step 1-6)



By clicking on the "Allow" button, the CS-AWARE system will automatically apply the provided self-healing action to the relevant system component. In the CS-AWARE threat

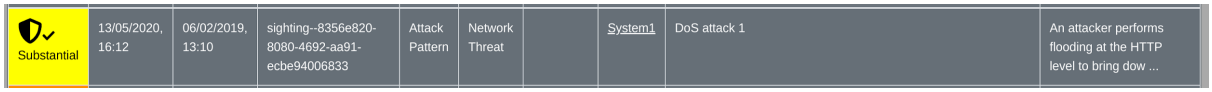
overview an accepted, but not yet applied, self-healing action is indicated with a thumbs up emoji:

3.1.8 Deny self-healing (Step 1-7)



By clicking on the “Deny” button, the self-healing option is ignored by the CS-AWARE system.

3.1.9 Self-healing succeeded state (Step 1-8)

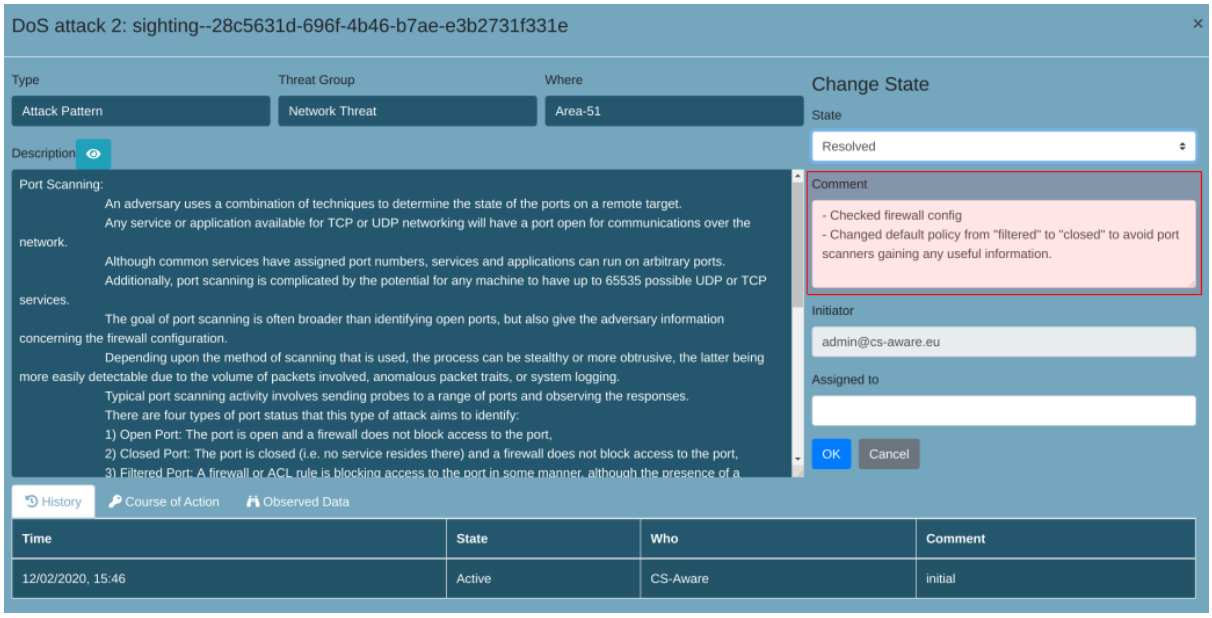


A successfully applied self-healing action is indicated with a check emoji in the CS-AWARE threat overview.

3.1.10 Self-healing failed state (Step 1-9)

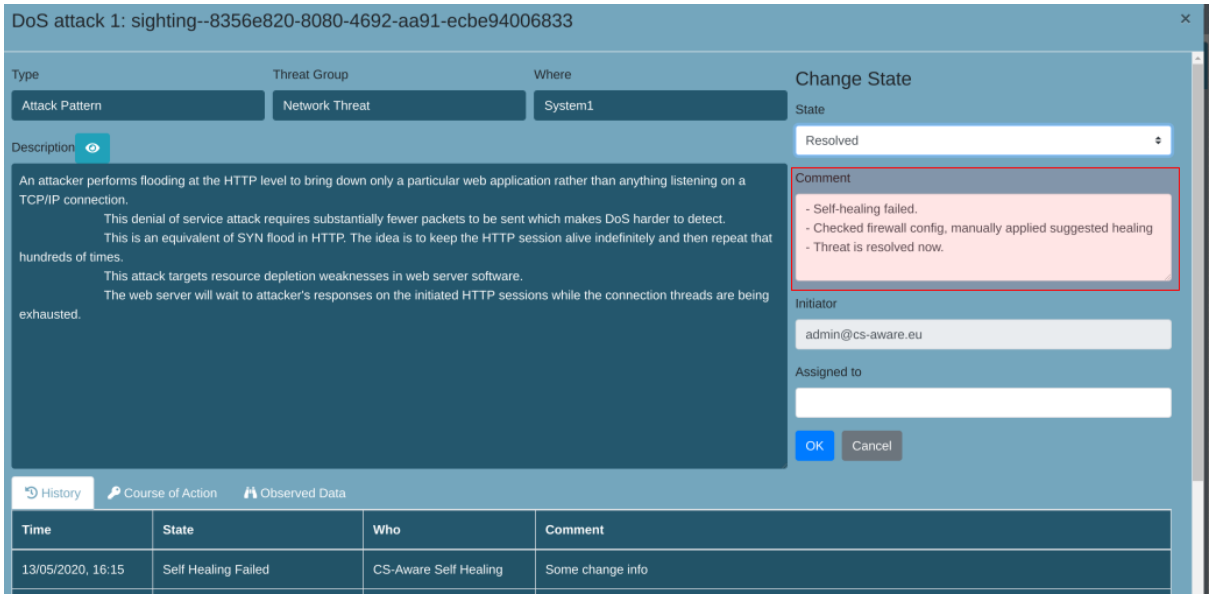
A failed self-healing action is indicated with a bolt emoji in the CS-AWARE threat overview.

3.1.11 Comment on course-of-action in threat details view (Step 1-10)



For later reference, a comment about the course-of-action taken to resolve an issue outside the CS-AWARE environment can be given.

3.1.12 Comment on course-of-action in threat details view (resolve after self-healing failed) (Step 1-10)



In case self-healing failed, a comment about the course-of-action taken to resolve the issue outside the CS-AWARE environment can be given.

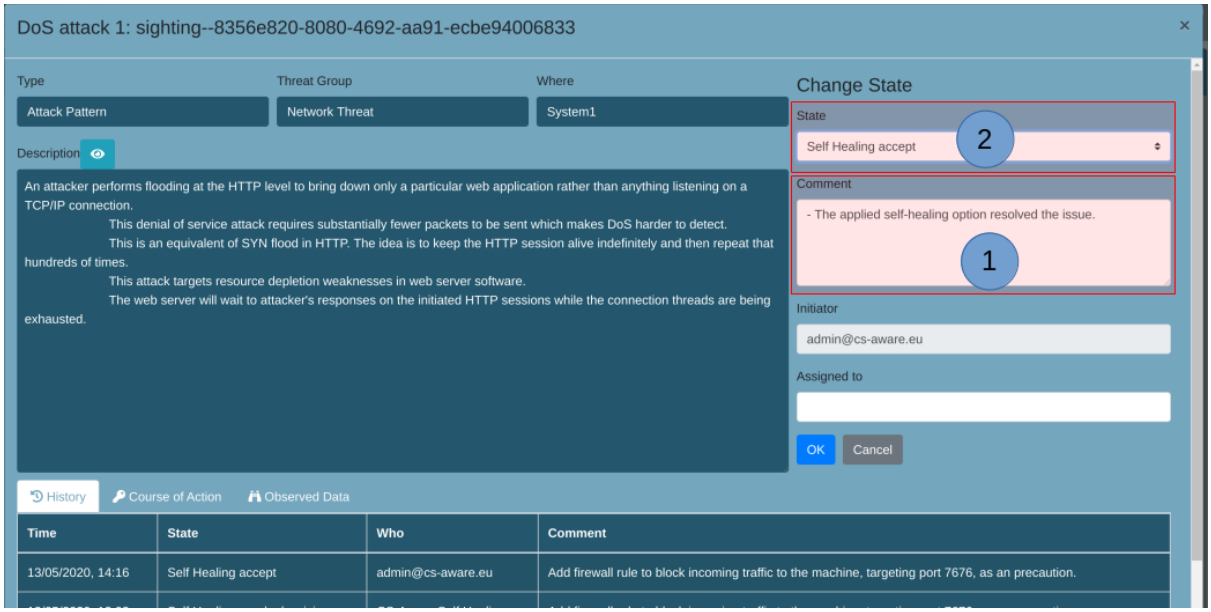
3.1.13 Mark threat state resolved/ignored in threat details view (resolved) (Step 1-11)

To resolve an event, the “State” is set to “Resolved” and applied by pressing the “OK” button.

3.1.14 Mark threat state resolved/ignored in threat details view (ignored) (Step 1-11)

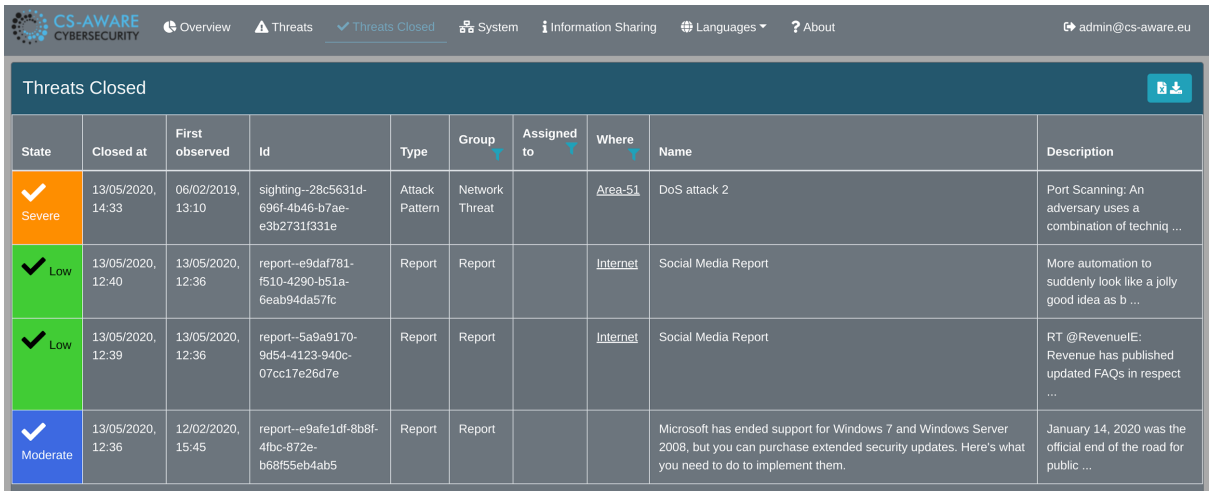
To resolve an event inside, the “State” is set to “Ignored” and applied by pressing the “OK” button.

3.1.15 Comment on self-healing and resolve in threat details view (Step 1-12)



After a self-healing action has been successfully applied, the user has the option to give additional information for future reference (1) and set the "State" to "Self Healing accept". Changes are applied by pressing the "OK" button.

3.1.16 Review resolved state in closed threats view (Step 1-13)



State	Closed at	First observed	Id	Type	Group	Assigned to	Where	Name	Description
Severe	13/05/2020, 14:33	06/02/2019, 13:10	sighting--28c5631d-696f-4b46-b7ae-e3b2731f331e	Attack Pattern	Network Threat		Area-51	DoS attack 2	Port Scanning: An adversary uses a combination of techniq ...
Low	13/05/2020, 12:40	13/05/2020, 12:36	report--e9daf781-f510-4290-b51a-6eab94da57fc	Report	Report		Internet	Social Media Report	More automation to suddenly look like a jolly good idea as b ...
Low	13/05/2020, 12:39	13/05/2020, 12:36	report--5a9a9170-9d54-4123-940c-07cc17e26d7e	Report	Report		Internet	Social Media Report	RT @RevenueIE: Revenue has published updated FAQs in respect ...
Moderate	13/05/2020, 12:36	12/02/2020, 15:45	report--e9afe1df-8b8f-4fbc-872e-b68f55eb4ab5	Report	Report			Microsoft has ended support for Windows 7 and Windows Server 2008, but you can purchase extended security updates. Here's what you need to do to implement them.	January 14, 2020 was the official end of the road for public ...

A record of the closed threat events ("resolved" or "ignored") can be found in the "Threats Closed" tab. Each event contains the same information as an open threat as described in Section 3.1.1. The check emoji indicates the closed state of the event.

3.1.17 Review threat history in threat details view (Step 1-14)

History | Course of Action | Observed Data

Time	State	Who	Comment
13/05/2020, 14:33	Resolved	admin@cs-aware.eu	- Checked firewall config - Changed default policy from "filtered" to "closed" to avoid port scanners gaining any useful information.
12/02/2020, 15:46	Active	CS-Aware	initial

The event "History" tab of each events detailed threat view presents an account of the steps taken to resolve the event. Each entry contains the time of the action, the state the event changed to, the person who conducted the action and the comment that was provided in this step.

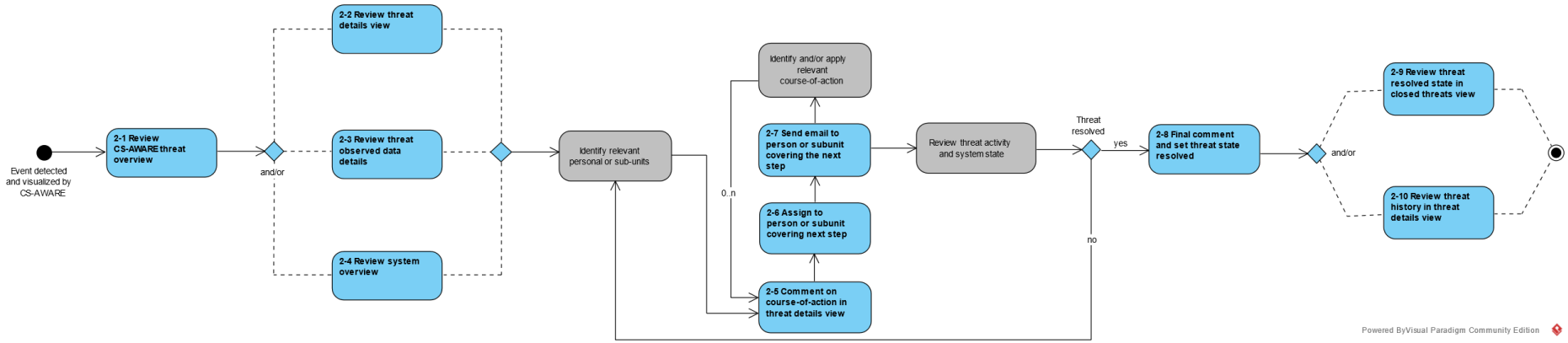
3.1.18 Review threat history in threat details view (with self-healing) (Step 1-14)

History | Course of Action | Observed Data

Time	State	Who	Comment
13/05/2020, 14:16	Self Healing accept	admin@cs-aware.eu	Add firewall rule to block incoming traffic to the machine, targeting port 7676, as an precaution.
13/05/2020, 13:03	Self Healing needs descision	CS-Aware Self Healing	Add firewall rule to block incoming traffic to the machine, targeting port 7676, as an precaution.
12/02/2020, 15:48	Active	CS-Aware	initial

The event "History" tab of each events detailed threat view presents an account of the steps taken to resolve the event. This example is similar to the event shown in Section 3.1.17, but shows the record of an event that had a self-healing action available. Each step in applying a self-healing action (e.g. "Self Healing needs decision" and "Self Healing accept") creates an entry in the event history.

3.2 Usage scenario 2: Threat handling (Complex organizational structure)



Scenario 2 represents a common usage scenario seen in large or metropolitan organization, in which the organizational responsibilities to maintain systems is split among many different departments/groups or is (partially) outsourced to external suppliers. In such a case, a security manager or security team would take responsibility of managing the events available in CS-AWARE, distributing tasks to the relevant persons or groups.

The first steps of this scenario (steps 2-1 to 2-4) are the same as steps 1-1 to 1-4 of scenario 1, described in Sections 3.1.1 to 3.1.5. In those steps the security manager gains awareness of the issues described by the threat event detected by CS-AWARE, via the CS-AWARE threat overview and/or the threat details view and/or the observed data tab and/or the system overview.

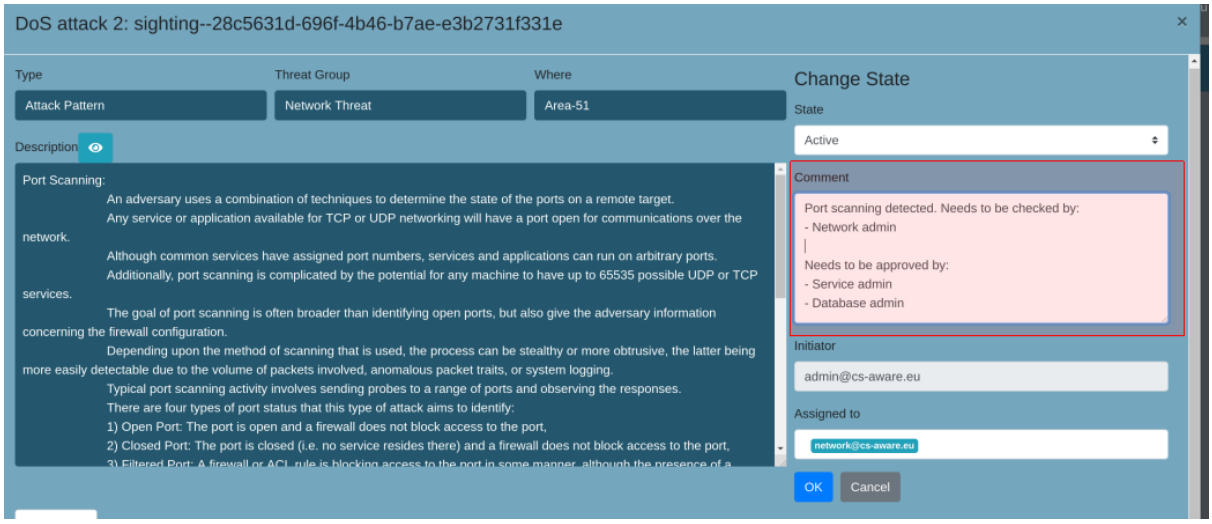
Once the security manager has identified the relevant persons or groups, the observations of the security manager are provided as comment in step 2-5 (Section 3.2.1), assigned to the first person or group to work on the issue in step 2-6 (Section 3.2.2) and send an email to that person or group in step 2-7 (Section 3.2.3). In this particular example, the security manager has identified that the network group, the service group and the database group need to be involved in this case, with the network group being the first to act.

The network group will, based on the information provided by CS-AWARE and the security manager, identify and/or apply the relevant course of action (or self-healing action, if available) and assign the event to the next relevant group (steps 2-5 to 2-7). The identification and or application of a course-of-action, as well as steps 2-5 to 2-7 are repeated till all identified persons or groups are satisfied that the threat event was resolved, and the event is assigned back to the security manager. Examples of this process for steps 2-5 and 2-6 for this particular example with a network group, a service group and a database group are described in Sections 3.2.4 to 3.2.6.

The security manager reviews the system and threat state after the threat event was assigned back. If issues still persist, a new round of identification of relevant persons or groups and assignment of tasks will be triggered. If the security manager is satisfied that the event is resolved, the manager can provide a final comment before setting the event state resolved in step 2-8 (Section 3.2.7).

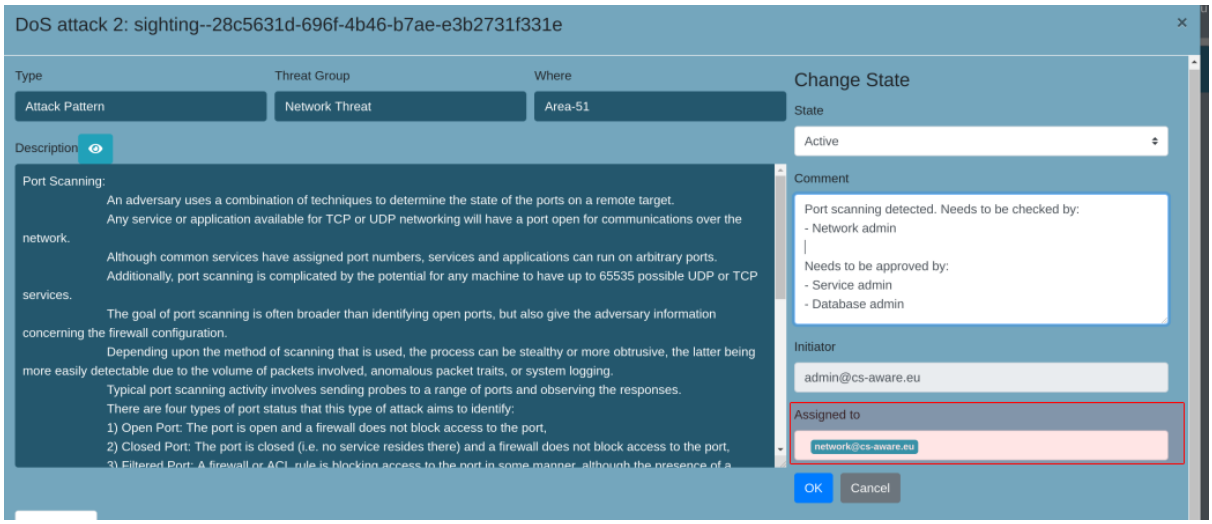
Similar to scenario 1, the event state can be reviewed in the closed threat view 2-9 (like shown in scenario 1 Section 3.1.16) and the threat details view of the relevant event in step 2-10 (Section 3.2.8).

3.2.1 Comment on course-of-action in threat details view (security manager) (Step 2-5)



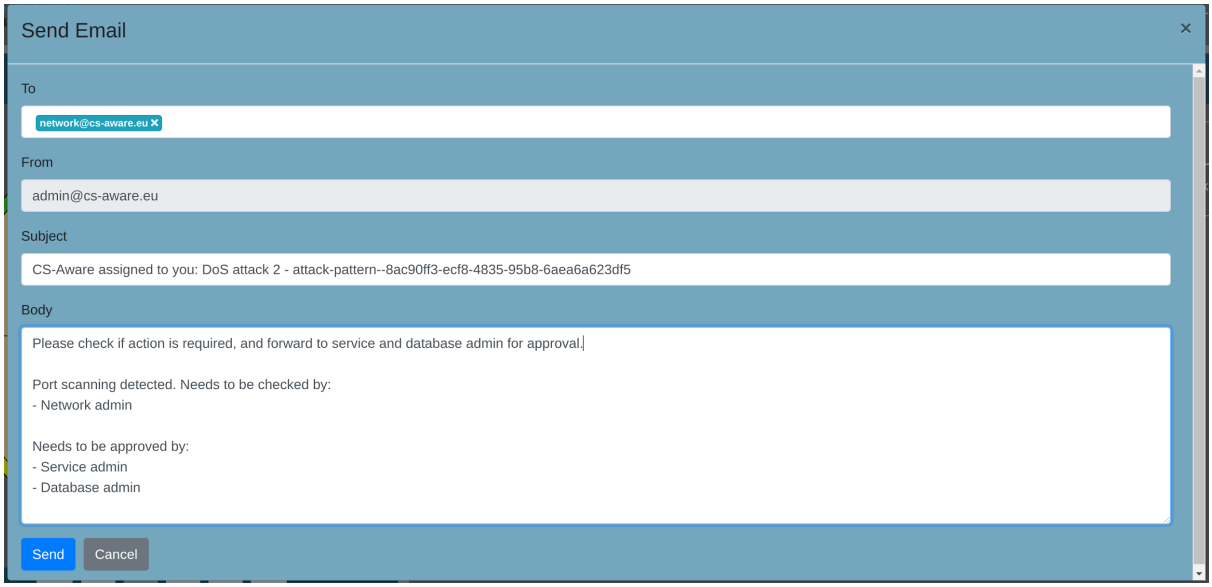
The security manager has the option to communicate the initial assessment of the issues in the "Comments" section of the event in the detailed threats view before assigning it to the relevant person or dealing with resolving the issues.

3.2.2 Assign to person or sub-unit covering next step (security manager) (Step 2-6)



The detailed threats view allows to assign the responsibility for the event to those persons or groups that are in charge of resolving them in the "Assigned to" field. A user account within the CS-AWARE system is required for the assignment functionality.

3.2.3 Send email to person or subunit covering the next step (security manager) (Step 2-7)



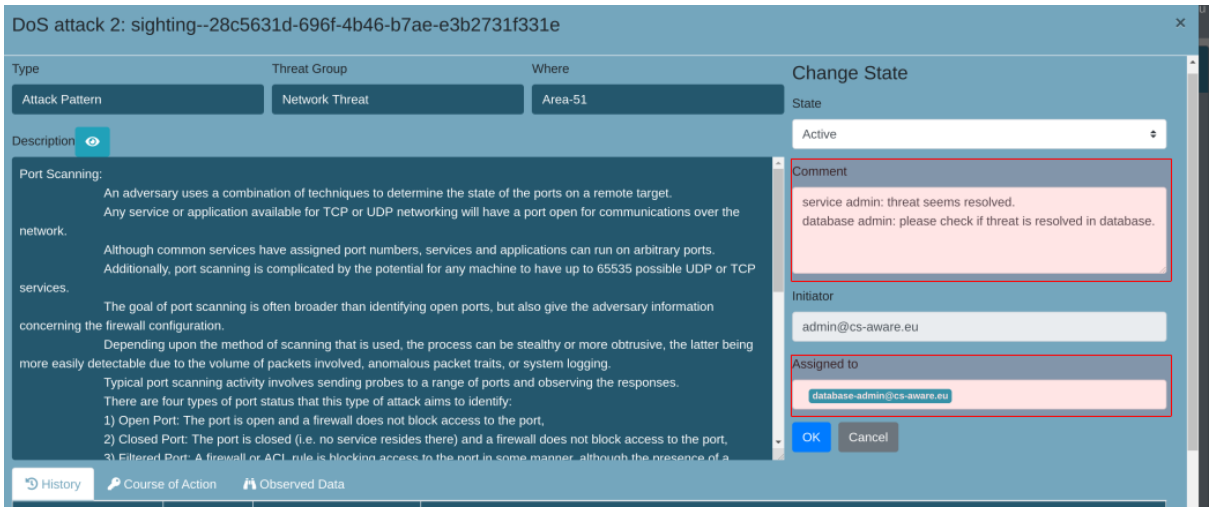
The CS-AWARE system automatically generates an email template containing the threat event name/ ID in the subject, and the comment provided in step 2-5 (Section 3.2.1) as body. The email message can be amended with a more personal message that will not be part of the threat event history. In the CS-AWARE threat overview, the current assignment of the threat event can be seen in the "Assigned to" field:

State	First observed	Assigned to	Group	Where	Name
Moderate	06/02/2019, 13:10	network@cs-aware.eu	Network Threat	Area-51	DoS attack 2

3.2.4 Comment on course-of-action in threat details view and assign to person or subunit covering next step (network group) (Steps 2-5 and 2-6)

In this example, the network group has the possibility to comment on the threat event state and/or course-of-action taken before assigning it to the next relevant person or group.

3.2.5 Comment on course-of-action in threat details view and assign to person or subunit covering next step (service group) (Steps 2-5 and 2-6)

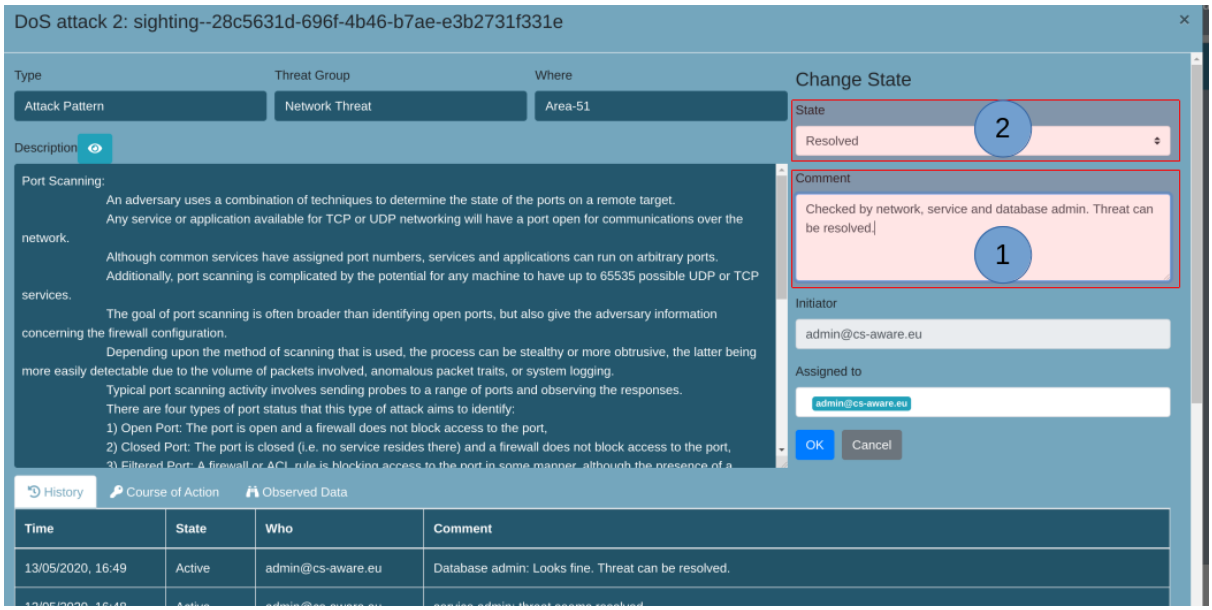


In this example, the service group has the possibility to comment on the threat event state and/or course-of-action taken before assigning it to the next relevant person or group.

3.2.6 Comment on course-of-action in threat details view and assign to person or subunit covering next step (database group) (Steps 2-5 and 2-6)

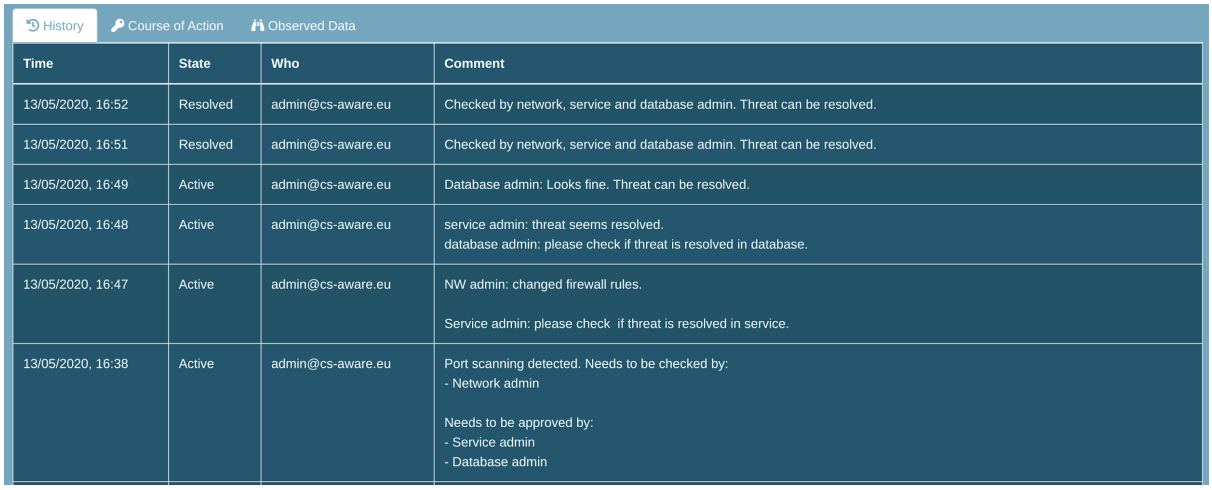
In this example, the database group has the possibility to comment on the threat event state and/or course-of-action taken before assigning it to the next relevant person or group.

3.2.7 Final comment and set threat state resolved (Step 2-8)



Once all relevant persons or groups relevant for resolving the threat event have implemented a course-of-action and/or provided a comment/opinion about the threat state, and the threat is considered resolved, the security manager has the ability to provide a final comment (1) before setting the threat state resolved (2).

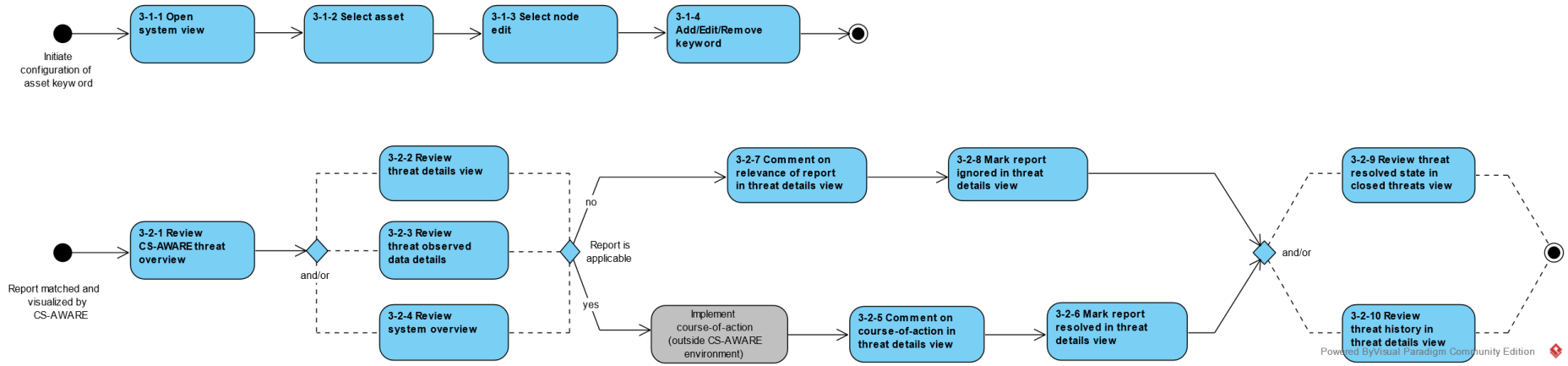
3.2.8 Review threat history in detailed threats view (Step 2-10)



Time	State	Who	Comment
13/05/2020, 16:52	Resolved	admin@cs-aware.eu	Checked by network, service and database admin. Threat can be resolved.
13/05/2020, 16:51	Resolved	admin@cs-aware.eu	Checked by network, service and database admin. Threat can be resolved.
13/05/2020, 16:49	Active	admin@cs-aware.eu	Database admin: Looks fine. Threat can be resolved.
13/05/2020, 16:48	Active	admin@cs-aware.eu	service admin: threat seems resolved. database admin: please check if threat is resolved in database.
13/05/2020, 16:47	Active	admin@cs-aware.eu	NW admin: changed firewall rules. Service admin: please check if threat is resolved in service.
13/05/2020, 16:38	Active	admin@cs-aware.eu	Port scanning detected. Needs to be checked by: - Network admin Needs to be approved by: - Service admin - Database admin

This example provides the history of the threat event record, including the initial assessment by the security manager, the comments on course-of-action and/or status of the different persons/groups involved in resolving the threat, and the final assessment by the security manager.

3.3 Usage scenario 3: Social media report handling

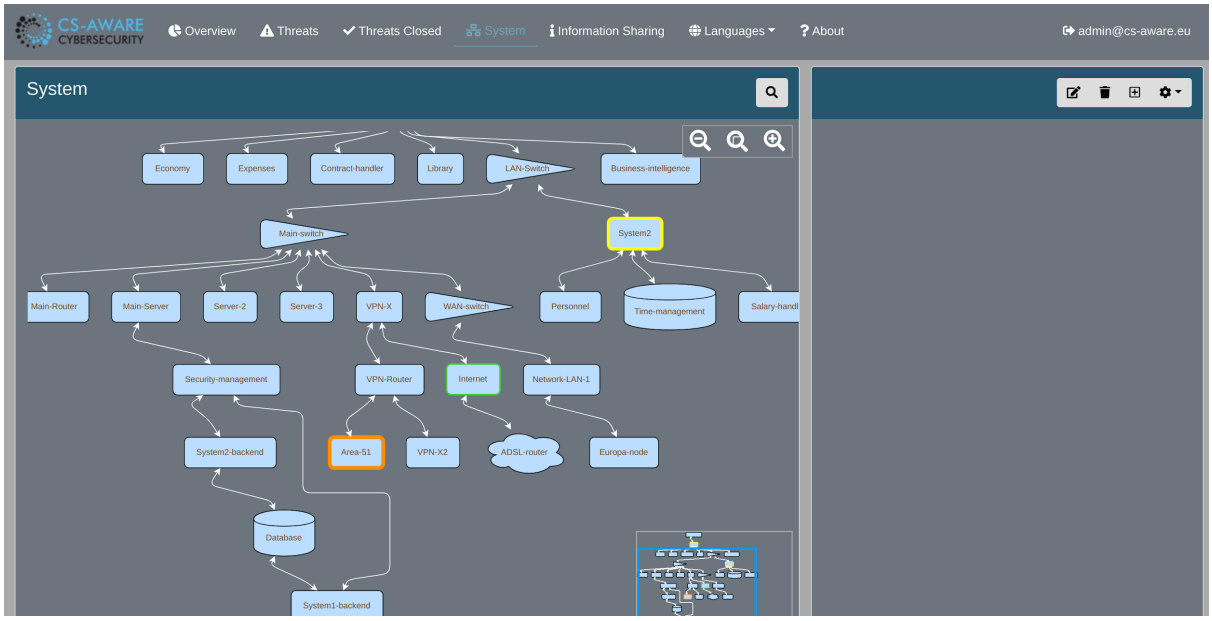


This scenario describes the use case where context specific security messages from relevant external information sources are handled. In CS-AWARE this is achieved by defining relevant keywords for assets, which will be monitored for by the CS-AWARE system in the available data sources like social media. This scenario involves two processes, the definition of keywords per asset, which is described in Section 3.3.1, and the handling of events that are triggered based on those keywords as described in Section 3.3.2.

3.3.1 Add keywords (Steps 3-1-X)

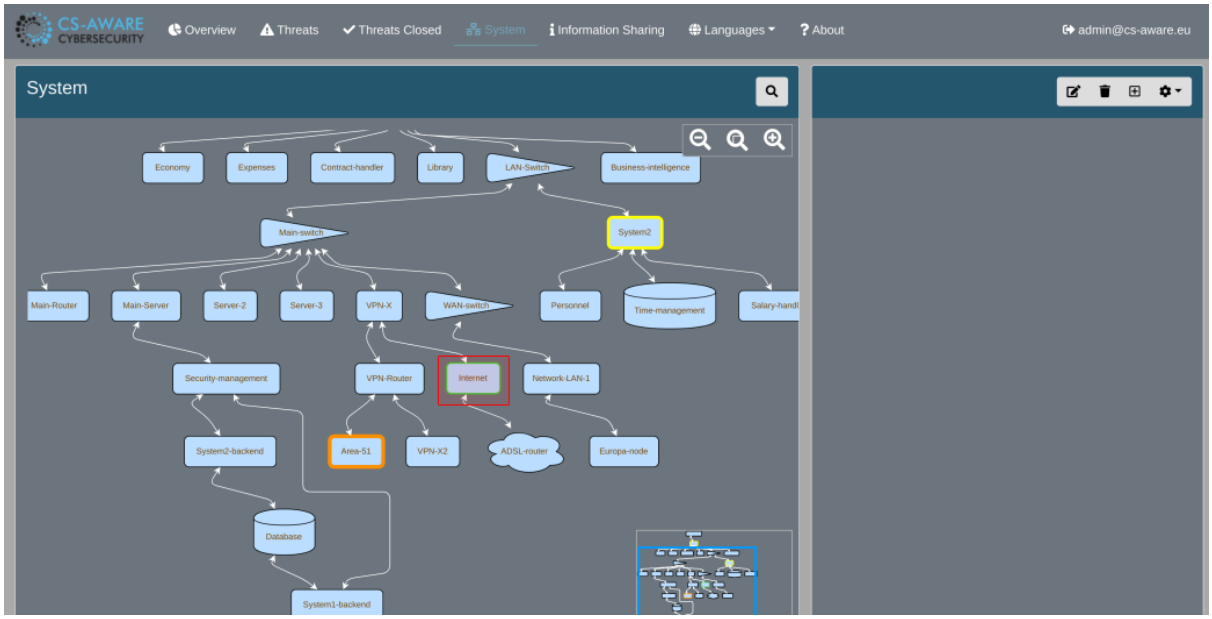
Keywords for monitoring of security events are defined on a per-asset basis in the "System" overview in step 3-1-1 (Section 3.3.1.1) by selecting the desired asset in step 3-1-2 (Section 3.3.1.2), pressing the node edit button in step 3-1-3 (Section 3.3.1.3) and adding/editing/removing the desired keywords in the "Categories" section of the node details in step 3-1-4 (Section 3.3.1.4).

3.3.1.1 Open system view (Step 3-1-1)



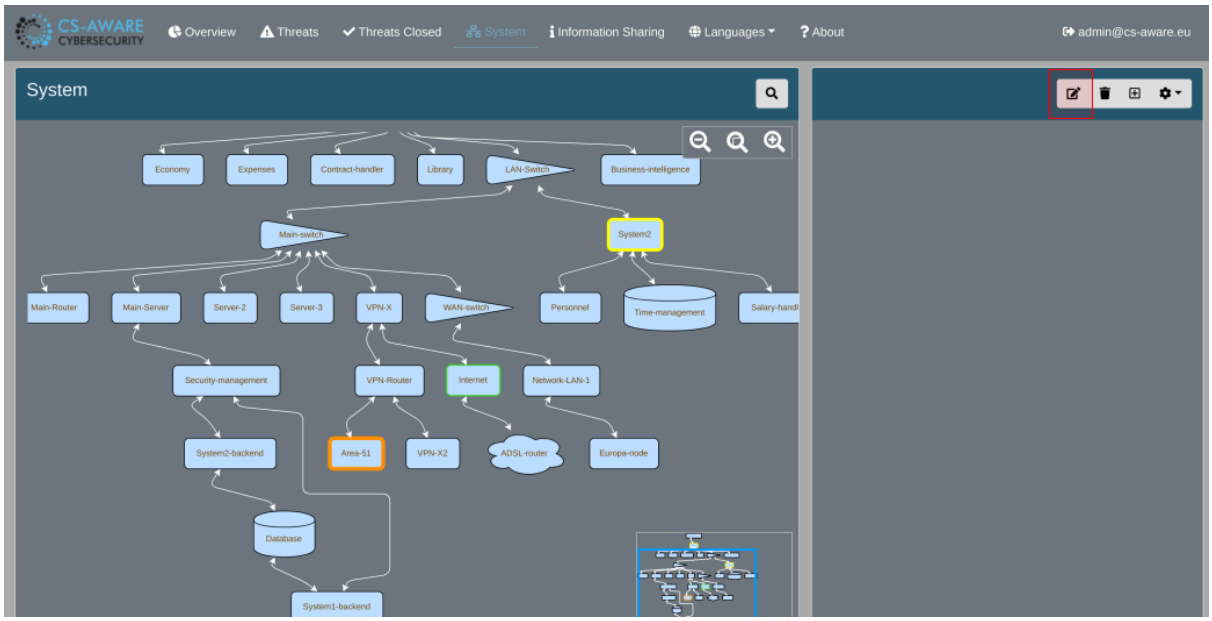
The system overview allows to review and edit the system asset and dependency structure, and to provide additional information for each asset node.

3.3.1.2 Select asset (Step 3-1-2)



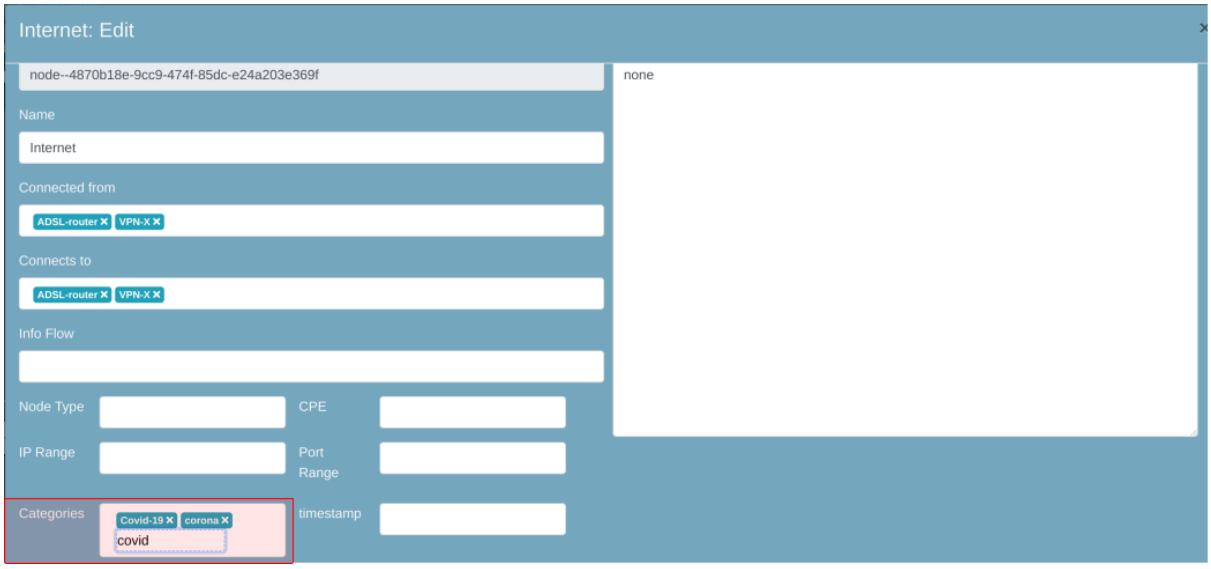
Specific assets can be selected by clicking on them.

3.3.1.3 Select node edit (Step 3-1-3)



Assets properties can be modified by clicking the node edit button.

3.3.1.4 Add/Edit/Remove keyword (Step 3-1-4)



In the node details view, the "Categories" section allows to add/remove/edit context specific keywords to be monitored for in external information sources like social media.

3.3.2 Check keyword-based events (Steps 3-2-X)

Security messages that are triggered by per-asset based keyword search are handled in a similar fashion than more specific security threats as described in usage scenarios 1 and 2. Such events are visualized by the CS-AWARE system as reports, e.g. "Social media reports" with a "Low" threat state by default.

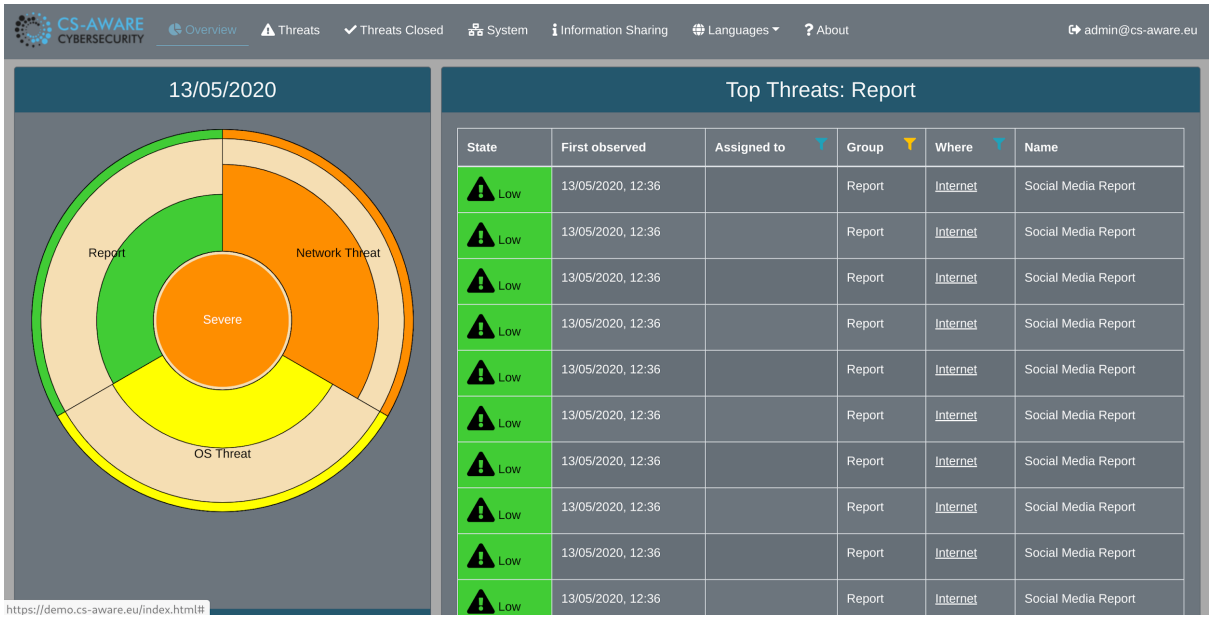
User interaction with such events follows the same interaction principles as all other threat events. A user is able to gain awareness of a security warning event displayed in the CS-AWARE threat overview in step 3-2-1 (Section 3.3.2.1) by observing the information provided in the detailed threat view in step 3-2-2 (Section 3.3.2.2) and/or the threat observed data details in step 3-2-3 (Section 3.3.2.3) and/or the location of an event in the systems view in step 3-2-4 (Section 3.3.2.4).

If the event is considered not applicable, the user has the ability to comment on the applicability of the message in step 3-2-7 (Section 3.3.2.7) and set the event state "ignored" in step 3-2-8 (Section 3.3.2.8).

If the event is applicable, the user can implement a relevant course-of-action outside the CS-AWARE environment based on the awareness gained though CS-AWARE, comment on the course-of-action in step 3-2-5 (Section 3.3.2.5) and set the event state "resolved" in step 3-2-6 (Section 3.3.2.6).

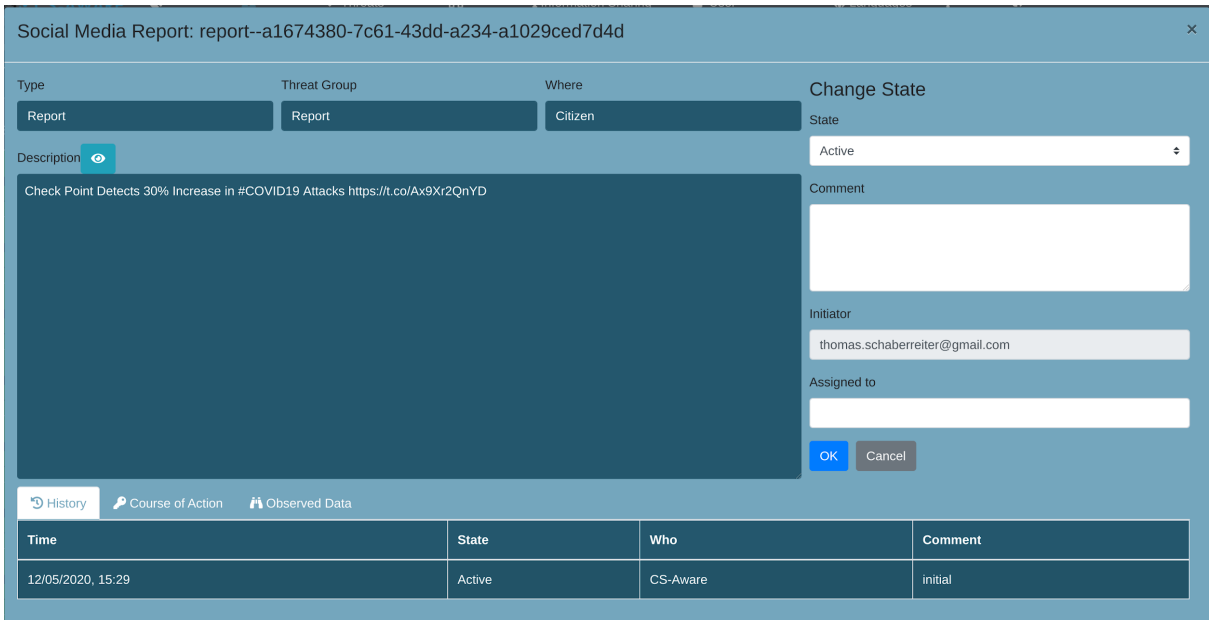
After events have been resolved, the event state can be reviewed in the closed threats view in step 3-2-9 (as described in scenario 1, Section 3.1.16) and the individual threat history in the threat details view in step 3-2-10 (as described in scenario 1 Section 3.1.17).

3.3.2.1 Review CS-AWARE threat overview (Step 3-2-1)



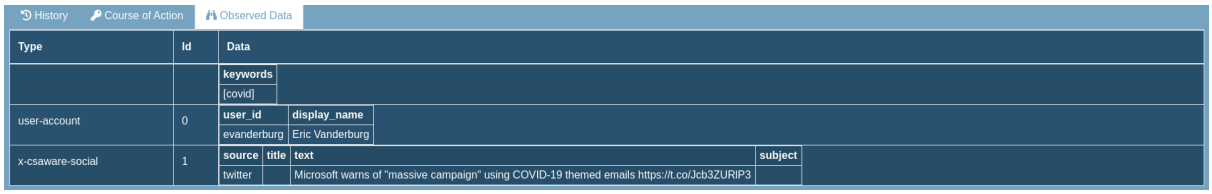
Keyword based security messages from external information sources like social media are displayed in the dartboard view on the left side in the "Report" category, and in the threats list on the right under the "Name" category as report, e.g. "Social Media Report". The event "State" of this type of events is "Low by default."

3.3.2.2 Review threat details view (Step 3-2-2)



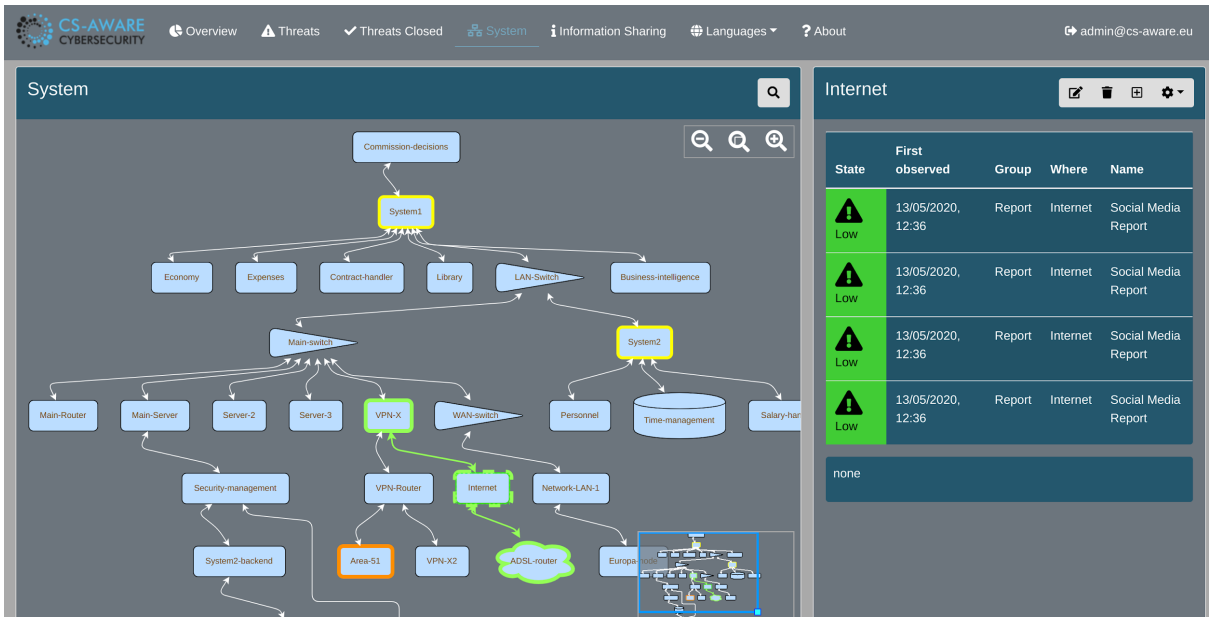
The threat details view of a keyword based report is the same as for all other types of threats. The view provides information about the “Type” and “Threat group” – which is defined as “Report” for this type of messages. The “Location” corresponds to the asset in the “system view” for which the triggering keyword was defined for. The “Description” field contains the actual message.

3.3.2.3 Review threat observed data details (Step 3-2-3)



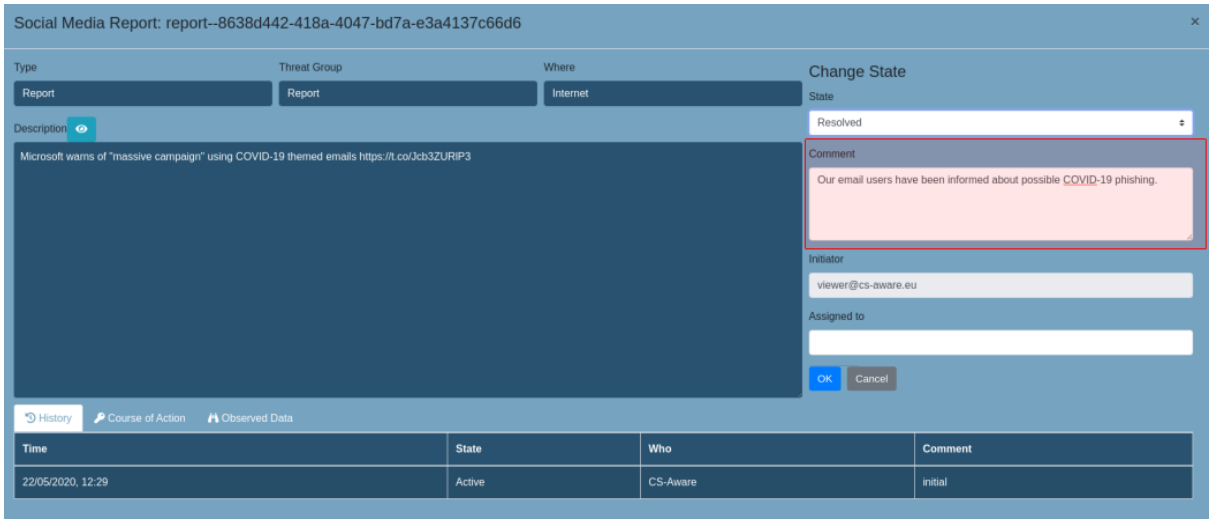
The threat event observed data details tab contains additional information about the message, like the triggering keywords or information about the source and origin of the message.

3.3.2.4 Review system overview (Step 3-2-4)



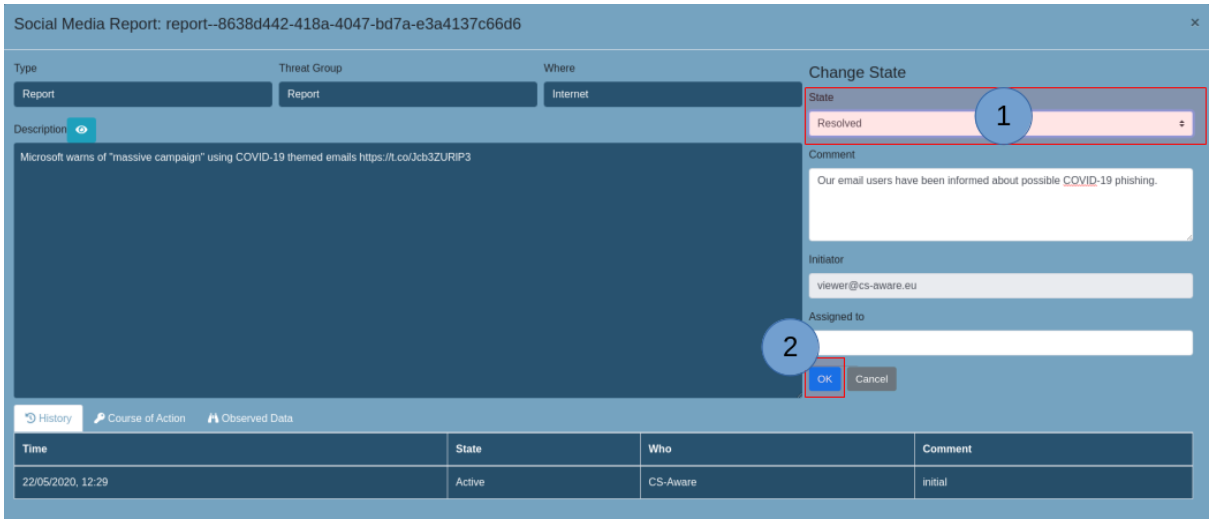
In the systems overview, security messages that were triggered by keywords are displayed in the same way as other threat events, and give awareness about potential dependencies that might be affected by such an event. Coloured node borders indicate the severity state of threat events associated to the node. When a node is selected, the associated threats including keyword-based security messages that were triggered by keywords defined for that particular asset are displayed on the right of the view.

3.3.2.5 Comment on course-of-action in threat details view (Step 3-2-5)



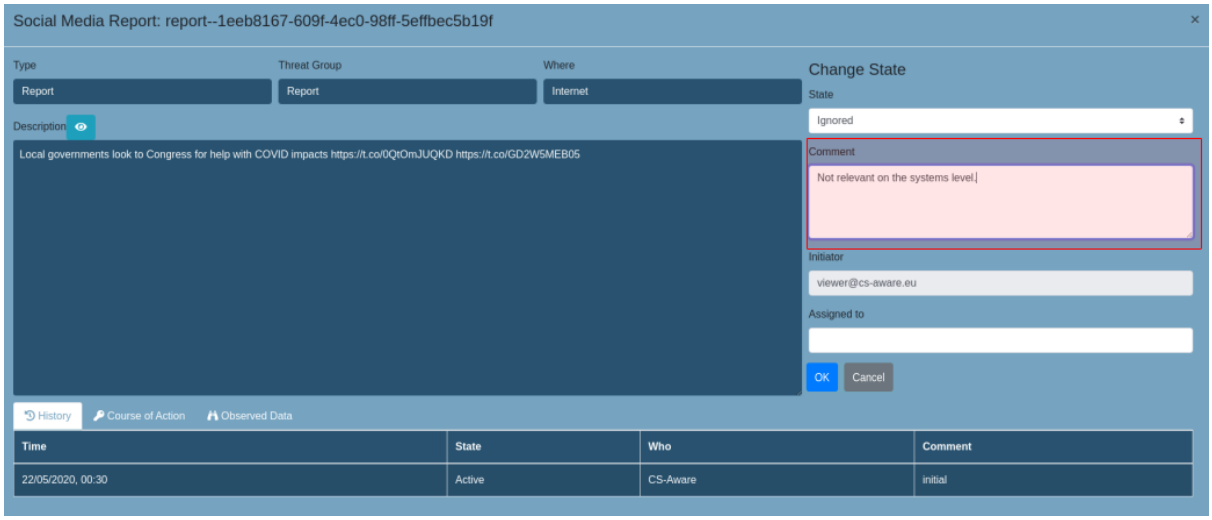
A user can comment on the course-of-action to resolve the keyword-based security message in the "Comment" section of the threat details view.

3.3.2.6 Mark report resolved in threat details view (Step 3-2-6)



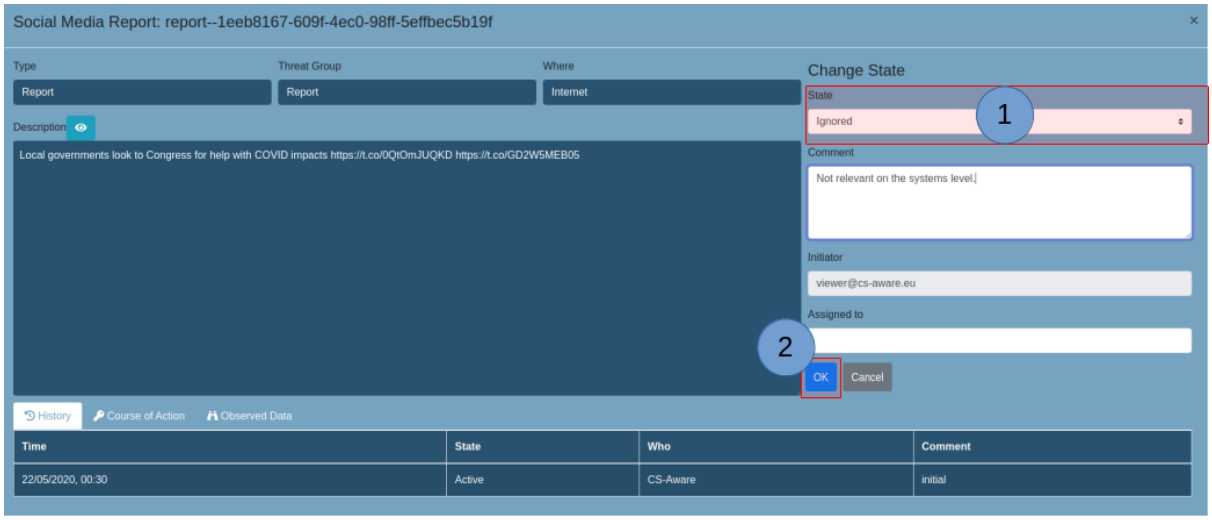
A keyword-based security message can be resolved by setting the "State" to resolved (1) and accepting the change by pressing "OK" (2).

3.3.2.7 Comment on relevance of report in threat details view (Step 3-2-7)



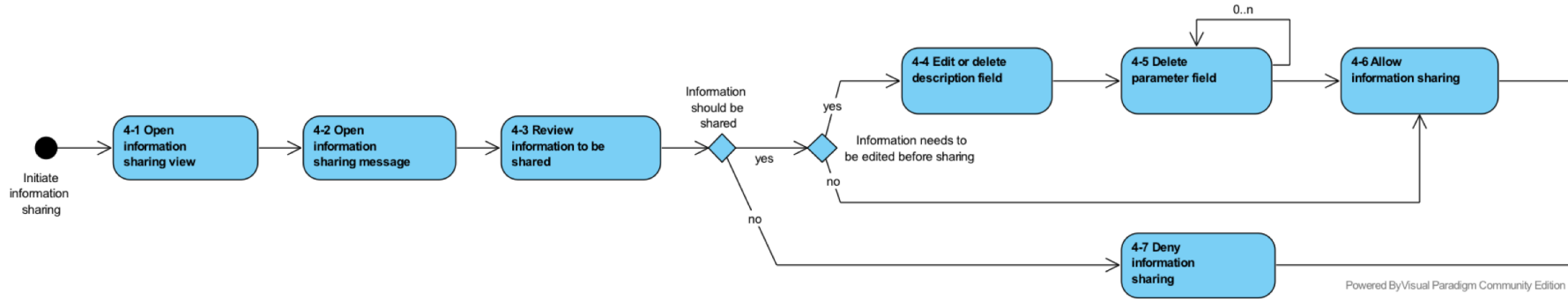
A user can comment on the applicability of a keyword-based security message in the "Comment" section of the threat details view.

3.3.2.8 Mark report ignored in threat details view (Step 3-2-8)



A keyword-based security message can be ignored by setting the "State" to "ignored" (1) in the threat details view and accepting the change by pressing "OK" (2).

3.4 Usage scenario 4: Information sharing



Scenario 4 describes the process of sharing information about security incidents detected by the CS-AWARE system with security communities external to the organization, in order to provide security experts with additional data that can help to better identify and classify threats, and devise better prevention and mitigation mechanisms.

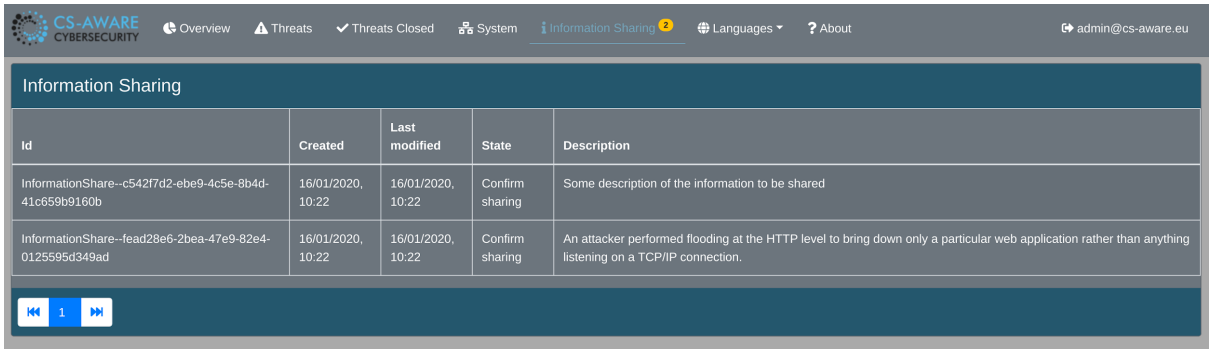
CS-AWARE automatically provides the option to share information about relevant incidents in the information sharing view in step 4-1 (Section 3.4.1). Clicking on an event in this view opens the information sharing details view for that message in step 4-2 (Section 3.4.2). This view is intended to allow reviewing the information to be shared with external communities in step 4-3 (Section 3.4.3), and allows to edit and/or delete information that is considered personal and/or sensitive and should thus not be shared outside the organizational context.

The user can decide not to share any information about the event by denying the information sharing for this event in step 4-7 (Section 3.4.7).

If the user decides to share the message, there are options available to edit the threat description field to give additional context, or delete the field in step 4-4 (Section 3.4.4).

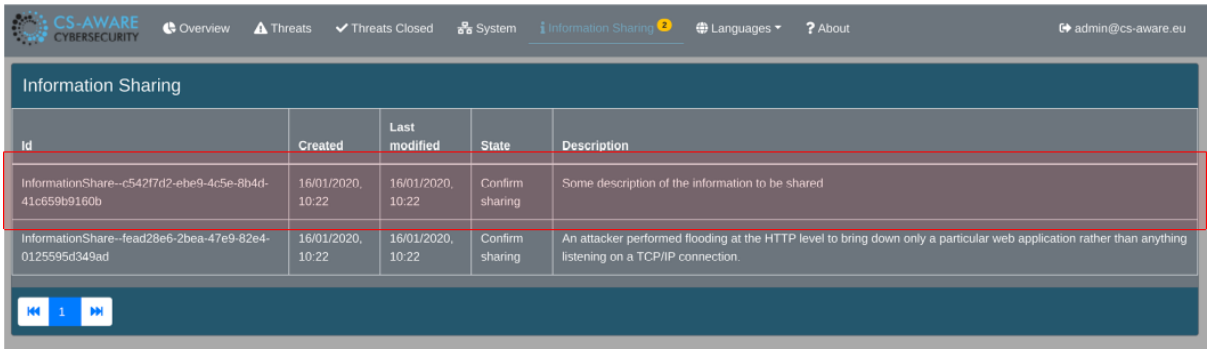
Furthermore, each parameter that is available for sharing can be deleted individually in step 4-5 (Section 3.4.5) before sharing the information in step 4-6 (Section 3.4.6).

3.4.1 Open information sharing view (Step 4-1)



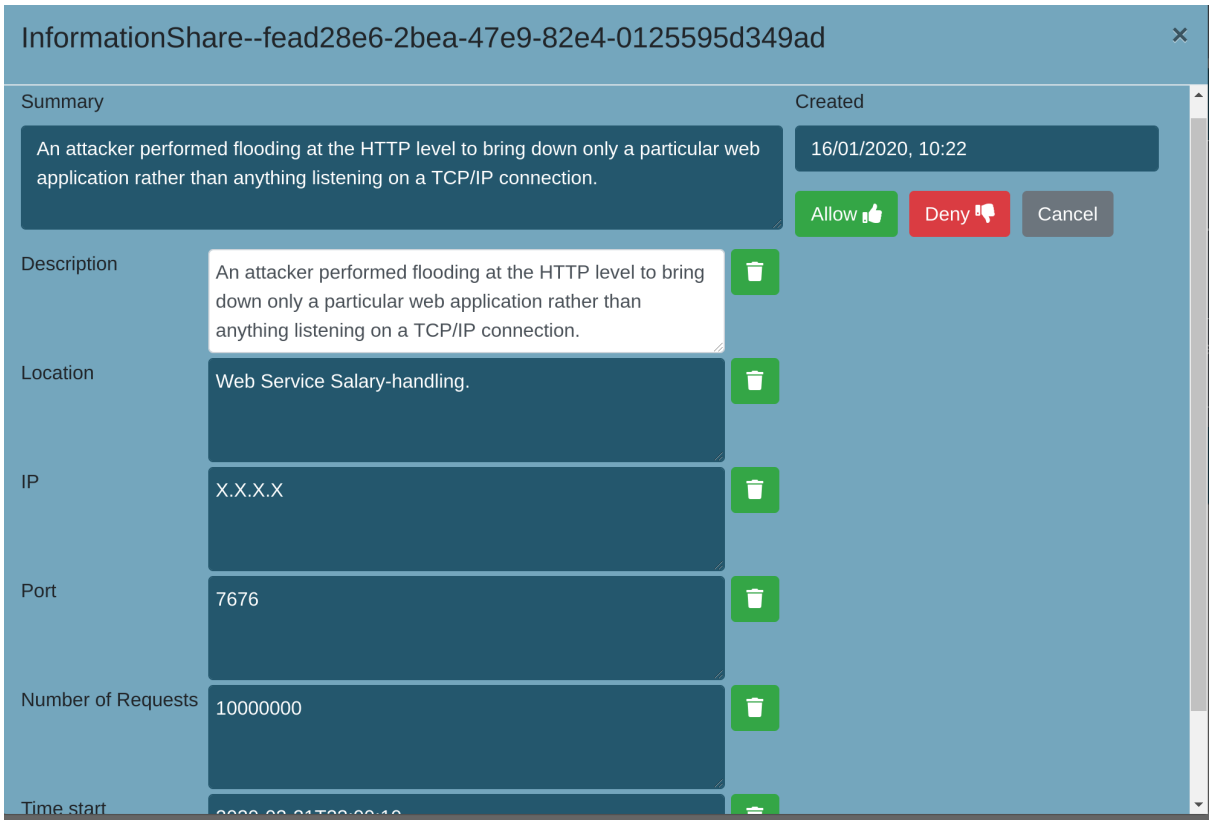
The information sharing view of the CS-AWARE system lists, for each sharing event, the unique ID, the date the event was created and last modified, the current state as well as the sharing event description.

3.4.2 Open information sharing message (Step 4-2)



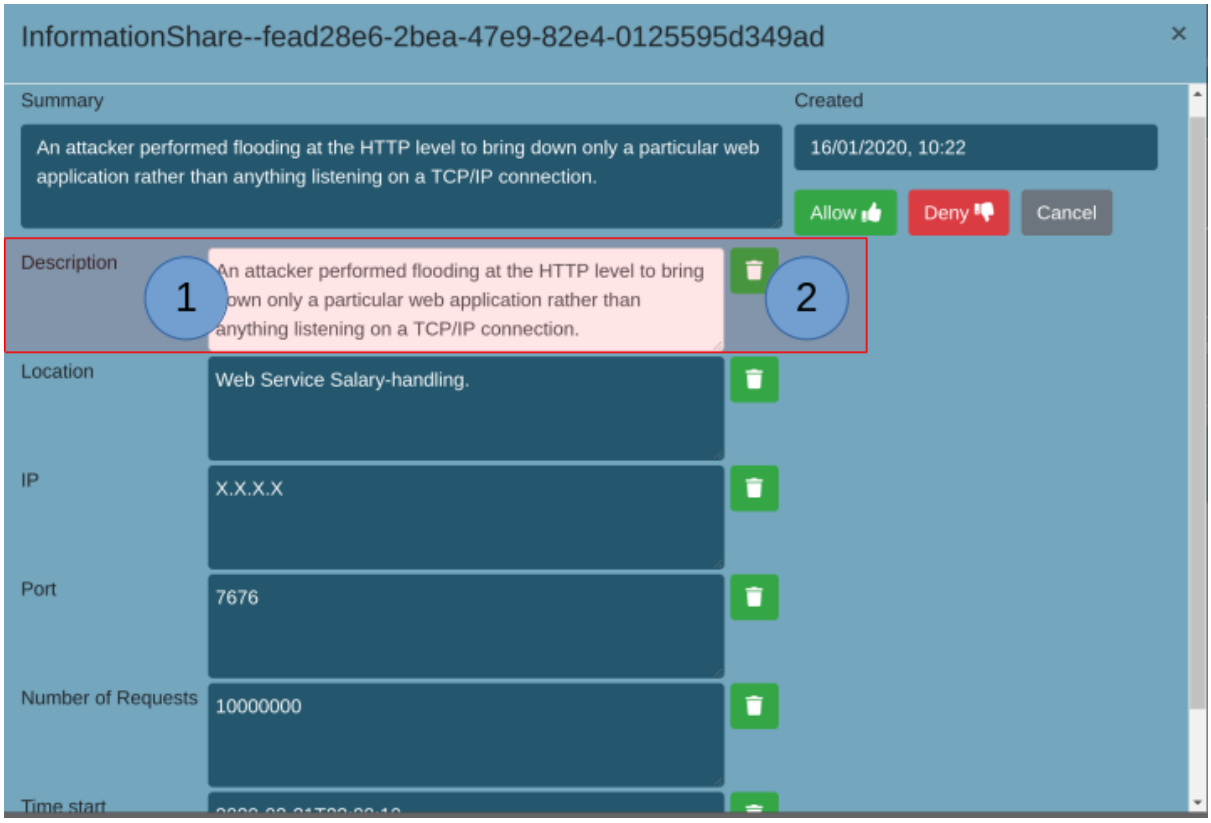
The information sharing details view of an information sharing event can be opened by clicking on the message.

3.4.3 Review information to be shared (Step 4-3)



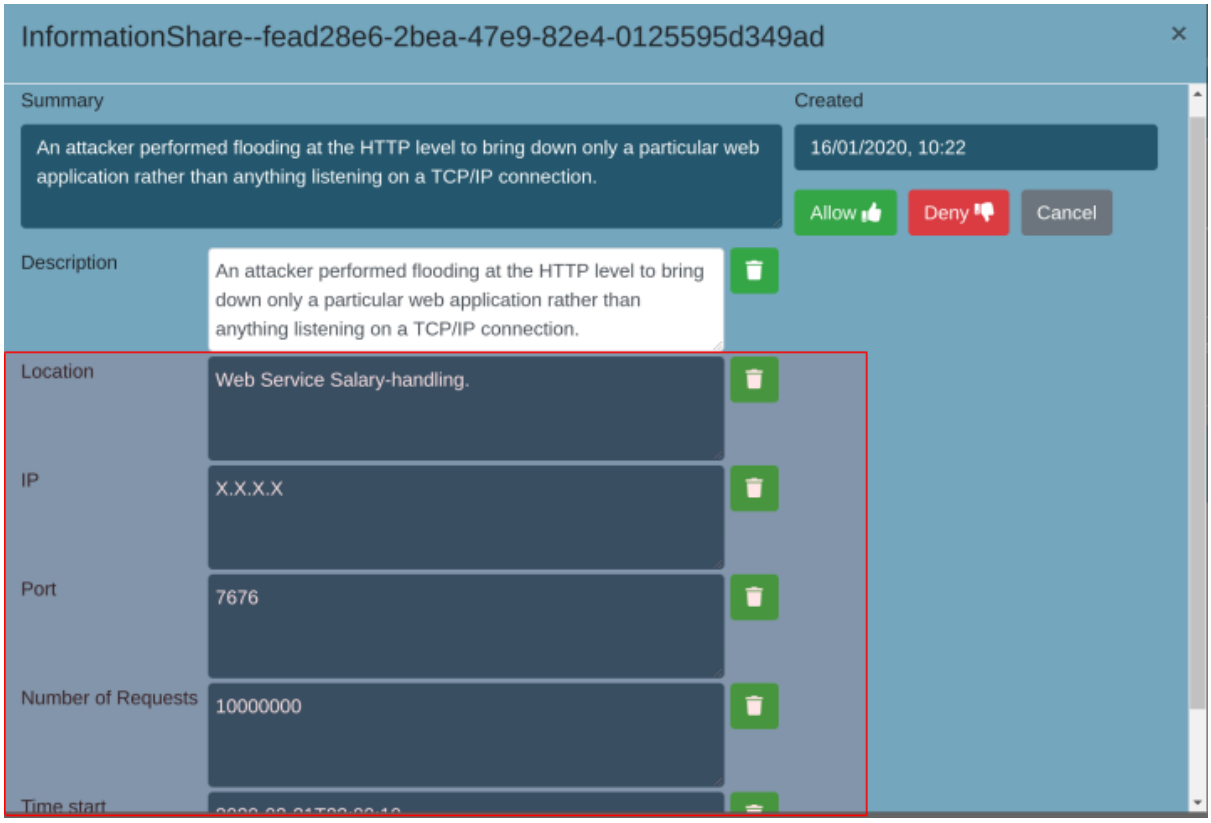
The information sharing details view shows a static "Summary" of the event that is visualized as a description to provide context to the user, and will not be shared. Furthermore, all the individual parameters that are available to be shared, including a general "Description" that can be edited and/or amended, are available on the left side of the view. The right side of the view contains the buttons to "Allow" or "Deny" the information share.

3.4.4 Edit or delete description field (Step 4-4)



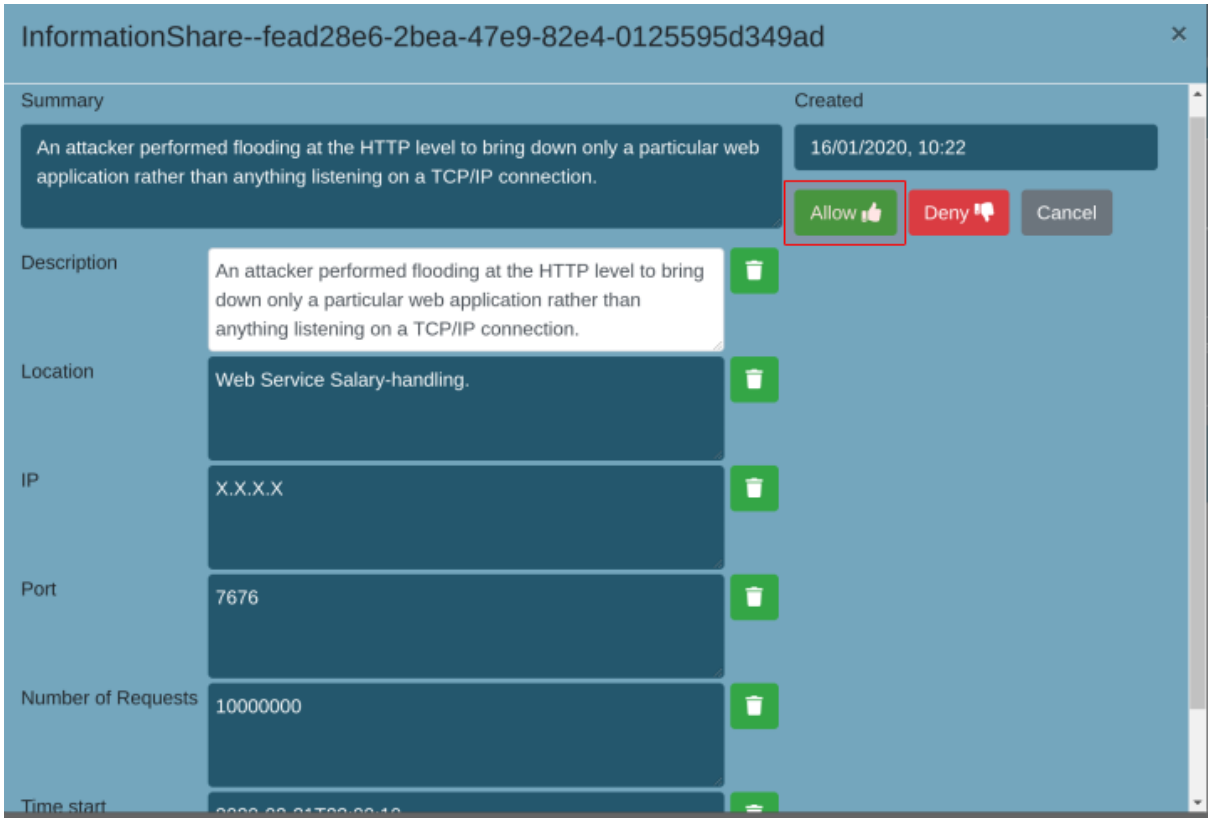
The “Description” field can be edited and/or amended (1) or deleted from the information share (2).

3.4.5 Delete parameter field (Step 4-5)



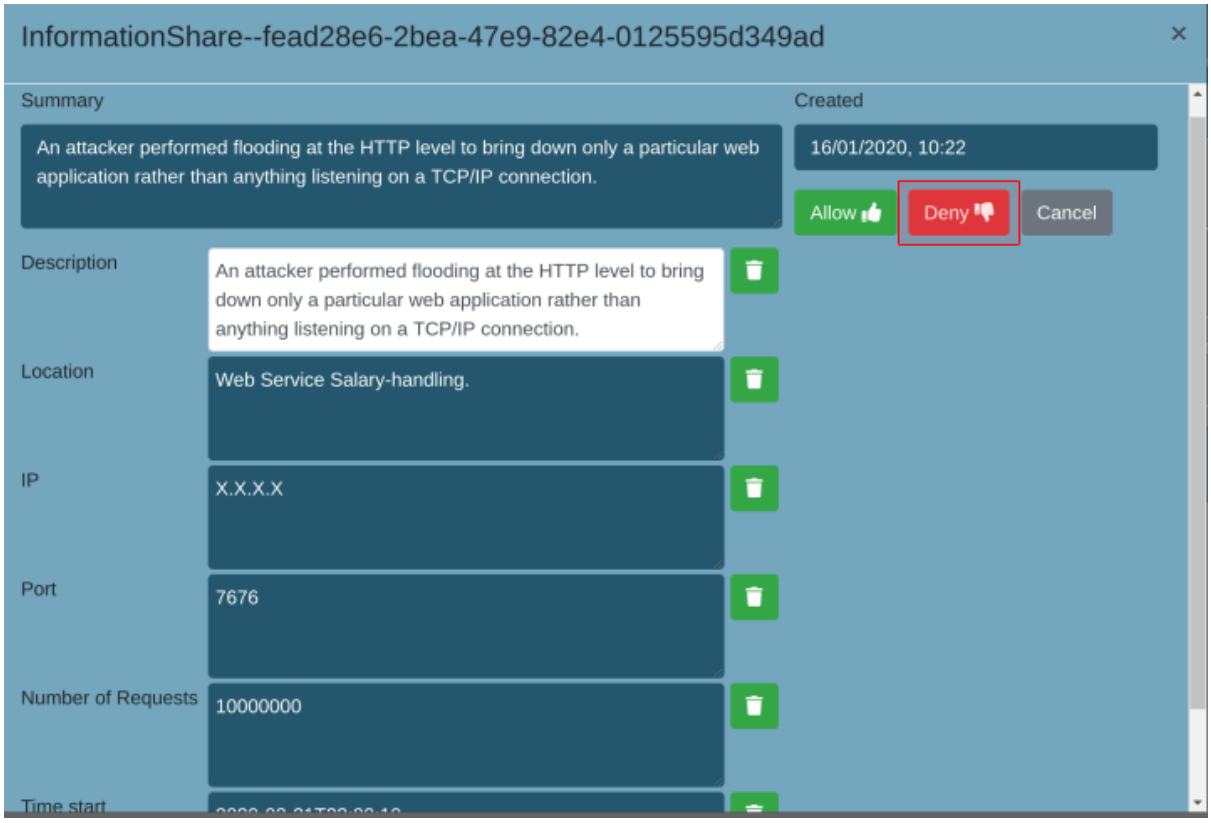
Each individual parameter can be deleted from the information share.

3.4.6 Allow information sharing (Step 4-6)



Pressing "Allow" will post the information in a protected sharing repository, accessible by everyone who is given access credentials to the repository.

3.4.7 Deny information sharing (Step 4-7)



Pressing the “Deny” button will remove the information sharing request from the information share list.

4 Annex 1: CS-AWARE user manual reading guidelines

A reading support meant for Users and Administrators

CS-AWARE USER MANUAL READING GUIDE

CS-AWARE CYBERSECURITY

Users Present in the CS-AWARE System

Inside the manual it is possible to find two main roles: administrators and users.

Administrator: System administrator and User administrator

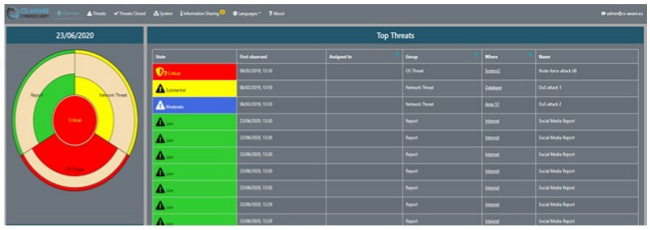
System administrator: can see all the threat views and can make changes. Currently the System Administrators can change information in the following: System Dependency Graph, available fields, and import (this may need a new role).

User administrator: can manager the role of users.

User: who is interfacing with the CS-AWARE platform. May have access to higher level of system privileges from the User Administrator.

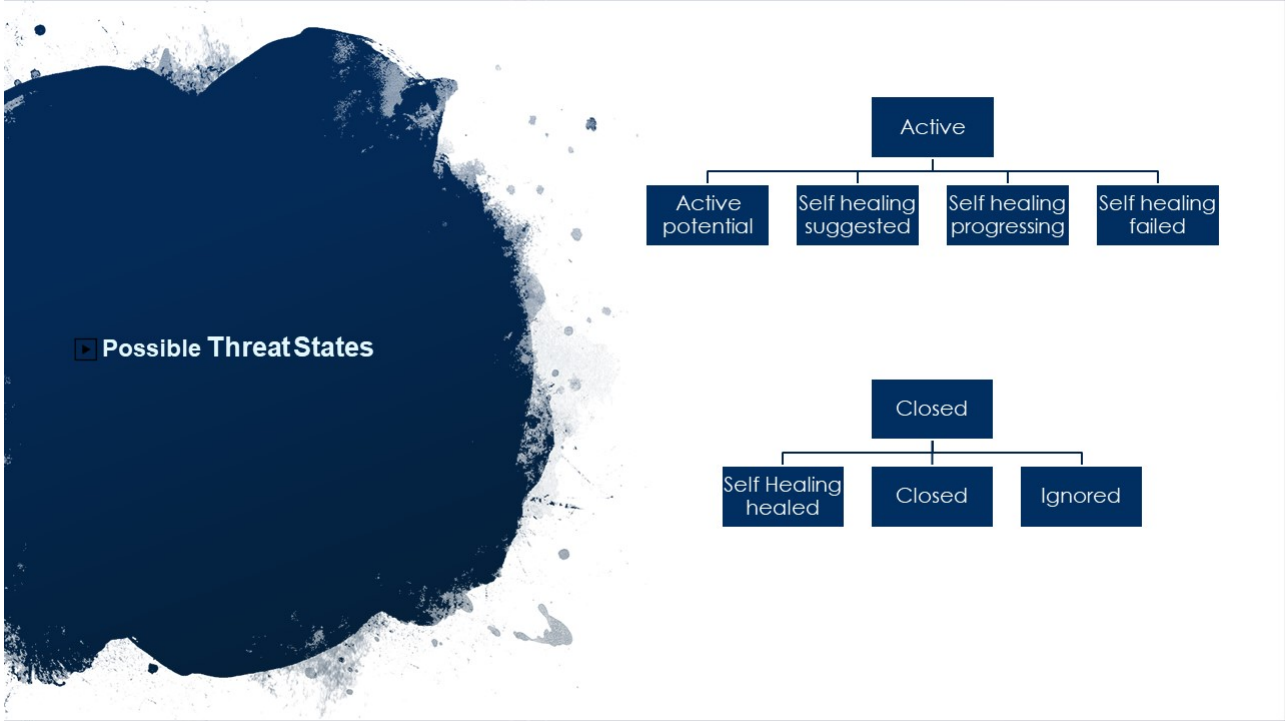
General Dashboard for CS-AWARE

- General Dashboard: indicates the overview of the system, including threats, level of criticality and in which part of the system it is at.
- Below are the categories of threats.
- User and administrator: can interface freely with the dashboard



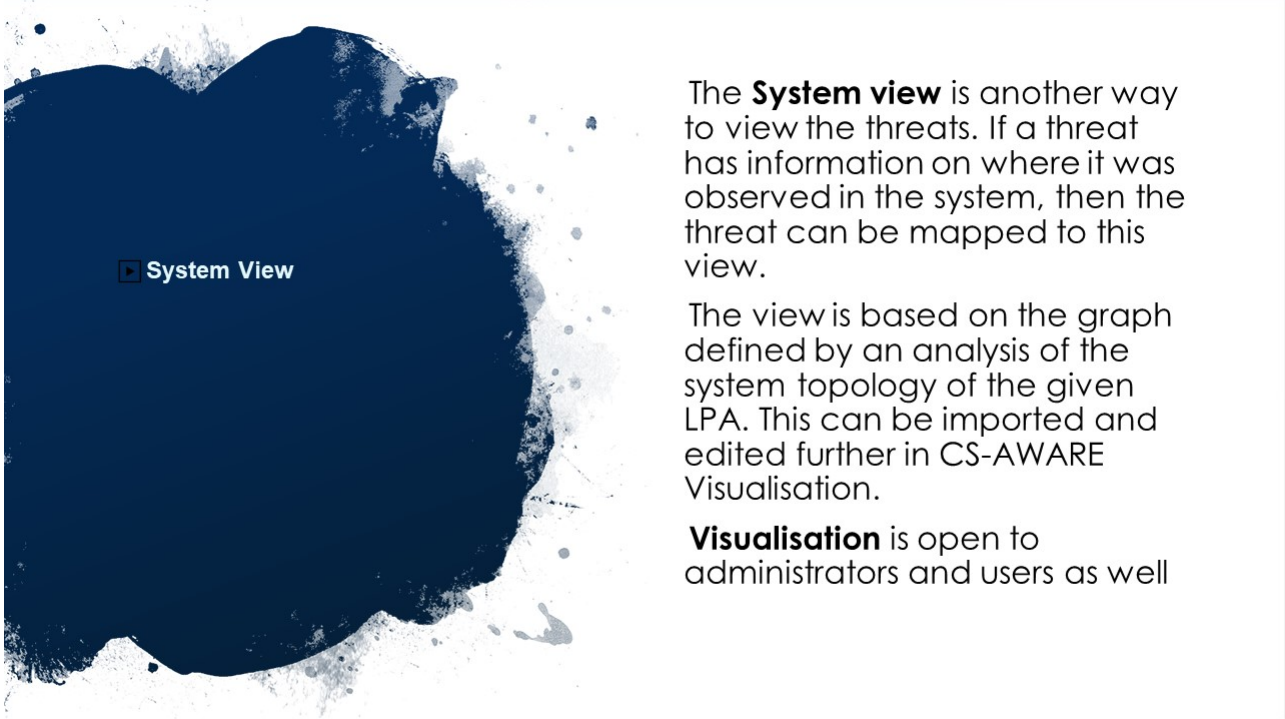
More Details about Threats

- **Threat detailed page**: more explanation on the threats can be found.
- **User**: can read and open notes on threats. If privileged can modify status.
- **Administrator**: can modify state


Possible Threat States
Active
Active potential
Self healing suggested
Self healing progressing
Self healing failed
Closed
Self Healing healed
Closed
Ignored


Description of Threats
Description of the threat: history of state's changes can be found. Also description of the threat.
Administrator: can change the state from there, inserting a description.
User: can change the state if privileges are granted.

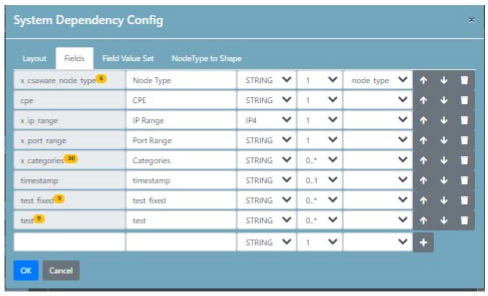

System Graph
System

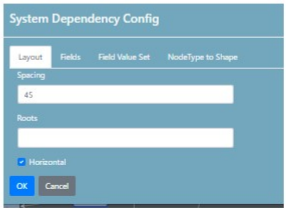

System View
The System view is another way to view the threats. If a threat has information on where it was observed in the system, then the threat can be mapped to this view.
The view is based on the graph defined by an analysis of the system topology of the given LPA. This can be imported and edited further in CS-AWARE Visualisation.
Visualisation is open to administrators and users as well

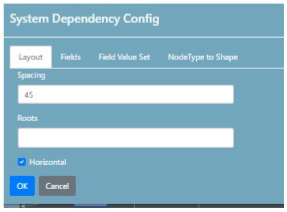
SYSTEM CONFIGURATION

- Full description of the process inside the extended user manual

Can be done only by System Administrators







USER MANAGEMENT TOOLS

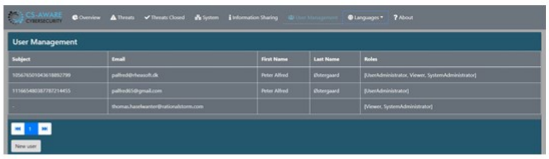
Tools available only for User Administrators

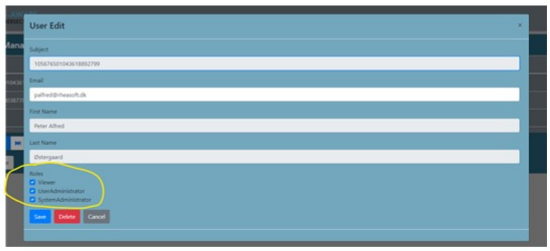
Possibility to grant privileges, roles and task for normal Users.

Viewer role: can see all the threat views but not allowed to make changes.

User edit interface

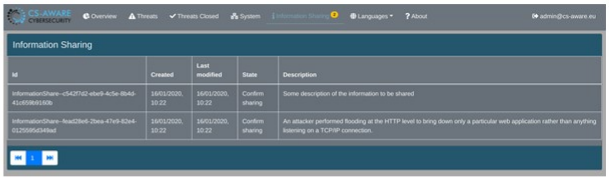
- Tools available only for User Administrators
- Possibility to grant privileges, roles and task for normal Users.
- Viewer role: can see all the threat views but not allowed to make changes.

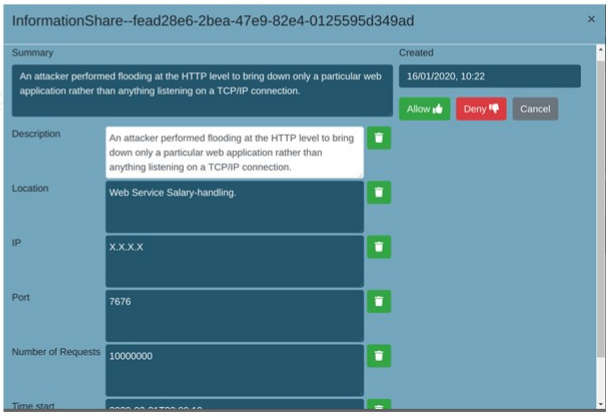




Information Sharing

- The information sharing view of the CS-AWARE system lists, for each sharing event, the unique ID, the date the event was created and last modified, the current state as well as the sharing event description.
- Clicking on a threat of interest opens the bottom window where the details view shows a "Summary" of the event to provide context to the user and will not be shared. Furthermore, all parameters that are available including a general "Description" can be edited on the left side of the view.





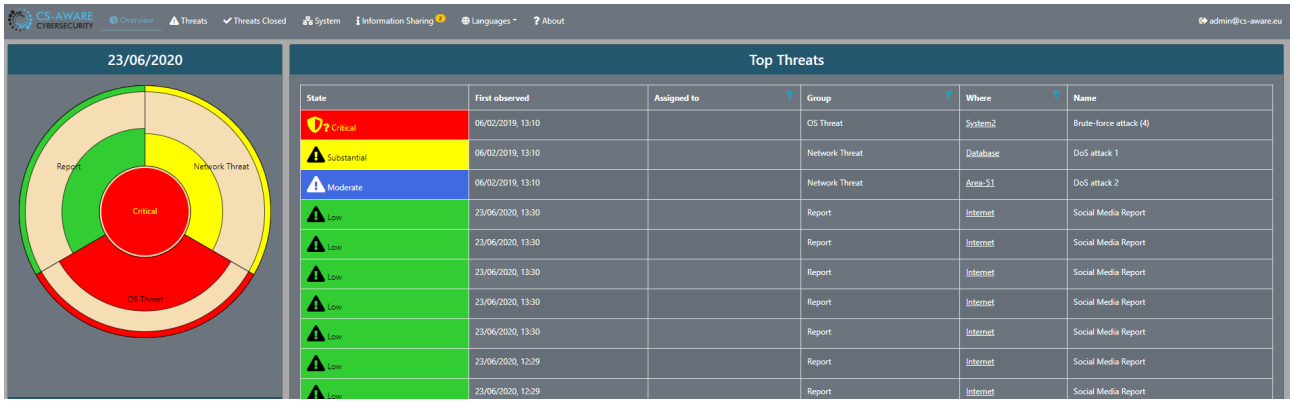
5 Annex 2: CS-AWARE quick user guidelines

5.1 Where do I start?

You start the application by typing something like following address in your browser;

https://www.NameOfMunicipality.CountrySuffix/csaware

5.2 Dashboard



You start with the Home Screen ("Overview") which is divided into two areas:

a. A **dashboard** contains a dartboard like a graph, which shows the current open threats[1]. The size of the coloured section of each group indicates how severe the threat is[2]. The centre (bullseye) of the dartboard shows the risk level according to severity levels including low (green), moderate (blue), substantial (yellow) and critical (red).

b. **Top Threats**: The table to the right of the "dartboard" lists the top threats. You can select all groups or one specific group by clicking on the centre or one of the slices in the "dartboard". Clicking on one of the threats will bring up a window with more details (See Section 5.5) with active threats ordered by descending severity and observation time.

Suggestion: First check on what threats are listed and click on the threat of interest. Read through the description of the critical threats before deciding how to proceed.

5.3 Threat Tables: Overview, Threats and Threats Closed

In addition to the threats list in the "Overview", which provides a limited list of the top threats, the "Threats" and "Threats closed" tabs provide comprehensive lists of all currently open and already closed threats:

[1] Grouped according to the CS-AWARE classification assigned by the analysis component.

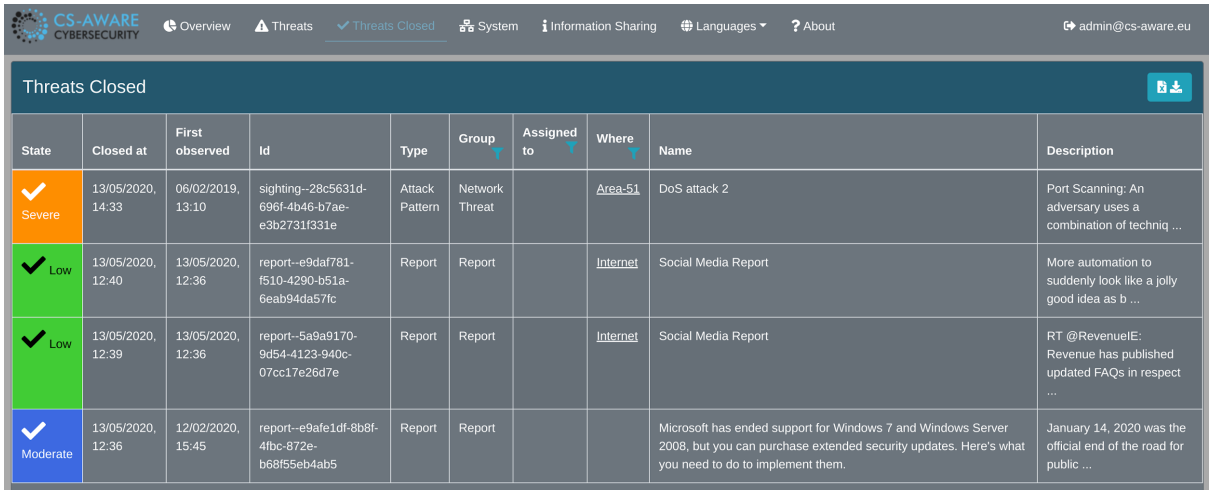
[2] The severity level is calculated on the basis on the risk-level and the number of observations for the given group.

In each of those lists, each individual item contains information about criticality, observed date, type and threat group, person responsible in “Assigned to” filed, as well as location in the system according to the system structure. The description of each threat is presented in an abbreviated form in the “Name” field:

Top Threats

State	First observed	Assigned to	Group	Where	Name
Critical	06/02/2019, 13:10		OS Threat	System2	Brute-force attack (4)
Substantial	06/02/2019, 13:10		Network Threat	Database	DoS attack 1
Moderate	06/02/2019, 13:10		Network Threat	Area-51	DoS attack 2
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 12:29		Report	Internet	Social Media Report
Low	23/06/2020, 12:29		Report	Internet	Social Media Report

The “Threats” and “Threats closed” lists additionally contain a unique ID of the threat an in the case of “Threats closed” also the date and time the threat was closed at:

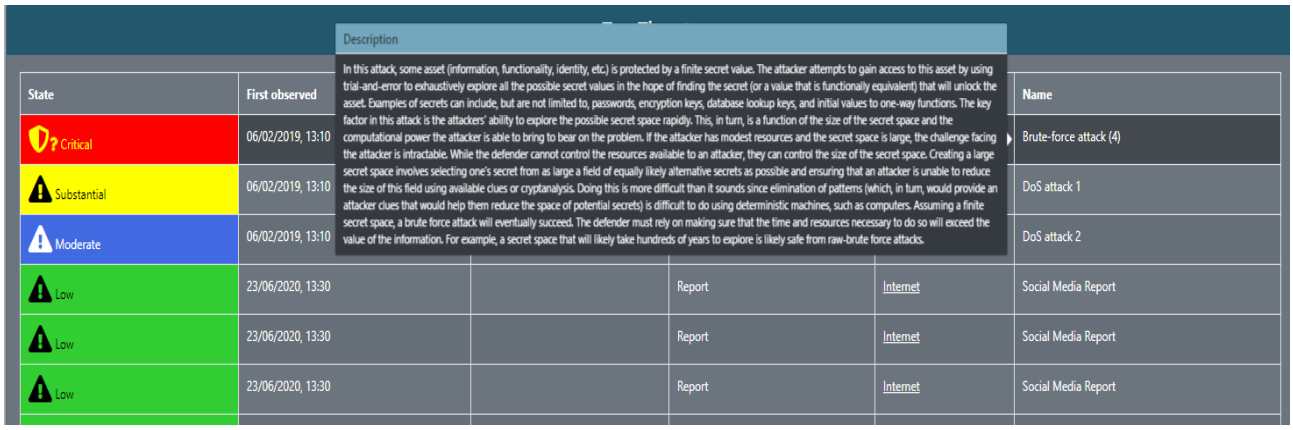


CS-AWARE CYBERSECURITY | Overview | Threats | Threats Closed | System | Information Sharing | Languages | About | admin@cs-aware.eu

Threats Closed

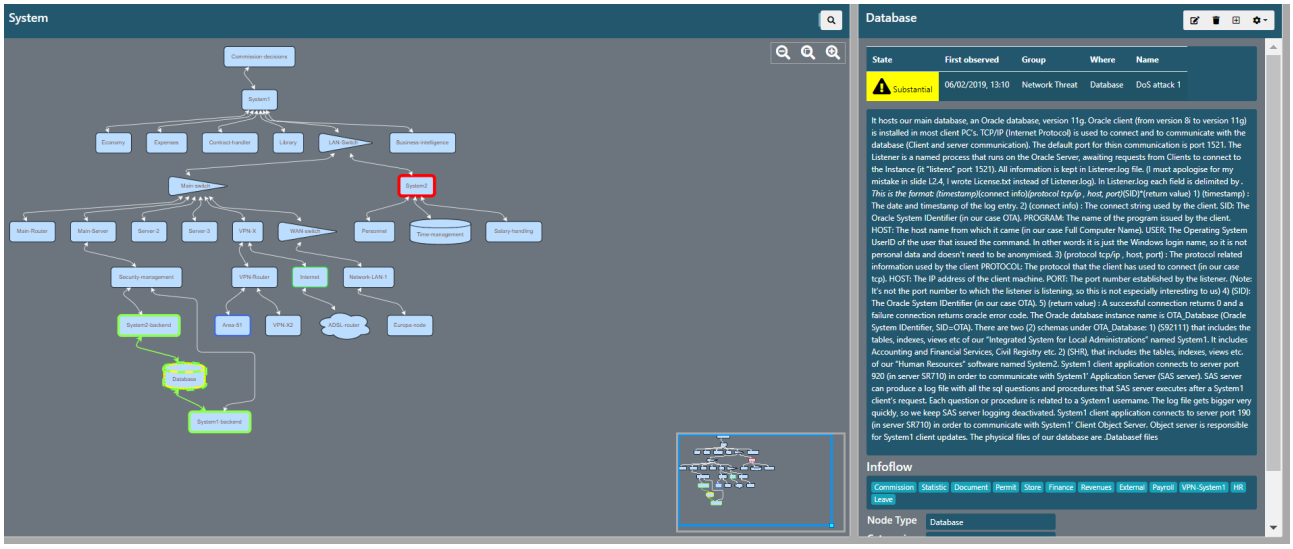
State	Closed at	First observed	Id	Type	Group	Assigned to	Where	Name	Description
Severe	13/05/2020, 14:33	06/02/2019, 13:10	sighting--28c5631d-696f-4b46-b7ae-e3b2731f331e	Attack Pattern	Network Threat		Area-51	DoS attack 2	Port Scanning: An adversary uses a combination of techniq ...
Low	13/05/2020, 12:40	13/05/2020, 12:36	report--e9daf781-f510-4290-b51a-6eab94da57fc	Report	Report		Internet	Social Media Report	More automation to suddenly look like a jolly good idea as b ...
Low	13/05/2020, 12:39	13/05/2020, 12:36	report--5a9a9170-9d54-4123-940c-07cc17e26d7e	Report	Report		Internet	Social Media Report	RT @RevenueIE: Revenue has published updated FAQs in respect ...
Moderate	13/05/2020, 12:36	12/02/2020, 15:45	report--e9afe1df-8b8f-4fbc-872e-b68f55eb4ab5	Report	Report			Microsoft has ended support for Windows 7 and Windows Server 2008, but you can purchase extended security updates. Here's what you need to do to implement them.	January 14, 2020 was the official end of the road for public ...

By hovering over the Name field, you can see a more detailed description without having to open the detail window:

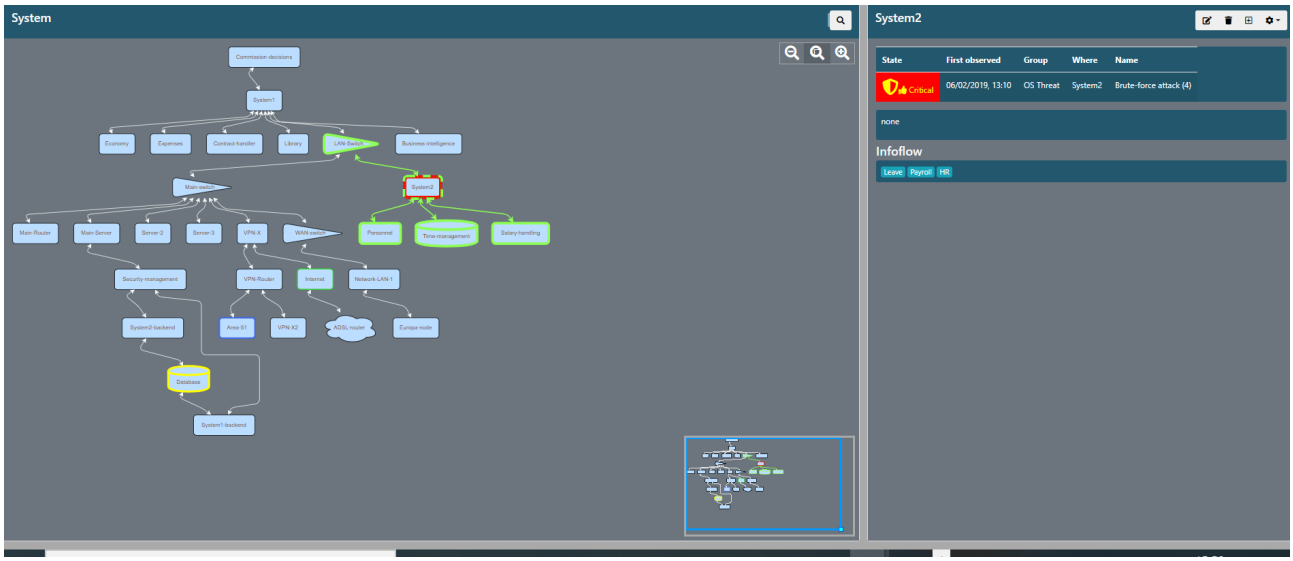


5.4 System Graph

The System view is another way to view the threats. If a threat has information on where it was observed in the system, then the threat can be mapped to this view. The view is based on graph defined by an analysis of the system topology of the given LPA. This can be imported and edited further in the CS-AWARE visualisation:

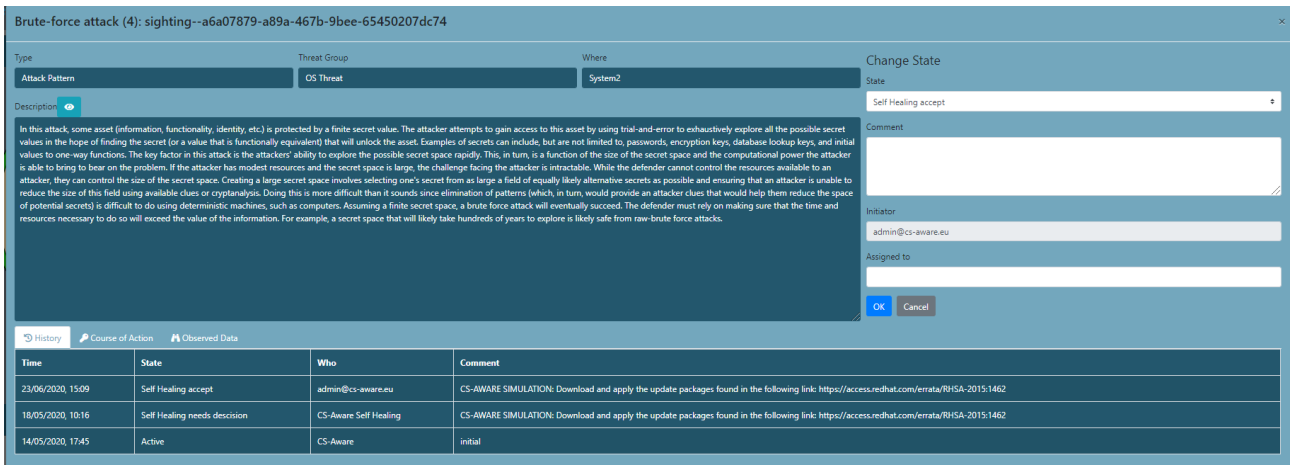


The graph on the left of each node is clickable to select the details shown to the right. If there are threats directly related to a node in the graph, then the node will have coloured border according to the risk level and there will be a table of the threats in the details when selected. The threat table is clickable like the other threat tables to open the threat details. The node details also show the name, description, and other fields that are relevant for the understanding and definition of the system, as defined in the system and dependency analysis results:



5.5 Threat details

The Threat details view can be opened by clicking on an individual threat in any of the above described threat lists (Overview, Threats, Closed Threats or System):



- The **left** side contains static information from the CS-AWARE system on where this threat was observed and a brief description.
- The **right** side is for changing state, which will be detailed in Section 5.6 and 5.7.
- The **bottom** portion of the screen includes a "history" tab, a "course of action" tab, and a "observed data" tab.

The History Tab contains information about each state change observed for this threat:

History | Course of Action | Observed Data

Time	State	Who	Comment
23/06/2020, 15:09	Self Healing accept	admin@cs-aware.eu	CS-AWARE SIMULATION: Download and apply the update packages found in the following link: https://access.redhat.com/errata/RHSA-2015:1462
18/05/2020, 10:16	Self Healing needs descision	CS-Aware Self Healing	CS-AWARE SIMULATION: Download and apply the update packages found in the following link: https://access.redhat.com/errata/RHSA-2015:1462
14/05/2020, 17:45	Active	CS-Aware	initial

The Course of Action tab contains a description and concrete suggestions from the self-healing process about the course of actions to mitigate the threat (in case self-healing is available):

History | Course of Action | Observed Data

Name	Description	Action
null mitigation	1: Add a firewall rule in order to block the given malicious IP address:.	iptables -A CSAWARE-IN -s csaware:pattern-bruteforcepw >= '0.95' -j drop

The Observed Data tab contains information about context of threat, as determined by the analysis component of CS-AWARE. Those are usually parameters describing system behaviour observed in log files from system components in your organization. This is intended for system administrators working with those aspects of the system to be able to better devise mitigations to the threat:

History | Course of Action | Observed Data

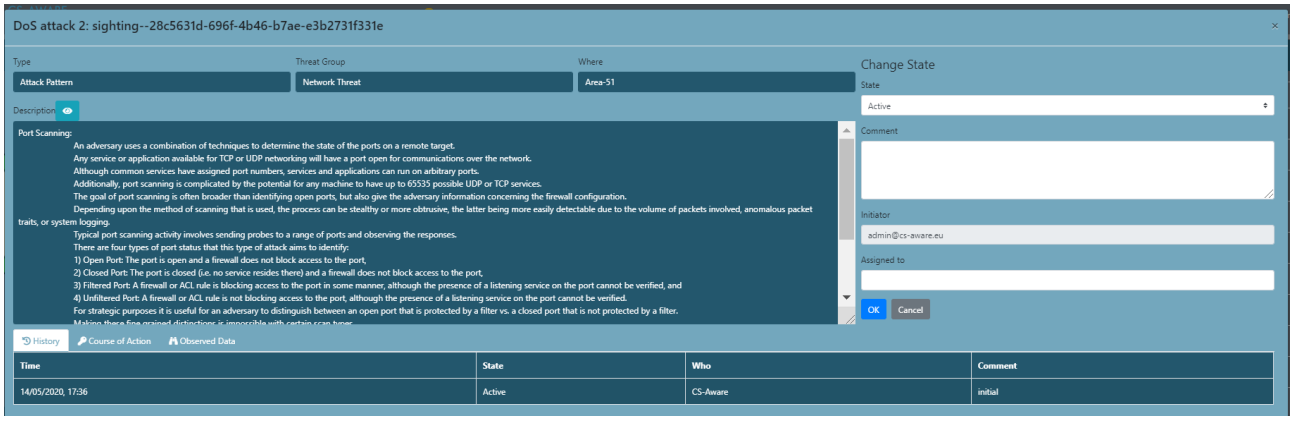
Type	Id	Data
software	0	name: Ubuntu Linux OS; vendor: Canonical; version: 16.04.5 LTS; cpe: cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*
software	1	name: iptables Firewall; vendor: Linux; version: 1.8.0
ipv4-addr	2	value: 2.3.4.5
process	3	pid: (value=314); name: SamS; extensions: (windows-service-ext=[service_name=SamS, display_name=Security Accounts Manager, start_type=SERVICE_AUTO_START, service_type=SERVICE_WIN32_SHARE_PROCESS , service_status=SERVICE_RUNNING])

5.6 Active States

Threats that are currently in an active state can be observed in the threats lists in Overview, Threats, and System.

Active states can be observed for threats with no self-healing available (Section 5.6.1) and a self-healing action available (Section 5.6.2). The latter replaces the manual state changing with automated handling of states, including visual feedback as shown in Section 5.6.3.

5.6.1 Threat view window in “Active” state



The “Active” state in cases with no self-healing available can be changed manually using the drop-down menu on the right side of the screen.

5.6.2 Self-Healing active state – waiting for manual confirmation

The self-healing active state is indicated by waiting for manual confirmation before applying the self-healing action

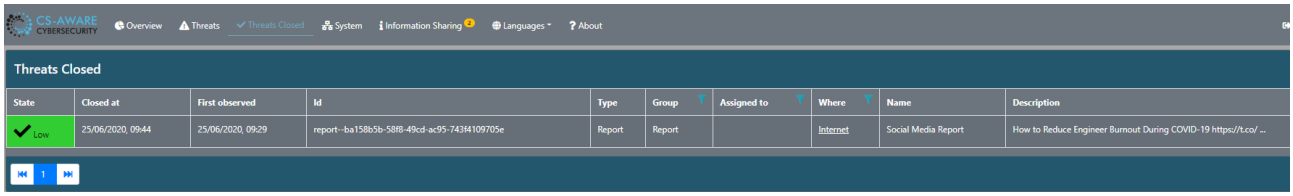
5.6.3 Self-Healing: Threat list items indicate the active states self-healing is currently in

Visual indication of self-healing confirmed by user, but waiting for results:

Visual indication of self-healing action failed. The threat remains in an active state:

5.7 Closed States

Non-active states. The last closed state can be seen under the view "Threats closed":

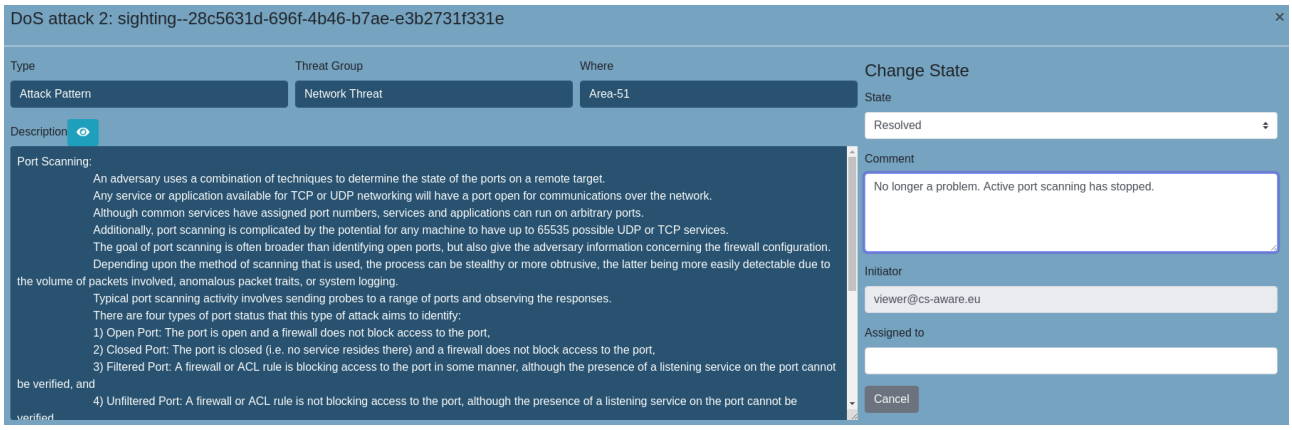


A successfully applied self-healing action results a threat closed state. Following visual feedback is provided in “Threats closed”:

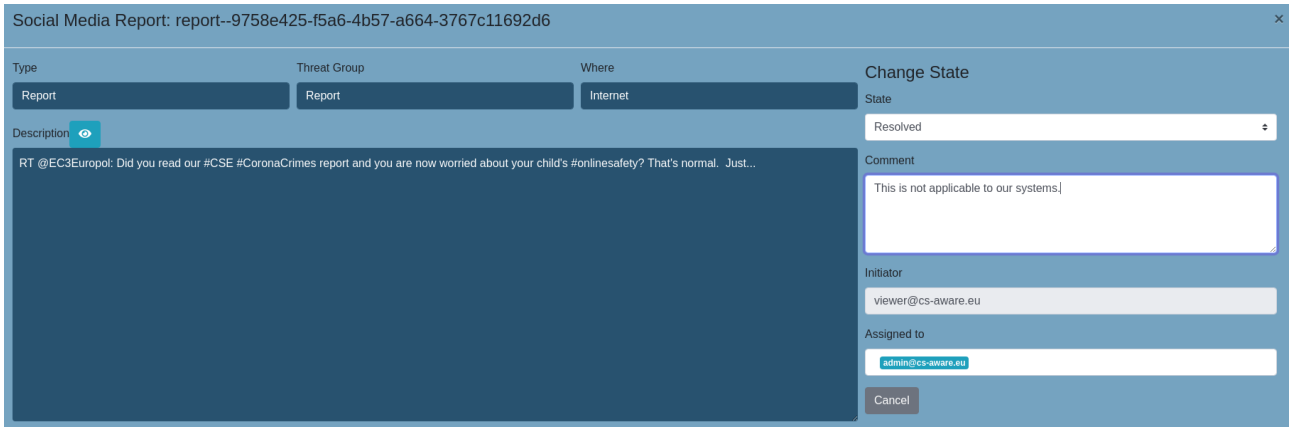
In the threats view, “Self Healing Done” indicates the self-healing module has applied the actions suggested:

A closed threat that did not have a self-healing action associated, can have the two possible states “resolved” and “ignored”.

Resolved refers to the state when appropriate mitigation actions were applied by the system administrator (outside the CS-AWARE context):



Ignored refers to a threat was marked as ignored by a system administrator, and no action has been taken to mitigate the threat:



5.8 Changing State

You can change the state of a threat in the **Threat Details** view shown above. For threats where self-healing is available, state changes are done automatically. What changes are possible depend on the current state of the threat. You can insert comments. In addition, the current state can be maintained.

- **Change a threat**: An active threat can be closed by indicating healed or ignored.
- **Reopen a threat**: A closed threat can be reopened. Use the dropdown box to select a state change except for self-Healing choices that have explicit buttons.

Suggestion: When changing states, it is always a good practice to write the actions taken into the State history message**.**

In the threats view bottom screen, the "History" tab indicates the state history of each threat. This particular example shows the history of self-healing applied with success. "State history" comments are shown in the "Comment" section:

OK Cancel

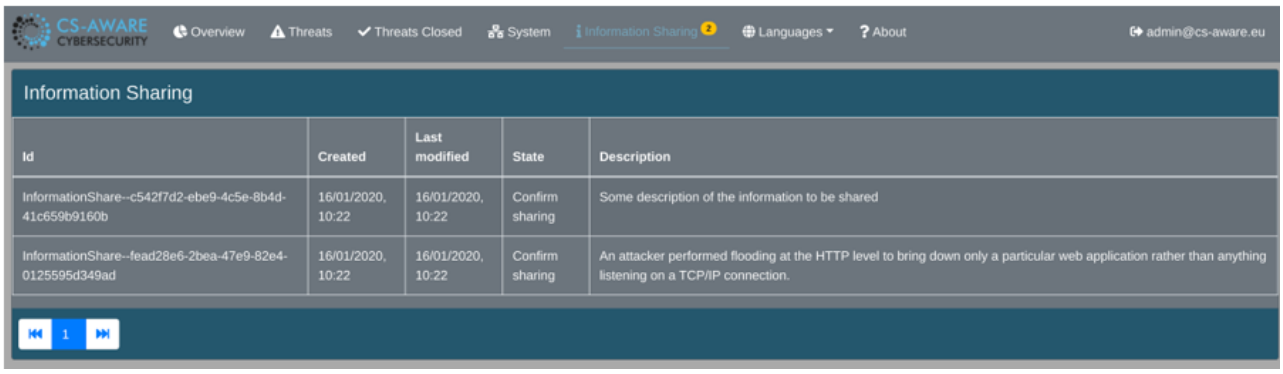
History | Course of Action | Observed Data

Time	State	Who	Comment
24/06/2020, 17:33	Self Healing Done	CS-Aware Self Healing	Success
24/06/2020, 17:33	Being Self Healed	CS-Aware Self Healing	Healing started
24/06/2020, 17:33	Self Healing accept	forrester.rome@gmail.com	1: Shutdown the database server and search the logs. 2: For applications that leverage remote schemas, use the HTTPS protocol to prevent modification of traffic in transit and to avoid unauthorized modification. 3: All user-controllable input must be validated and filtered for illegal characters as well as SQL content. Keywords such as UNION, SELECT or INSERT must be filtered in addition to characters such as a single-quote(') or SQL-comments (--) based on the context in which

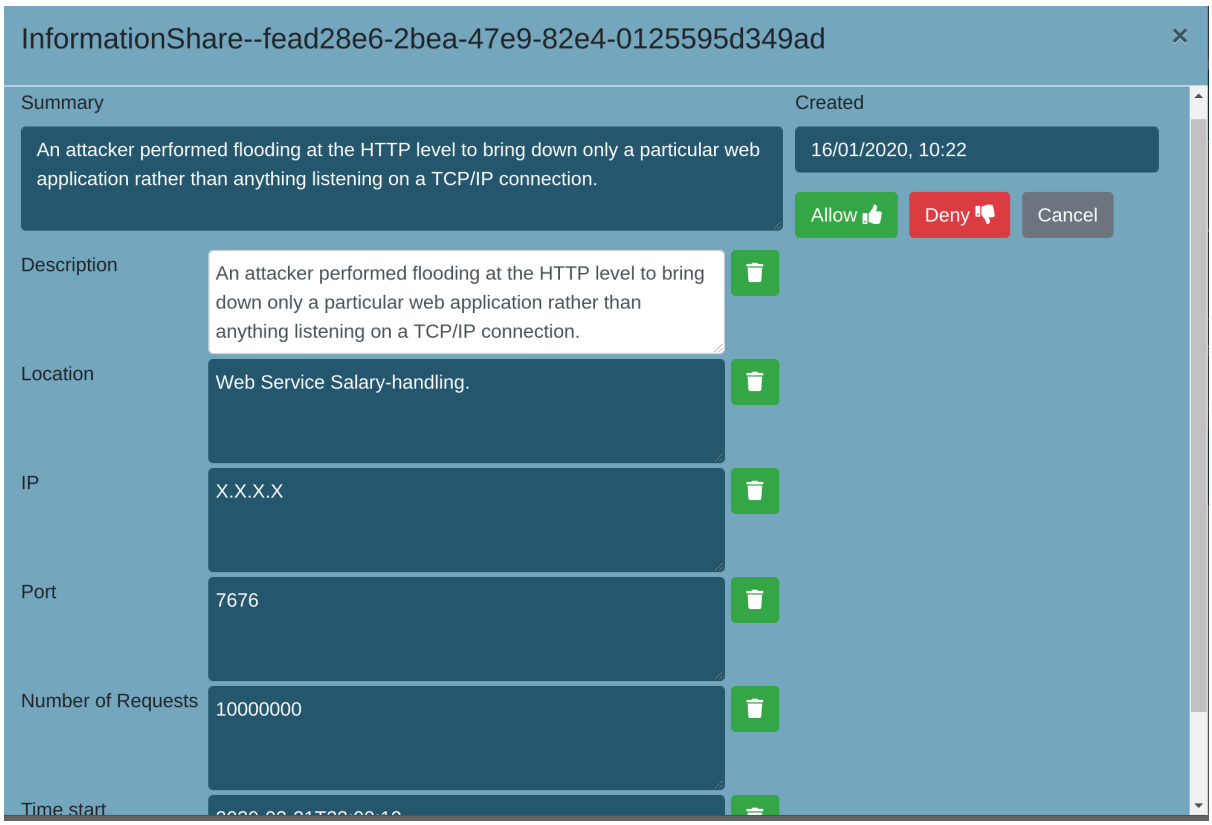
5.9 Information Sharing

Information sharing allows to share information about individual threats with experts or communities outside of your organization. If you allow information sharing for individual threats, the information is posted in a dedicated repository. Only experts or communities that you share the access credentials with will have access to the information.

The information sharing view of the CS-AWARE system lists, for each sharing event, the unique ID, the date the event was created and last modified, the current state as well as the sharing event description:



The information sharing details for each listed information share contain a summary of the threat to give context to the user allowing the share (this summary will not be shared), a description of the context that can be edited or deleted before sharing, and a set of parameters that were relevant in the detection and handling of the threat the information share relate to. Each individual parameter can be deleted before allowing or denying the information share:



6 Annex 3: CS-AWARE extended user manual

6.1 Where do I start?

You call the application by typing in the CS-AWARE system address in your browser. It will usually be something like: https://www.name-municipality.countrysuffix/csaware

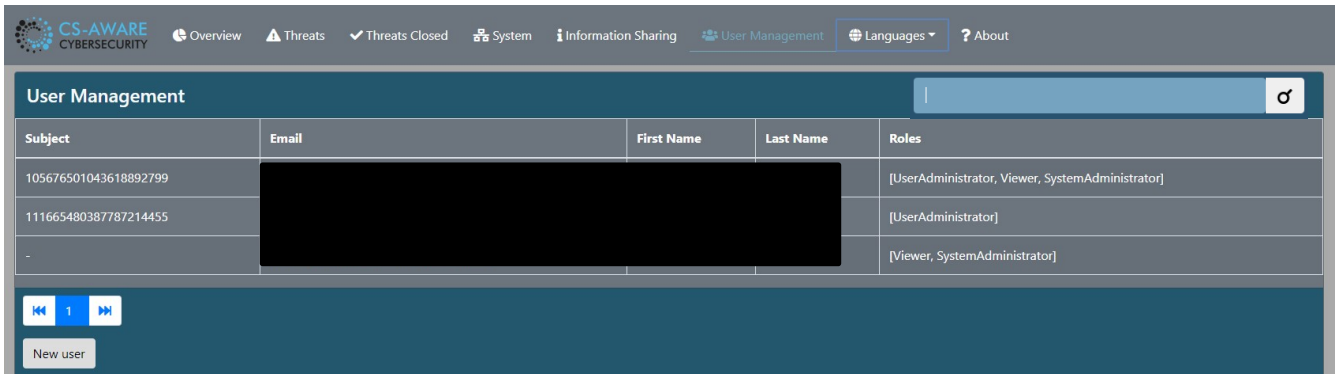
6.2 Authentication and Authorization/ User Management

The User Management view of the CS-AWARE system allows a user manger to add/delete users and manage the authorisation of users. The authentication is handled by an external OAUTH/OIDC provider, which could be a Google login, or AWS Cognito, or Facebook, etc. Almost all identity management systems support OAUTH2/OIDC.

Authorisation is currently zero or more of the following roles (this may be extended to more roles in future versions):

- **User Administrator** can create/delete users and manage the roles of other users.
- **Viewer** may see all the threat views (Overview, Threats, Threats Closed, System), but is not allowed to change anything.
- **System Administrator** sees all the threat views and can do changes. Currently the System Administrators can change information in the following:
    - System Dependency Graph (System view): Import/Export of a graph; layout configuration, custom fields configuration, node shape configuration.

Only **User Administrators** can see and do "User Management", which means that a user that needs to do both threats and user administration needs two roles. The state of “No roles” allows a user to be authenticated and see the "About", but nothing else is allowed until a role is assigned. Any authenticated user will be automatically registered with an empty set of roles. At the first authentication the fields with the subject, first name, and last name are updated.

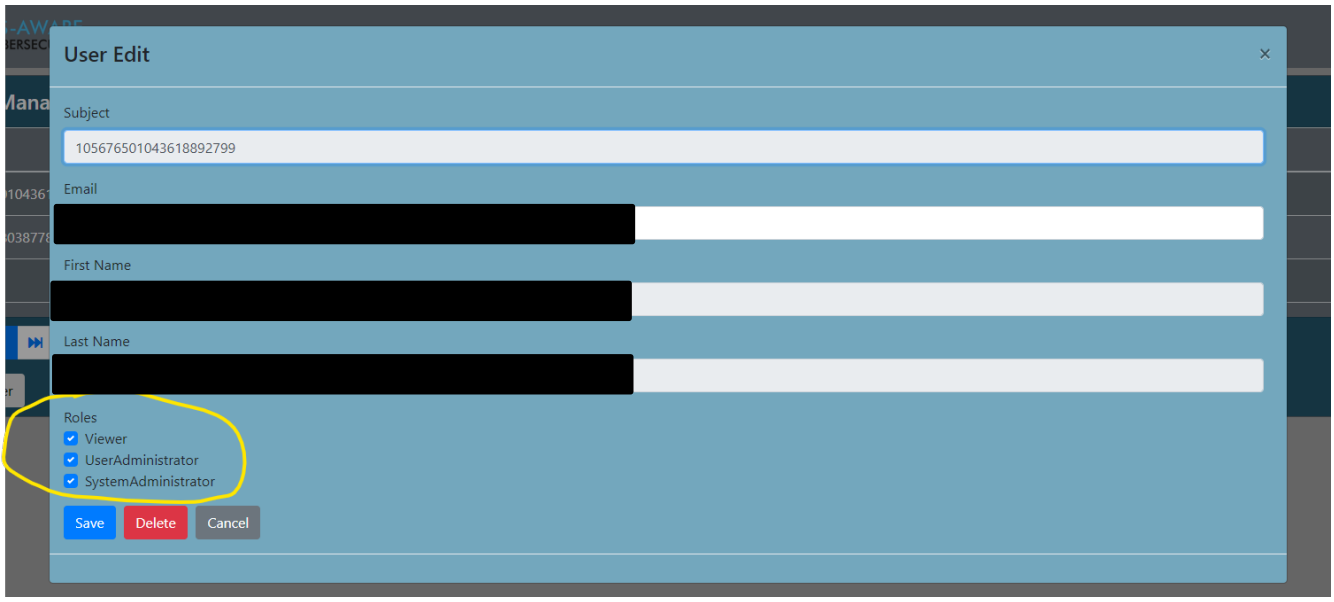


In the user management view, a search field on top of the user list allows to search for individual users (name or email) in cases where many users are registered with the CS-AWARE instance:

The "New User" allows one to associate roles to an email of a user that has not yet been authenticated.

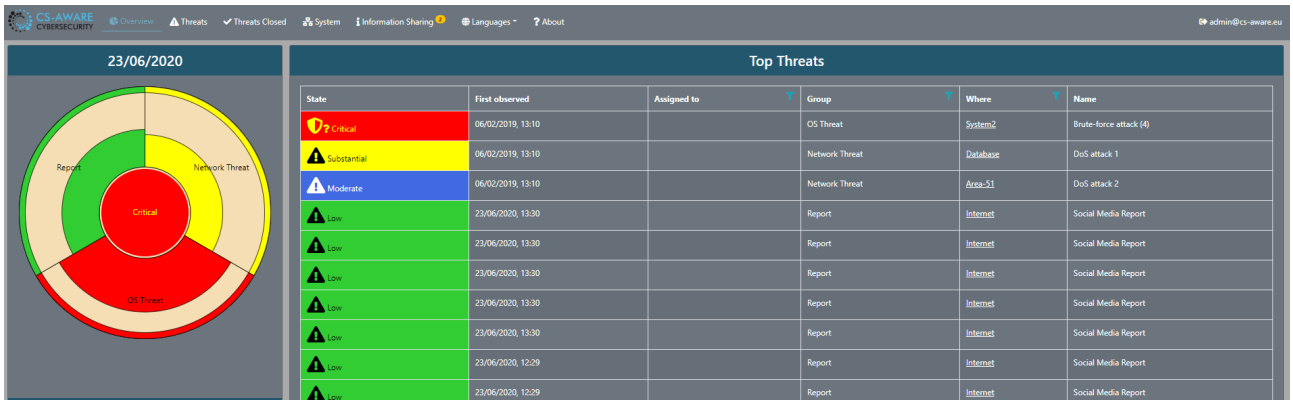
The subject and names will be automatically updated when the user is authenticated. It is only necessary to call the function of “New User" when roles need to be assigned before first login:

The roles are the only part that should need editing. In this example all roles are checked, but the "Viewer" option does not need to be checked, because the System Administrator can view everything a Viewer can do:

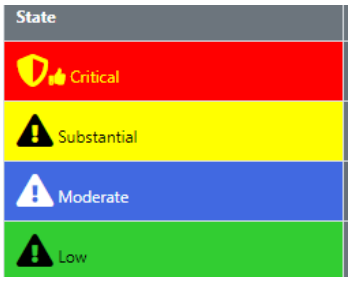


6.3 Dashboard

You start with the Home Screen ("Overview") which is divided into two main areas:



1. A **dashboard** contains a dartboard like a graph, which shows the current open threats[3]. The size of the coloured section of each group indicates how severe the threat is[4]. The centre (bullseye) of the dartboard shows the risk level according to severity levels including low (green), moderate (blue), substantial (yellow) and critical (red).



2. **Top Threats**: The table to the right of the "dartboard" lists the top threats. You can select all groups or one specific group by clicking on the centre or one of the slices in the "dartboard". Clicking on one of the threats will bring up a window with more details (see Section 6.6) with active threats ordered by descending severity and observation time.

First check on what threats are listed and click on the threat of interest. Read through the description of any critical threat before deciding how to proceed.

6.4 Threat Tables: Overview, Threats and Threats Closed

In addition to the threats list in the "Overview", which provides a limited list of the top threats, the "Threats" and "Threats closed" tabs provide comprehensive lists of all currently open and already closed threats:

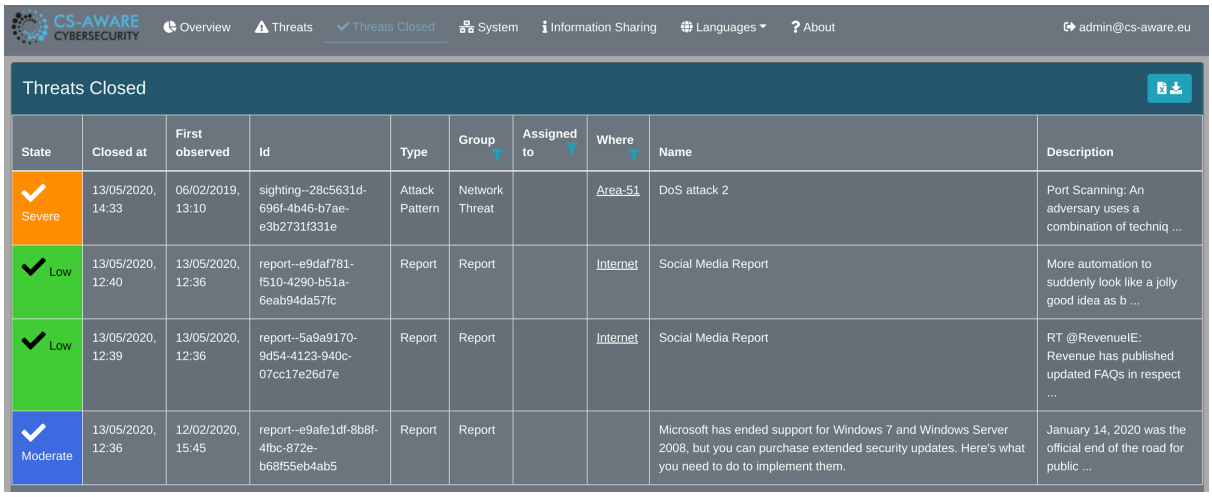
[3] Grouped according to the CS-aware classification assigned by the analysis component.
[4] The severity level is calculated on the basis of the risk-level and the number of observations for the given group.

In each of those lists, each individual item contains information about criticality, observed date, type and threat group, person responsible in “Assigned to” filed, as well as location in the system according to the system structure. The description of each threat is presented in an abbreviated form in the “Name” field:

Top Threats

State	First observed	Assigned to	Group	Where	Name
Critical	06/02/2019, 13:10		OS Threat	System2	Brute-force attack (4)
Substantial	06/02/2019, 13:10		Network Threat	Database	DoS attack 1
Moderate	06/02/2019, 13:10		Network Threat	Area-51	DoS attack 2
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 13:30		Report	Internet	Social Media Report
Low	23/06/2020, 12:29		Report	Internet	Social Media Report
Low	23/06/2020, 12:29		Report	Internet	Social Media Report

The “Threats” and “Threats closed” lists additionally contain a unique ID of the threat an in the case of “Threats closed” also the date and time the threat was closed at:

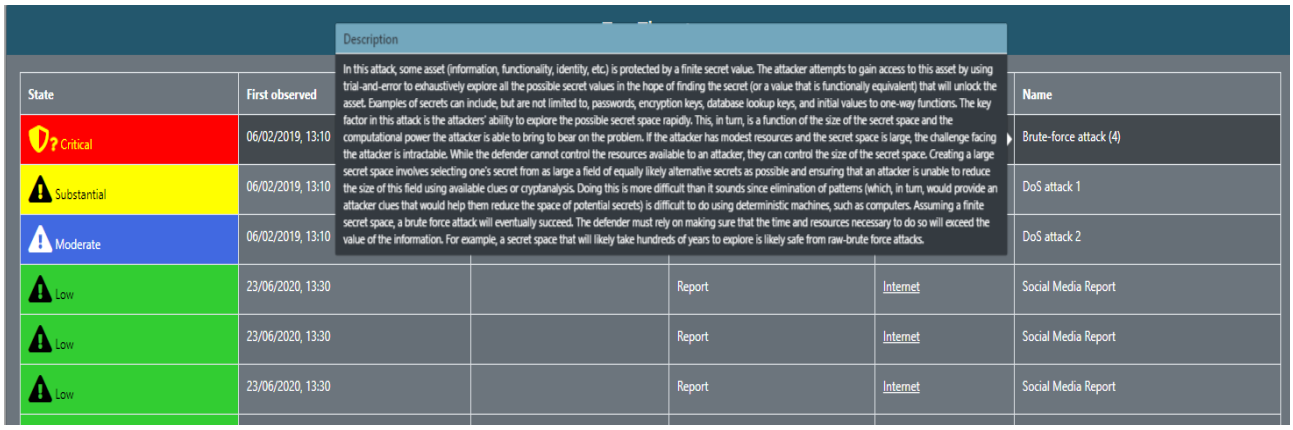


CS-AWARE CYBERSECURITY | Overview | Threats | Threats Closed | System | Information Sharing | Languages | About | admin@cs-aware.eu

Threats Closed

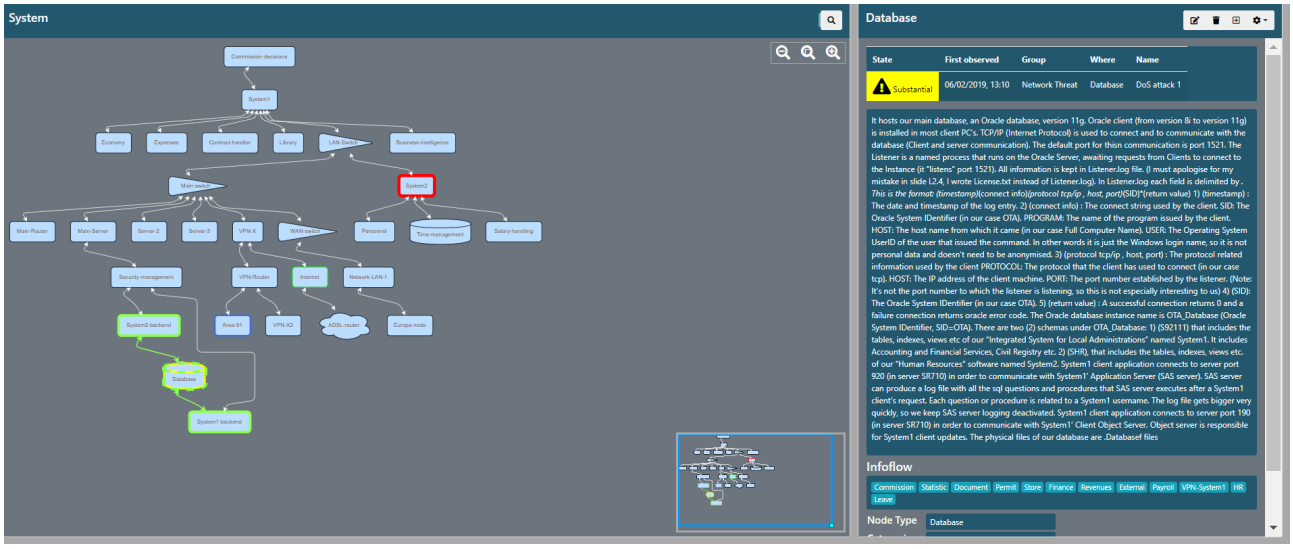
State	Closed at	First observed	Id	Type	Group	Assigned to	Where	Name	Description
Severe	13/05/2020, 14:33	06/02/2019, 13:10	sighting--28c5631d-696f-4b46-b7ae-e3b2731f331e	Attack Pattern	Network Threat		Area-51	DoS attack 2	Port Scanning: An adversary uses a combination of techniq ...
Low	13/05/2020, 12:40	13/05/2020, 12:36	report--e9daf781-f510-4290-b51a-6eab94da57fc	Report	Report		Internet	Social Media Report	More automation to suddenly look like a jolly good idea as b ...
Low	13/05/2020, 12:39	13/05/2020, 12:36	report--5a9a9170-9d54-4123-940c-07cc17e26d7e	Report	Report		Internet	Social Media Report	RT @RevenueIE: Revenue has published updated FAQs in respect ...
Moderate	13/05/2020, 12:36	12/02/2020, 15:45	report--e9afe1df-8b8f-4fbc-872e-b68f55eb4ab5	Report	Report			Microsoft has ended support for Windows 7 and Windows Server 2008, but you can purchase extended security updates. Here's what you need to do to implement them.	January 14, 2020 was the official end of the road for public ...

By hovering over the Name field, you can see a more detailed description without having to open the detail window:

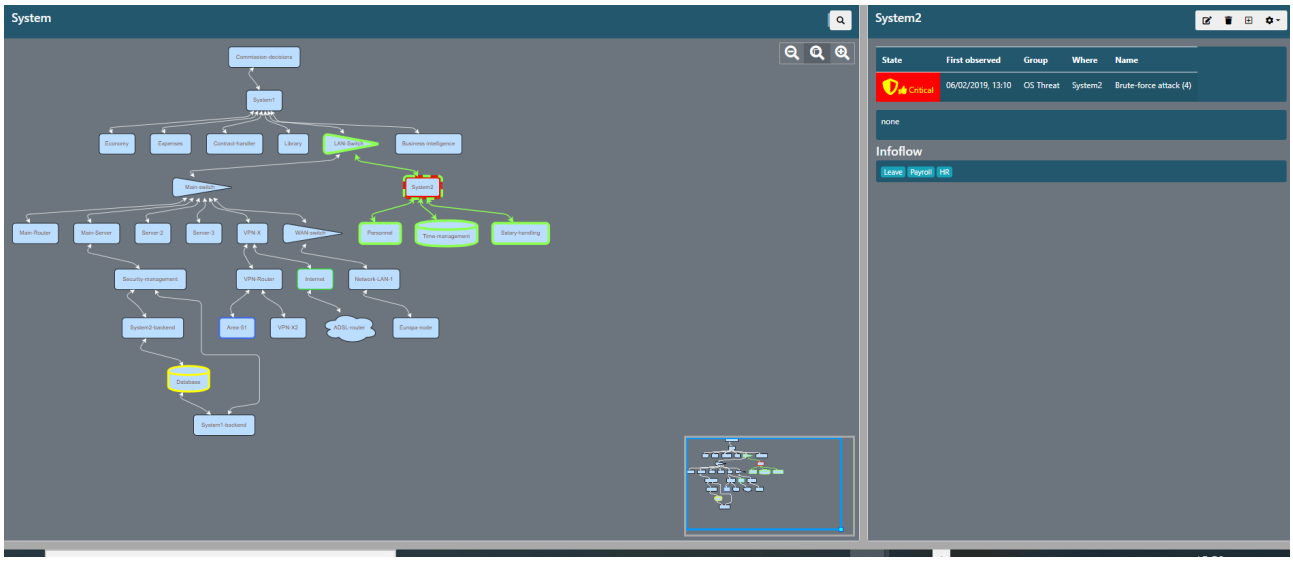


6.5 System Graph

The System view is another way to view the threats. If a threat has information on where it was observed in the system, then the threat can be mapped to this view. The view is based on graph defined by an analysis of the system topology of the given LPA. This can be imported and edited further in the CS-AWARE visualisation:

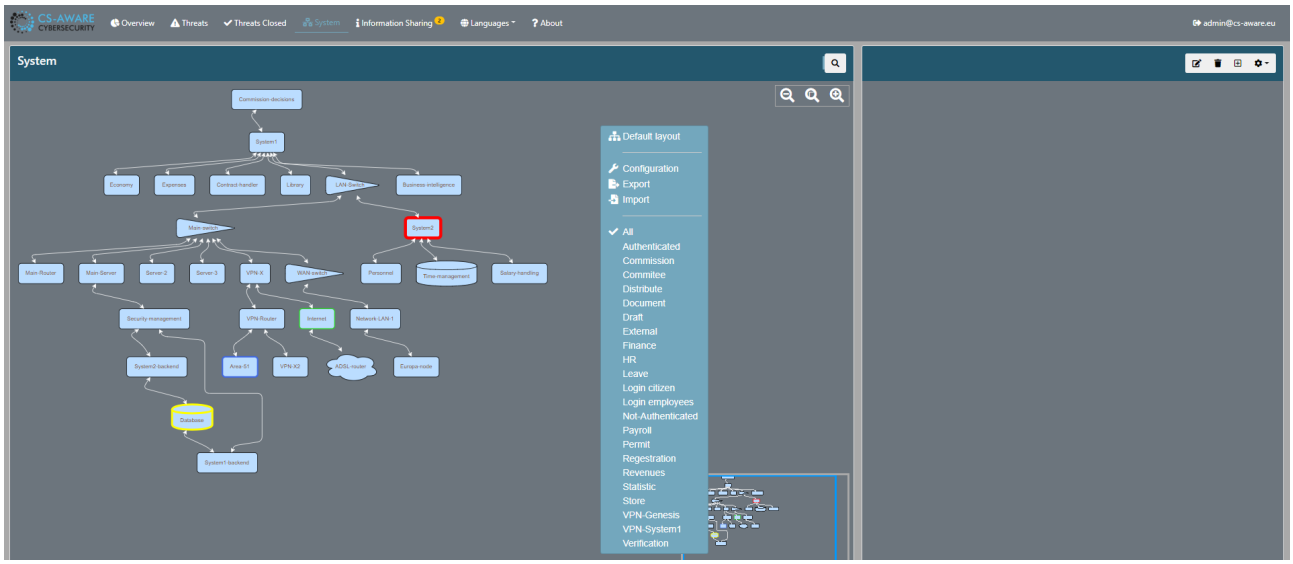


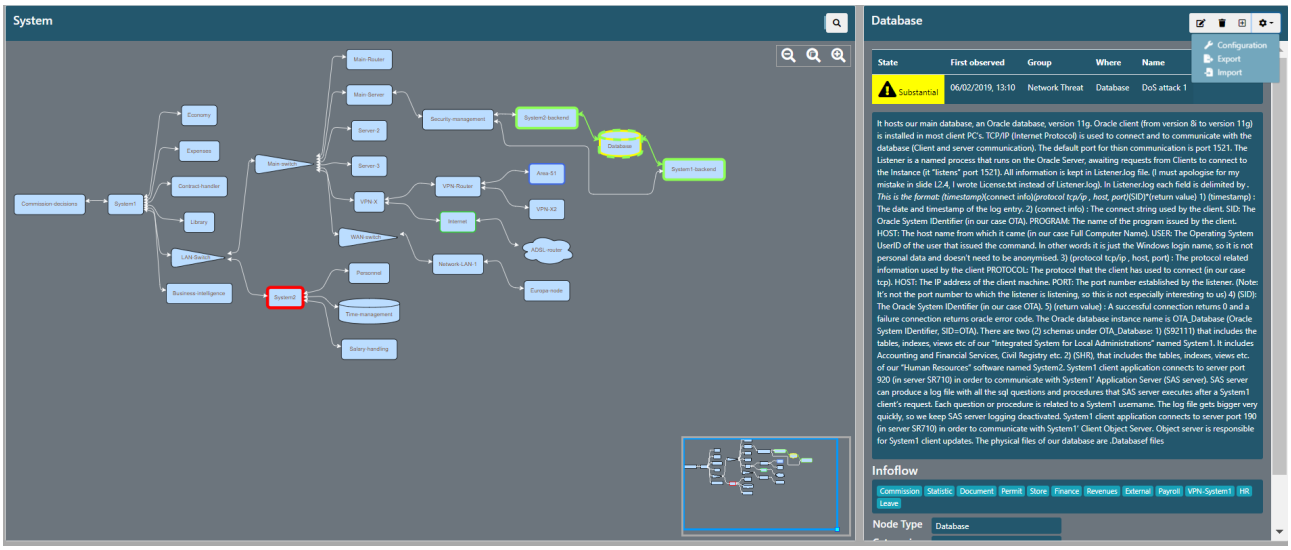
The graph on the left of each node is clickable to select the details shown to the right. If there are threats directly related to a node in the graph, then the node will have coloured border according to the risk level and there will be a table of the threats in the details when selected. The threat table is clickable like the other threat tables to open the threat details. The node details also show the name, description, and other fields that are relevant for the understanding and definition of the system, as defined in the system and dependency analysis results:



6.5.1 System Graph Editing

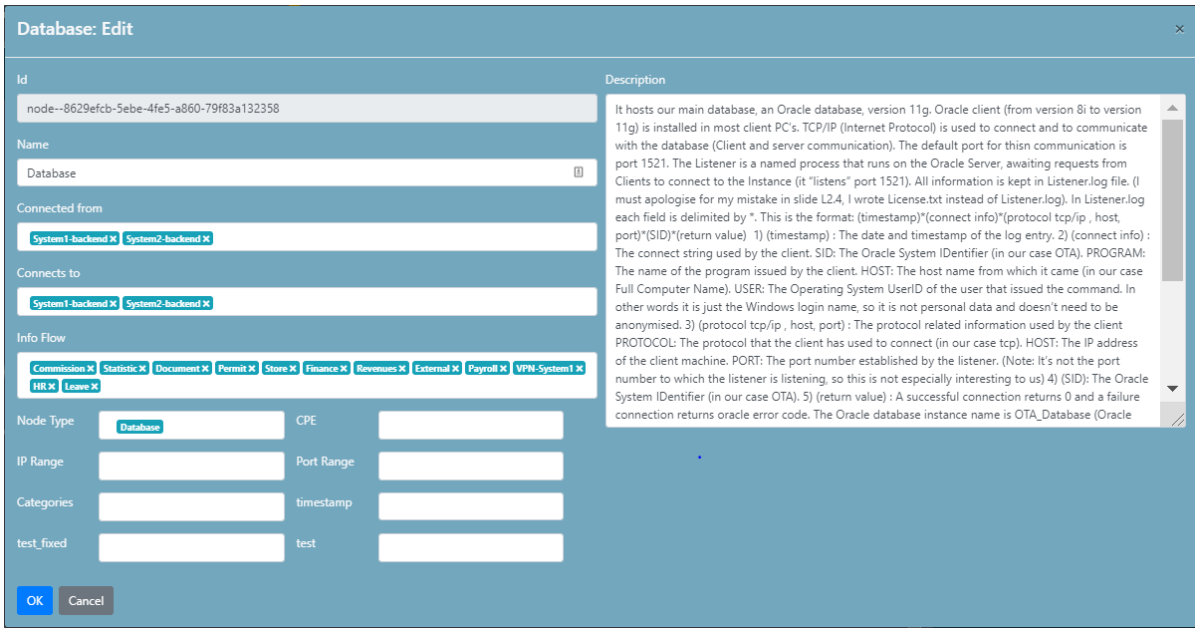
You can access the editing functions if you have sufficient authorisation. The functions can be found with either a right click on the graph, or on the top right action bar over the details for the selected node:





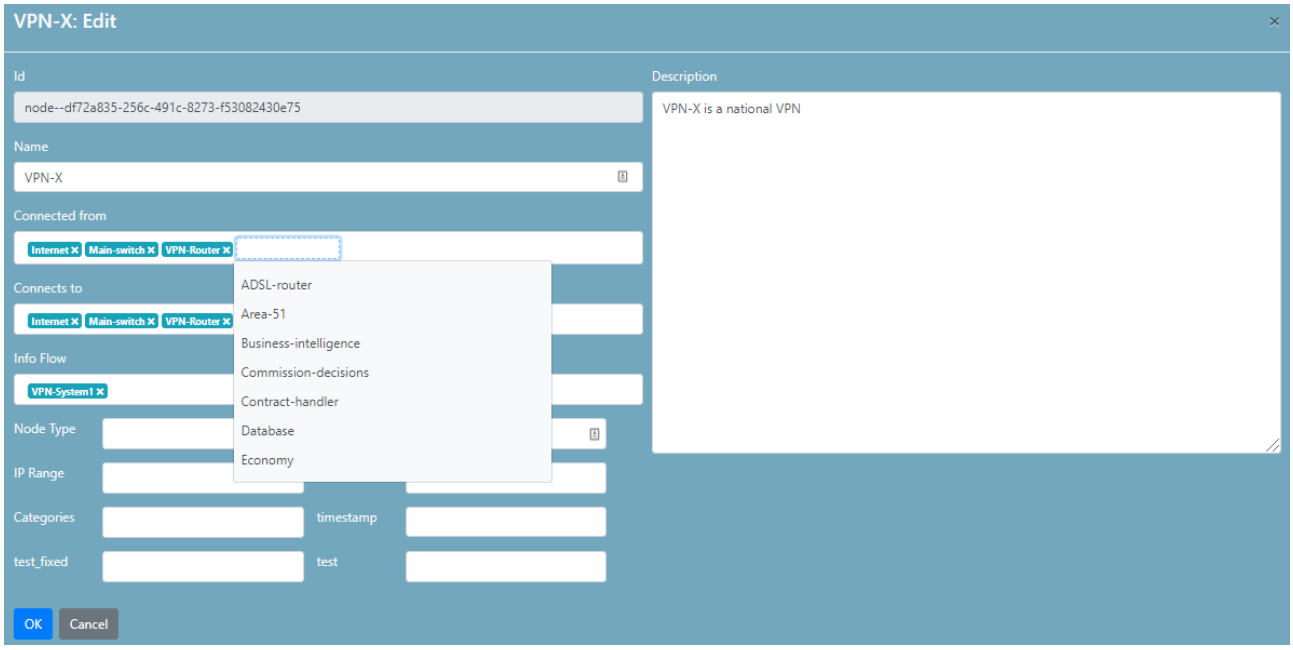
6.5.1.1 Edit, add, or remove a node

The edit dialog allows for editing of the name, description, and other fields you can also connect incoming and outgoing edges. The "Connect From", "Connect To" and "Infoflow" inputs allow for multiple values and have completion/selection enabled. Close the window clicking on the “x” in the upper right-hand corner. The “Categories” field allows one to add/remove/edit context specific keywords to be monitored in external information sources like social media. Security related messages triggered by peer-asset based keyword searches will show up in reports (e.g. “Social media reports” with a “low” threat state associated by default. There are fields that allow to specify more technical parameters (like IP or Port) for each node, but can be left empty if they are not applicable for specific nodes:



6.5.1.2 Multi value edit/select

When you select a multi value field, the edit function will appear and a dropdown with suggested matches will be shown when text is entered:

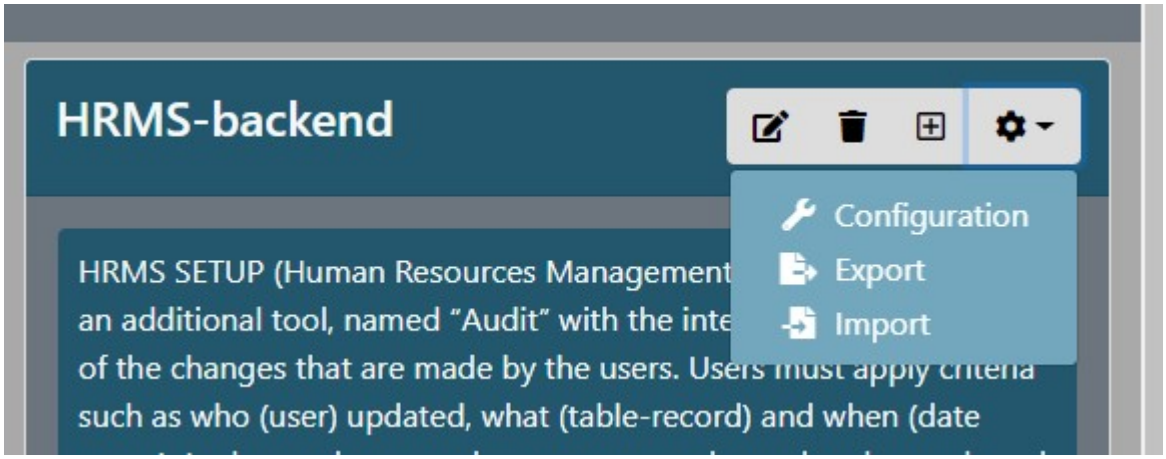


The value can be selected by using up/down arrows. You enter by clicking the value of interest. If the input is empty then left/right arrows will move the input, which can be valuable if the order of

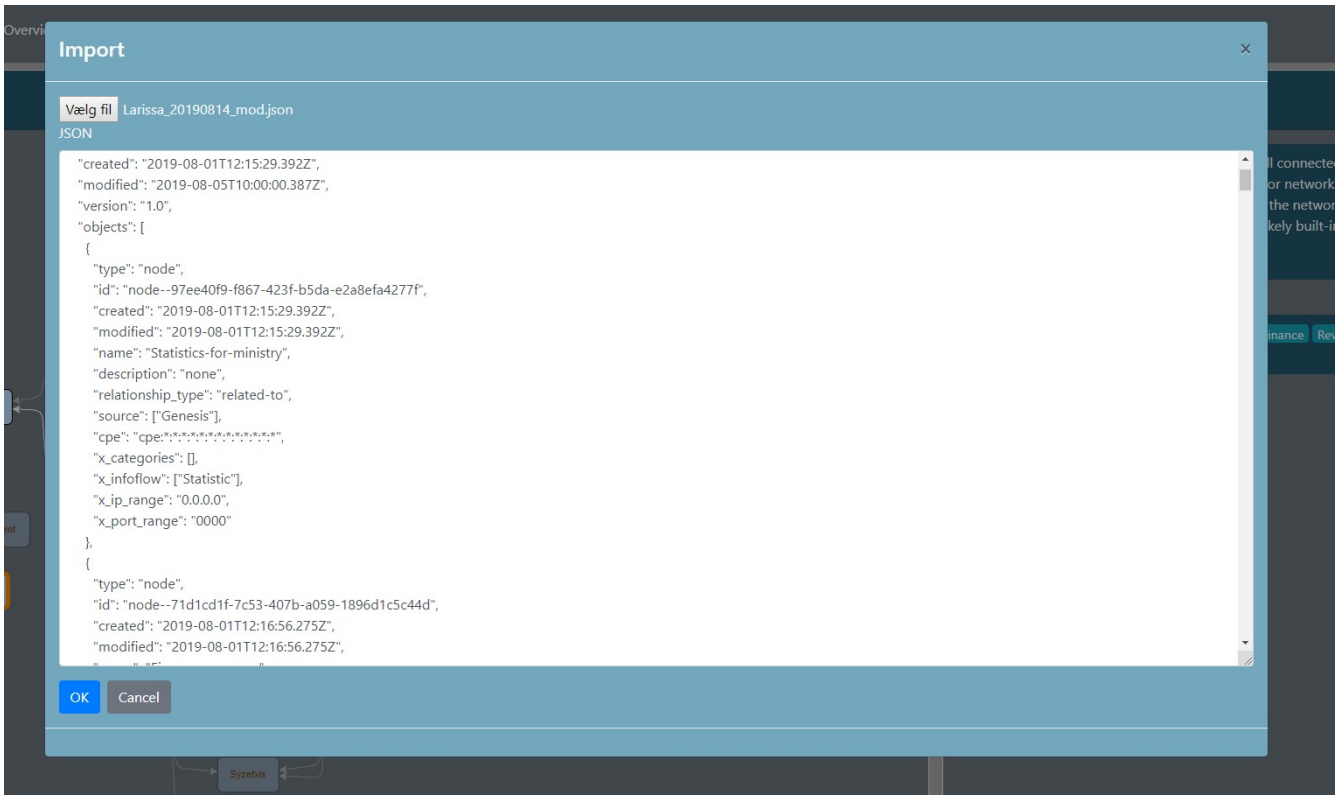
values is important, likewise delete/backspace will remove element to the right or left of an empty input.

6.5.2 System Graph Import and Export

This is a configuration option currently available only for the system administrator user role. On the button in top right of the detail window there are options to import or export a system graph. The format is like STIX in that it has a set of objects where each node is of type node having a set of standard properties and possibly also some custom properties. CS-AWARE visualisation module allows custom properties to be defined and used, but a new import will overwrite all existing system dependency graph data:

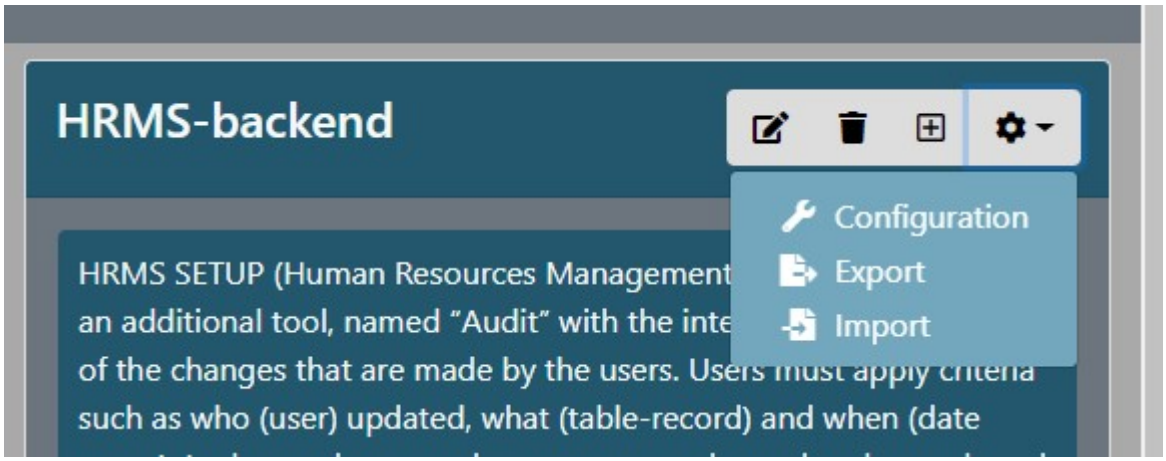


The import dialog allows you to load a file into a text area in order to be able to verify the file before importing, but as it **overwrites existing content** this is **only to be used with caution (and a backup, of course!)**:



6.5.3 System Graph Configuration

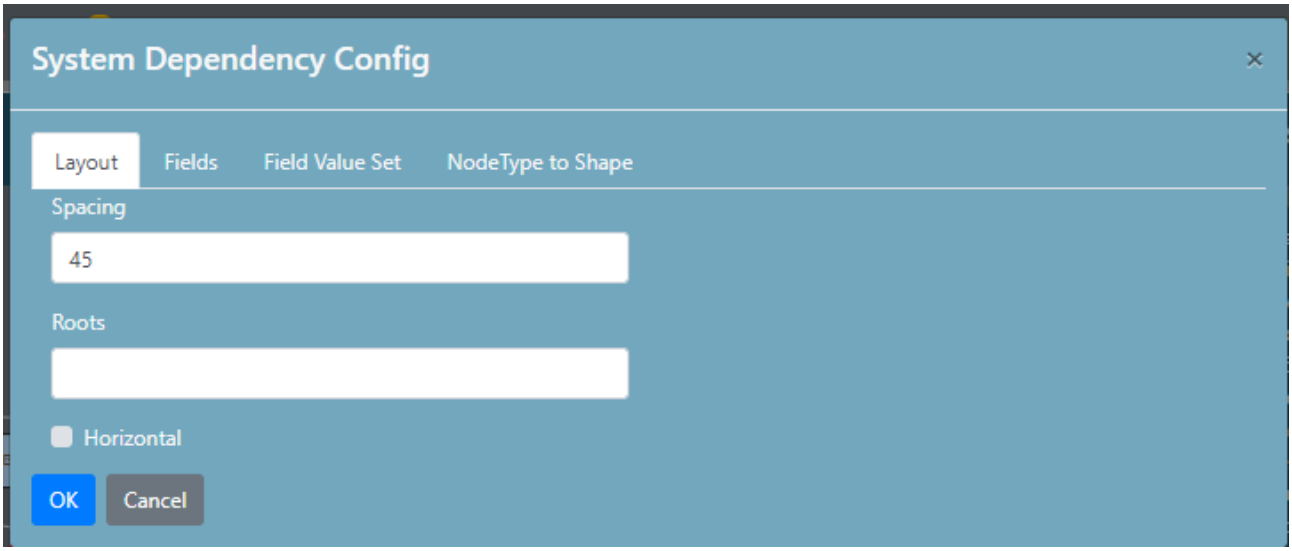
The CS-AWARE system offers configuration options for the system graph relating to layout, field and shape customization. The customization can be reached by selecting “Configuration” in the graph settings:



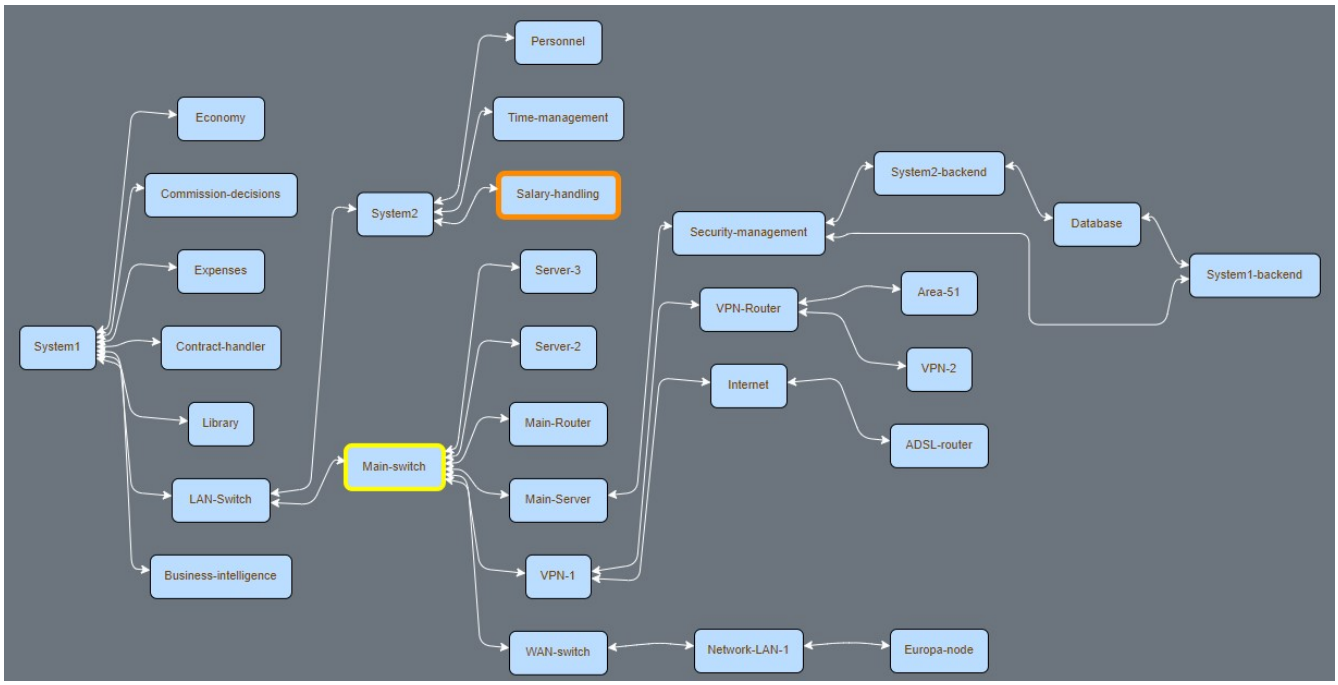
6.5.3.1 Layout

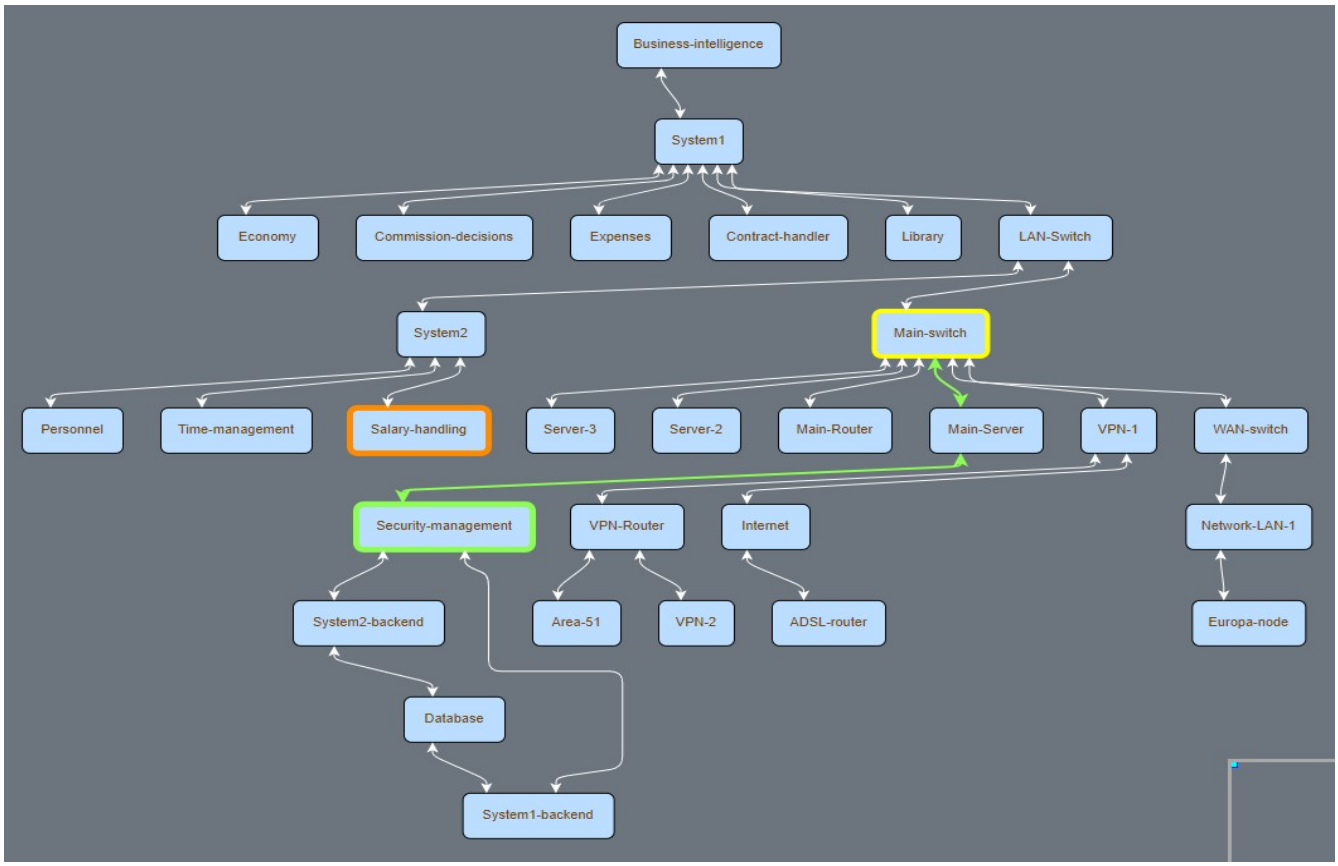
The layout configuration allows you to configure the following

- **Spacing** between nodes
- **Node(s) used as roots**, currently the first root is the major node used.
- **Direction of the hierarchy**: either vertical (top-down) or horizontal if checked (left-right)



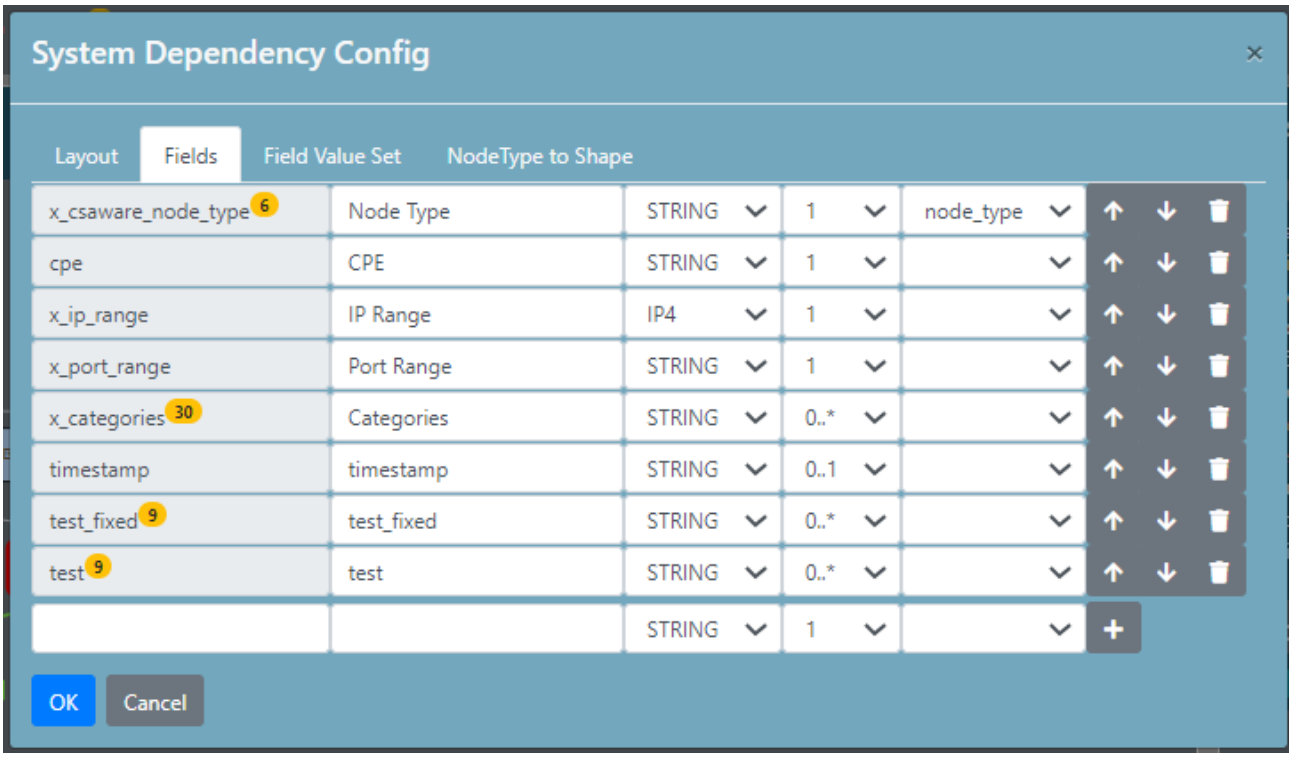
The following screenshots illustrate examples of a graph using horizontal vs. vertical system root configuration:





6.5.3.2 Fields

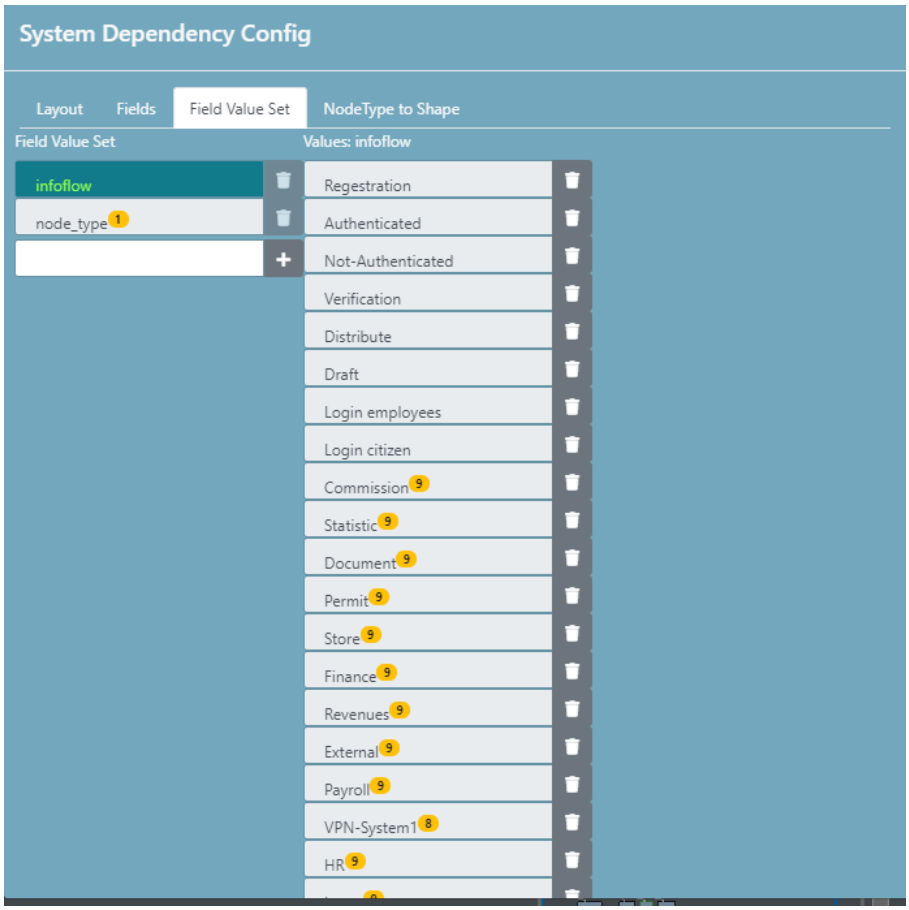
The System Dependency Nodes have some fixed fields like Name, Description and Infoflow, but other data may be valuable to store in nodes like CPE, IP, DNS, etc. To do this, the CS-AWARE supports custom fields, which can be defined in this configuration:



The badges with numbers indicate how many nodes that have values for the given field. The arrow buttons can be used to order the presentation of the fields if a node has values in more than one field. The last line is used to define new fields, and the waste basket buttons can be used to remove already defined fields, in which case the number badge can help avoid the deletion of fields having data.

6.5.3.3 Field Value Sets

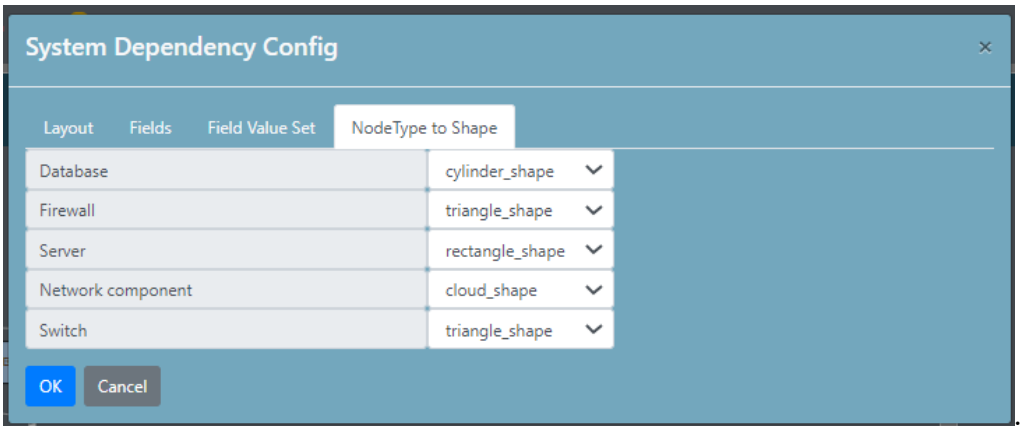
The field value sets are used to restrict the values for a field as described previously. The value sets can be defined and the values for each set can also be defined in this configuration tab:



The first list is the defined value sets. The second list contains the values of the selected value set, which is selected by clicking in the first list. The number badges in the first list are an indicator of how many field definitions that use the value set. On the second list this is how many times the values are used in system nodes. This information is used to avoid unintentional deletion of values that are in use.

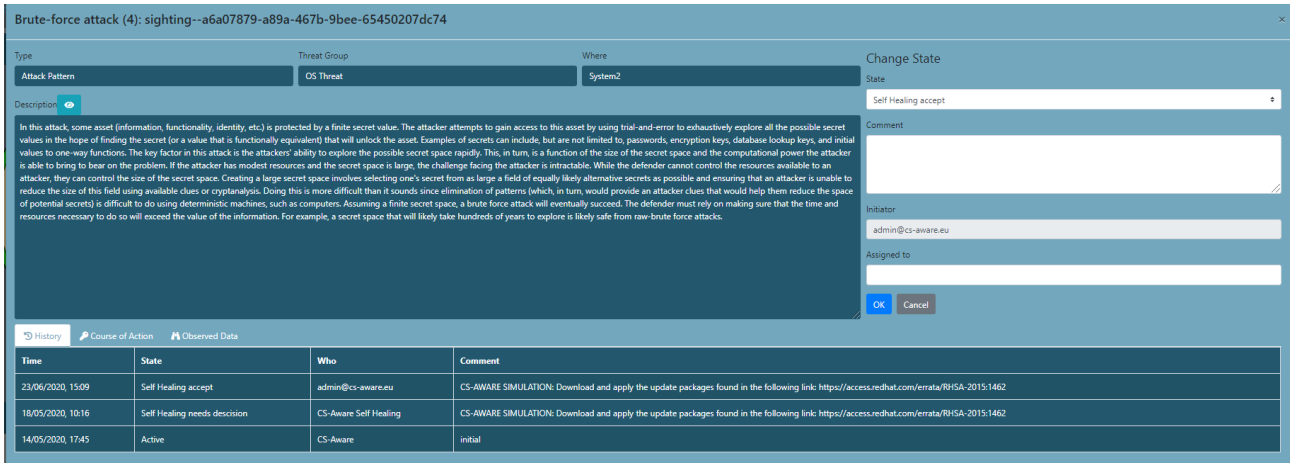
6.5.3.4 Assign custom node shapes

The nodes in the System Graph can be associated with various shapes (see above on the right hand side there is a pull-down menu for each node):



6.6 Threat details

The Threat details view can be opened by clicking on an individual threat in any of the above described threat lists (Overview, Threats, Closed Threats or System):



- The **left** side contains static information from the CS-AWARE system on where this threat was observed and a brief description.
- The **right** side is for changing state, which will be detailed in Section 6.7 and 6.8.
- The **bottom** portion of the screen includes a "history" tab, a "course of action" tab, and a "observed data" tab.

The History Tab contains information about each state change observed for this threat:

History | Course of Action | Observed Data

Time	State	Who	Comment
23/06/2020, 15:09	Self Healing accept	admin@cs-aware.eu	CS-AWARE SIMULATION: Download and apply the update packages found in the following link: https://access.redhat.com/errata/RHSA-2015:1462
18/05/2020, 10:16	Self Healing needs descision	CS-Aware Self Healing	CS-AWARE SIMULATION: Download and apply the update packages found in the following link: https://access.redhat.com/errata/RHSA-2015:1462
14/05/2020, 17:45	Active	CS-Aware	initial

The Course of Action tab contains a description and concrete suggestions from the self-healing process about the course of actions to mitigate the threat (in case self-healing is available):

History | Course of Action | Observed Data

Name	Description	Action
null mitigation	1: Add a firewall rule in order to block the given malicious IP address:.	iptables -A CSAWARE-IN -s csaware:pattern-bruteforcepw >= '0.95' -j drop

The Observed Data tab contains information about context of threat, as determined by the analysis component of CS-AWARE. Those are usually parameters describing system behaviour observed in log files from system components in your organization. This is intended for system administrators working with those aspects of the system to be able to better devise mitigations to the threat:

History | Course of Action | Observed Data

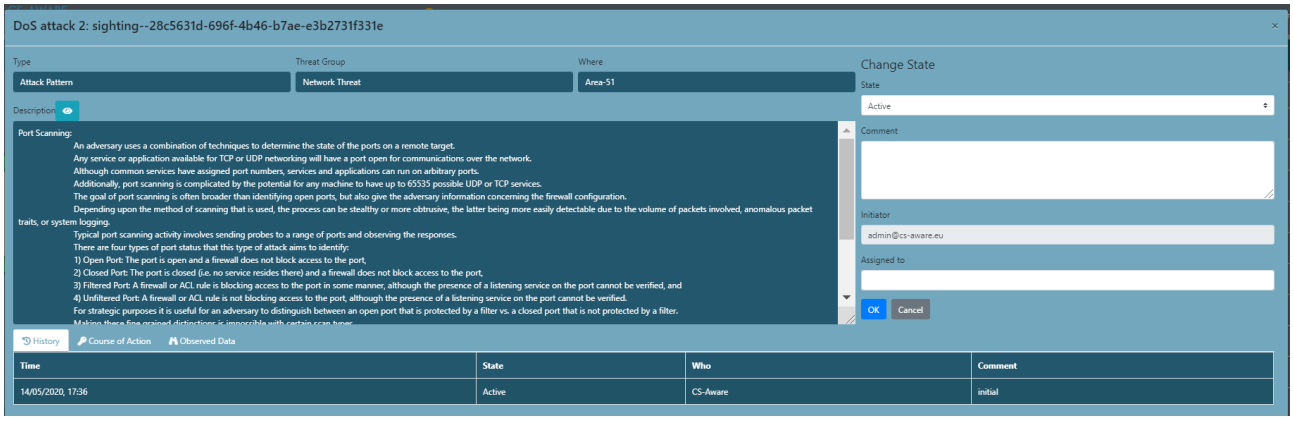
Type	Id	Data			
software	0	name	vendor	version	cpe
		Ubuntu Linux OS	Canonical	16.04.5 LTS	cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*
software	1	name	vendor	version	
		iptables Firewall	Linux	1.8.0	
ipv4-addr	2	value			
		2.3.4.5			
process	3	pid	name	extensions	
		(value=314)	SamS	(windows-service-ext={service_name=SamS, display_name=Security Accounts Manager, start_type=SERVICE_AUTO_START, service_type=SERVICE_WIN32_SHARE_PROCESS , service_status=SERVICE_RUNNING})	

6.7 Active States

Threats that are currently in an active state can be observed in the threats lists in Overview, Threats, and System.

Active states can be observed for threats with no self-healing available (Section 6.7.1) and a self-healing action available (Section 6.7.2). The latter replaces the manual state changing options as seen in Section 6.7.1 with automated handling of states, including visual feedback as shown in Section 6.7.3.

6.7.1 Threat view window in “Active” state



The “Active” state in cases with no self-healing available can be changed manually using the drop-down menu on the right side of the screen.

6.7.2 Self-Healing active state – waiting for manual confirmation

The self-healing active state is indicated by waiting for manual confirmation before applying the self-healing action

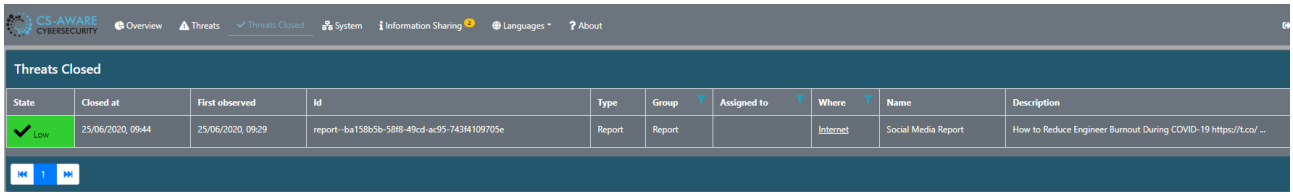
6.7.3 Self-Healing: Threat list items indicate the active states self-healing is currently in

Visual indication of self-healing confirmed by user, but waiting for results:

Visual indication of self-healing action failed. The threat remains in an active state:

6.8 Closed States

Non-active states. The last closed state can be seen under the view "Threats closed":

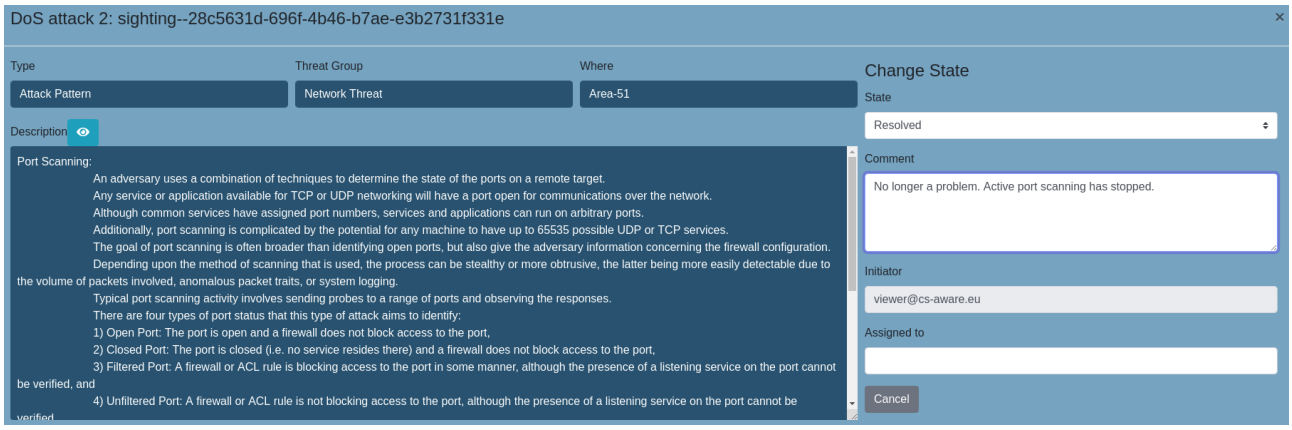


A successfully applied self-healing action results a threat closed state. Following visual feedback is provided in “Threats closed”:

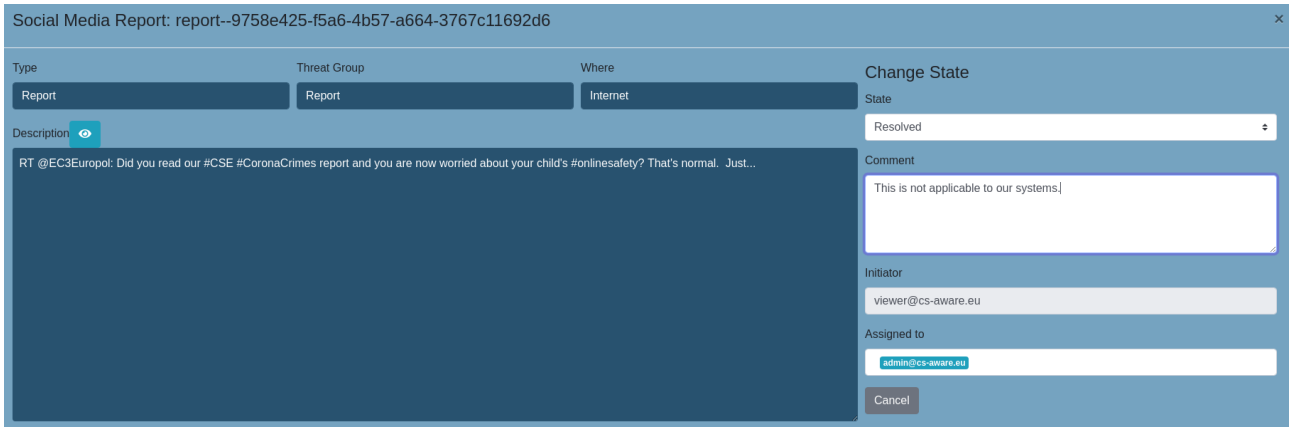
In the threats view, “Self Healing Done” indicates the self-healing module has applied the actions suggested:

A closed threat that did not have a self-healing action associated, can have the two possible states “resolved” and “ignored”.

Resolved refers to the state when appropriate mitigation actions were applied by the system administrator (outside the CS-AWARE context):



Ignored refers to a threat was marked as ignored by a system administrator, and no action has been taken to mitigate the threat:



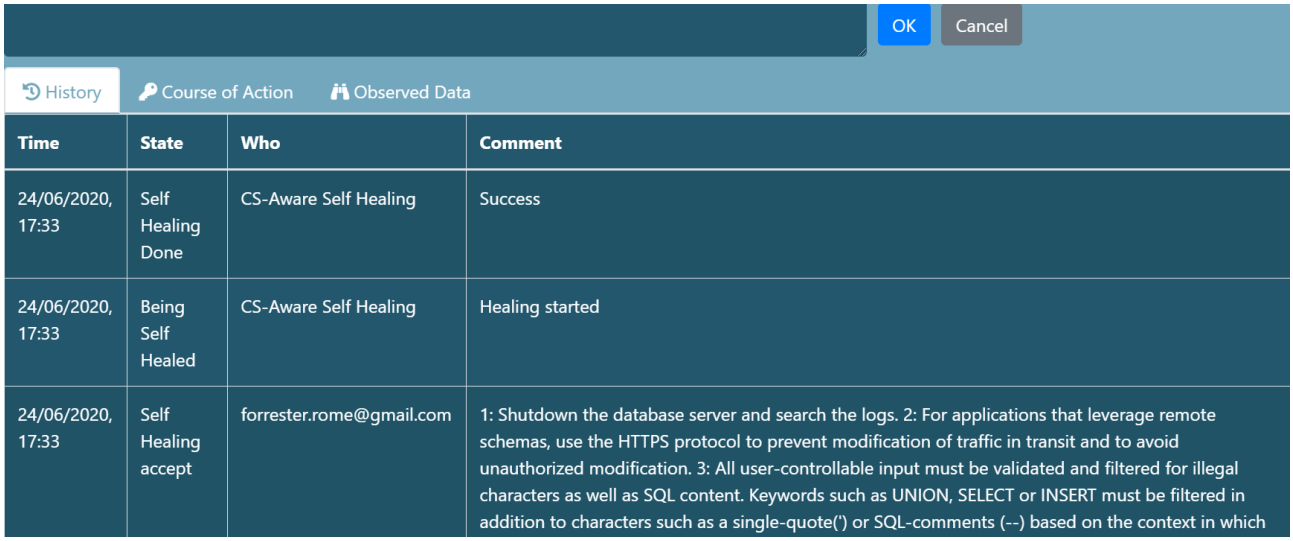
6.9 Changing State

You can change the state of a threat in the **Threat Details** view shown above. For threats where self-healing is available, state changes are done automatically. What changes are possible depend on the current state of the threat. You can insert comments. In addition, the current state can be maintained.

- **Change a threat**: An active threat can be closed by indicating healed or ignored.
- **Reopen a threat**: A closed threat can be reopened. Use the dropdown box to select a state change except for self-Healing choices that have explicit buttons.

Suggestion: When changing states, it is always a good practice to write the actions taken into the State history message**.**

In the threats view bottom screen, the "History" tab indicates the state history of each threat. This particular example shows the history of self-healing applied with success. "State history" comments are shown in the "Comment" section:

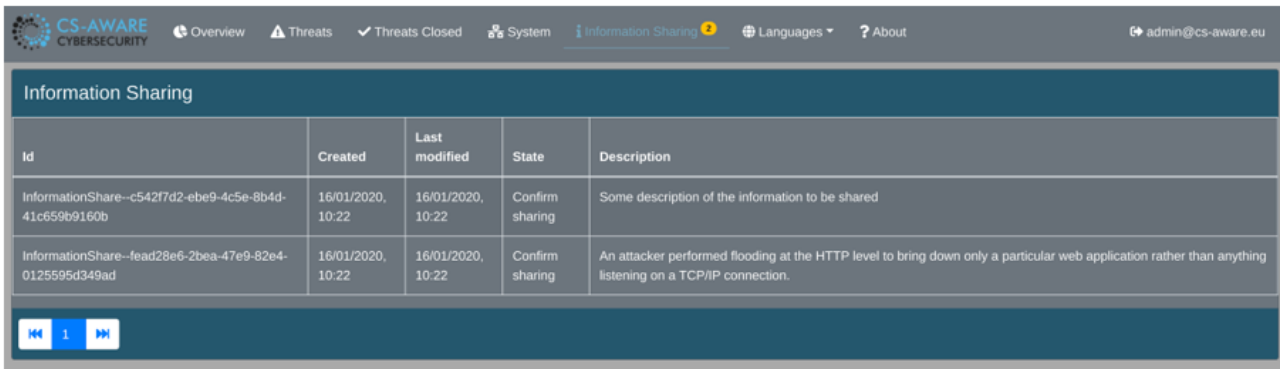


Time	State	Who	Comment
24/06/2020, 17:33	Self Healing Done	CS-Aware Self Healing	Success
24/06/2020, 17:33	Being Self Healed	CS-Aware Self Healing	Healing started
24/06/2020, 17:33	Self Healing accept	forrester.rome@gmail.com	1: Shutdown the database server and search the logs. 2: For applications that leverage remote schemas, use the HTTPS protocol to prevent modification of traffic in transit and to avoid unauthorized modification. 3: All user-controllable input must be validated and filtered for illegal characters as well as SQL content. Keywords such as UNION, SELECT or INSERT must be filtered in addition to characters such as a single-quote(') or SQL-comments (--) based on the context in which

6.10 Information Sharing

Information sharing allows to share information about individual threats with experts or communities outside of your organization. If you allow information sharing for individual threats, the information is posted in a dedicated repository. Only experts or communities that you share the access credentials with will have access to the information.

The information sharing view of the CS-AWARE system lists, for each sharing event, the unique ID, the date the event was created and last modified, the current state as well as the sharing event description:



The information sharing details for each listed information share contain a summary of the threat to give context to the user allowing the share (this summary will not be shared), a description of the context that can be edited or deleted before sharing, and a set of parameters that were relevant in the detection and handling of the threat the information share relate to. Each individual parameter can be deleted before allowing or denying the information share: