Increasing Cybersecurity Awareness and Collaboration in Organisations and Local / Regional Networks: The CS-AWARE-NEXT Project

Christian Luidold[1,*,†], Thomas Schaberreiter[2,*,†], Christian Wieser[3,*,†], Adamantios Koumpis[4,*,†], Cinzia Cappiello[5,*,†], Tiziano Citro[6,*,†], Jerry Andriessen[7,*,†] and Juha Röning[8,*,†]

[1]*Multimedia Information Systems, University of Vienna, Austria*
[2]*CS-AWARE Corporation, Estonia*
[3]*BISG, University of Oulu, Finland*
[4]*Institute for Biomedical Informatics, University Hospital Cologne, Germany*
[5]*Dipartimento di Elettronica, Politecnico di Milano, Italy*
[6]*Department of Computer Science, Università degli Studi di Salerno, Italy*
[7]*Wise & Munro Learning Research, Netherlands*
[8]*BISG, University of Oulu, Finland*

Abstract

The Horizon Europe CS-AWARE-NEXT project aims to improve the cybersecurity management capabilities of organisations and local or regional supply networks. These organisations operate in a highly dynamic cybersecurity environment and are required to comply with European legislation, such as the Network and Information Security (NIS/NIS2) directive.

To effectively manage cybersecurity, these organisations need to adopt a more dynamic and collaborative approach, building on a shared situational awareness of potential cybersecurity issues relevant to the organisations. It is well known that flexibility increases when the availability of information increases. The goal of the paper is to discuss the architecture required to gather and share relevant information with the organisations in the network. Smart collaboration about cybersecurity data requires intelligent selection of data, adapted to the goals of the collaborative scenario, as well as object oriented interfacing, facilitating the inclusion and selection of particular data types during online interaction. Collaboration about specific data, used as evidence or as resource for discussion, has to take place online due to the opportunistic nature of data selection.

In contrast to traditional technologies, we highlight the need for experimenting with novel approaches to information systems engineering which are capable of addressing emerging needs from the inclusion of dedicated Artificial Intelligence and Machine Learning modules, and components for self-healing, self-protecting, and self-configuration.

CCS CONCEPTS Social aspects of security and privacy, Usability in security and privacy, Systems theory, Interactive systems and tools, Collaborative and social computing systems and tools

Keywords

Business Continuity, Disaster Recovery, Critical Infrastructure Protection, Cybersecurity Management, Corporate Information Infrastructures

1. Introduction

Cybersecurity awareness helps organisations to protect their information systems from unauthorized behaviour. Its aim is to provide information on the importance of cybersecurity, assist in identifying potential threats and recommend appropriate responses. CS-AWARE-NEXT is a follow-up project to CS-AWARE [1, 2], a successful H2020 project that concluded in August 2020. CS-AWARE provides an advanced real-time cybersecurity awareness and management framework and platform implementation for local public administrations and NIS sector organisations. Its main features include a socio-technical and organisational focus, intra-organisational collaboration and skill building, multi-lingual semantics support, AI-based real-time awareness and visualization utilizing threat intelligence, system self-healing and cybersecurity information sharing. A demo of the CS-AWARE platform is available on the CS-AWARE Corporation's [2] web page.

CS-AWARE was designed around the multi-level collaborative European cybersecurity framework as defined by the European cybersecurity strategy of 2013 [3] and subsequent legislation, e.g., NIS directive. A major outcome of the CS-AWARE project was the establishment of the CS-AWARE Corporation for facilitating the exploitation of the CS-AWARE project results and to bring the CS-AWARE platform to the market.

The European cybersecurity strategy of 2020 [4] and the updated NIS2 [5] proposal directive emphasise the need for stronger collaboration on all levels of the multi-level collaborative cybersecurity environment. Furthermore, the proposal directive on the resilience of critical entities [6] has been designed to replace current legislation for critical infrastructure protection and builds on the success of the NIS directive by aligning the framework for managing physical and cyber-physical risks with the collaborative framework defined by the NIS directive for managing cyber risks.

One may consider CS-AWARE as the first socio-technical cybersecurity platform that reinforces organisational defences against malicious attacks by 'mapping' the grey areas in the interaction between systems and humans. It aims to make companies and organisations aware of the unique complex socio-technical relationshipsthat exist, while providing the technical means to monitor and manage them. As the majority of security technology is almost exclusively focused on security on the technical level, CS-AWARE considers the systemic aspect of cybersecurity in an organisation, e.g., network weakness, where clusters of machines interact without a clear understanding of their connections. It also takes into account the human element, e.g., where human 'workarounds' have been implemented to address system deficiencies. CS-AWARE is designed to detect and manage these blind spots in a unique and innovative way.

S3C'23: Sustainable, Secure, and Smart Collaboration Workshop, Hosted by CHITALY 2023, SEPTEMBER 20–22, 2023, TURIN, ITALY

[*] Corresponding author.

[†] These authors contributed equally.

christian.luidold@univie.ac.at (C. Luidold); thomas.schaberreiter@cs-aware.com (T. Schaberreiter); christian.wieser@oulu.fi (C. Wieser); adamantios.koumpis@gmail.com (A. Koumpis); cinzia.cappiello@polimi.it (C. Cappiello); t.citro5@studenti.unisa.it (T. Citro); jerry@wisemunro.eu (J. Andriessen); juha.roning@oulu.fi (J. Röning)

CEUR Workshop Proceedings (CEUR-WS.org)

Cybersecurity is socio-technical in nature and heavily depends on the human factor in an organisation, and the interactions between humans and systems. All the security in the world cannot prevent malicious behaviours that exploit human ignorance and vulnerability. Thus, cybersecurity is an organisational issue that goes beyond the IT department and needs to be treated accordingly by cybersecurity solutions. What sets CS-AWARE apart is its organisation centric approach, as opposed to other event centric approaches. CS-AWARE allows organisations to define what is normal or abnormal based on their specific business, social and technical context. AI/machine learning is used to identify abnormal behaviour based on those patterns, contextualized with information about the threat/attack causing this behaviour, and provide tailored mitigations to counter the attacks – in line with, and supported by, European collaborative cybersecurity legislation (e.g., NIS/NIS2). The socio-technical consideration of cybersecurity, holism and systemic thinking, sustainable skill transfer to organisations/collaboration, and focus on supporting legal cybersecurity compliance efforts (e.g., NIS, GDPR) constitute the unique and distinguishing characteristics of CS-AWARE in the cybersecurity ecosystem.

The paper is organised as follows. Section 2 provides a reference scenario to cater for the management of local and regional incidents and risks. As story-telling was one of the main methodologies for working with our end users (the other being the soft systems methodology), our aim for the scenarios was to collect as much actionable information as possible. Section 3 presents the methodological framework that is later (in Section 5) 'translated' into a system. This comprises three different levels which are presented separately in respective subsections, followed by a discussion of the organisational policies for sharing data among different stakeholders. Section 4 presents what we call the AI pipeline of the system that aims to support operations within the multi-level European cybersecurity framework, by means of filtering relevant data, and identifying and correcting errors and inconsistencies. To our knowledge, this is a distinct and innovative element of our approach, as there are no other systems that offer such functionality in the addressed field. Section 5 presents the architecture of the system with elaborate information on the platform user interfaces and the interaction elements of the system. For this reason, we have included sufficient number of visuals (screenshots and flow diagrams), to enable a better understanding of the platform. The last two Sections 6 and 7 present related work in the field, and also some aspects that we consider important for future research activities.

2. CS-AWARE-NEXT Motivating Scenario

To illustrate more concretely what CS-AWARE aims to accomplish, we present the context of a prototypical case that can take place in every organisational context, both public and private. It concerns the review (by several stakeholders), of a cybersecurity incident that took place at one company. In this particular case no other companies were attacked, but the local server, maintained through a third-party company, was affected causing the loss of 2 months of data. As a result, the configuration was changed, a newer version of Windows was installed, and also a hardware firewall.

Usually, only a few people from the IT department are involved in handling an incident; perhaps some managers, and some users had experienced problems with access to and retrieval of Information. Usually, after an incident has been resolved, it is not reviewed, and business continues as if nothing happened. However, in our scenario, this review is extensive and involves many stakeholders. In particular, stakeholders from other organisations in the region are included in the review as well, because they are part of the same supply chain. This requires collaboration, and when executed well, all involved will have increased awareness of this type of incident, and of the internal machinery of incident handling, and risk management. Moreover, the company would have increased resilience against attackers, and improved business recovery.

This could be achieved through a review of supply chain interdependencies, finding weaknesses and problems that came to surface during the attack. Among many things, this requires awareness of the dependencies within and between local and regional organisations, joint security policies, or awareness of the differences, awareness of supplier cybersecurity awareness and standards. Clearly, much can only be resolved through collaboration and the sharing of many policies and data. Some information comes from the Internet, some from social media, some from places where information about cybersecurity issues is shared. Other knowledge is from a specific organisation, including incident history. There is a third level that is relevant as well, which we call the ecosystem level, where knowledge is shared that is relevant for local and regional organisations. In this contribution, we discuss this sharing of information, and the supporting architecture.

3. Information Sharing for Cybersecurity Awareness

In the continuously evolving landscape of cybersecurity, it is crucial for organisations to stay ahead of potential threats. An established approach to achieve this is through collecting, processing, analysing, and correlating data from various sources to facilitate the understanding of motives, targets, and behaviours of potential threat actors. This allows organisations to make informed decisions regarding proactive measures to increase their resilience against cyber-attacks and mitigation actions to decrease their impact.

One of the issues addressed in Section 2 is the gap in awareness, the ability to collaborate effectively, and ultimately the availability of data and information when dealing with cybersecurity incidents that are not contained within one organisation, but span across an organisations supply ecosystem. We have identified the need to improve cybersecurity awareness and collaboration in this context, especially when dealing with local/regional networks, as much of the supply chain dependencies of an organisation still have a local/regional context. Henceforth, we use data-driven collaboration as a collaborative approach where users are provided with a continuous view of data to enhance the availability and referentiality of information, enabling them to effortlessly keep up with messages and reply in context, even on complex topics that involve significant amounts of data. To that end, we have identified the need for a data-driven collaboration platform that connects individual organisations and that utilises all the available data and intelligence to foster and facilitate collaboration on cybersecurity.

In this chapter, we propose a three-level framework for classifying and analysing cyber-related data: internal data, ecosystem data, and global data. We also discuss the organisational policies for sharing data among different stakeholders.

3.1. Data to Improve Cybersecurity Awareness and Collaboration

Cybersecurity awareness and collaboration are critical to helping organisations protect their assets from those seeking to compromise them. Yet, many organisations struggle to develop and maintain a strong culture of cybersecurity among their employees, partners, and customers. One way to overcome these challenges is to provide relevant and timely information about the cyber threat landscape, best practices for cybersecurity awareness, and the benefits of collaboration among stakeholders, using data collected from a variety of sources, according to the data-driven approach of CS-AWARE.

We rely on a diverse set of cybersecurity related data to contextualize cyber incidents, with knowledge and intelligence created by others in order to facilitate the prevention and mitigation of cyber incidents, as well as helping people in an organisation to manage cybersecurity in the most holistic, efficient and effective way possible. Table 1 summarises the knowledge sources that are available to facilitate data-driven collaboration in CS-AWARE-NEXT.

3.2. Data at Different Levels

We categorize the knowledge sources set out in Table 1 with respect to our proposed three-level framework regarding its availability for stakeholders: Internal data, ecosystem data, and global data. A schematic illustration is provided in Figure 1. The goal of this framework is to facilitate the correlation and enrichment of data to support cybersecurity awareness, the understanding of incidents anomalies in an organisational network and in its supply chain, while enabling user-defined privacy settings to prevent unintended disclosure of internal data.

- Internal data: This refers to the data generated and collected within an organisation's own network. Defined as **Organisational Cybersecurity Knowledge** and **Organisational Incident History**, it includes user activity logs, firewall logs, antivirus alerts, system configurations, vulnerability scans, network topology maps, asset inventories, and incident reports, but also best practices, cybersecurity strategies, and lessons learned. Internal data can help organisations monitor their own security posture, identify threats and anomalies, perform analysis and forensics, and execute mitigation actions. However, to provide a comprehensive view of the threat landscape or the threat actor's objective, internal data may not be sufficient.
- Ecosystem data: This refers to the data shared among organisations having common interests and goals, e.g., by being part of the same sector, supply chain, or interest group. It consists of anonymized internal data, which is further enhanced by the **Ecosystem Knowledge** provided by members of the ecosystem. Ecosystem data can help an organisation gain insight from the experiences and resources of other organisations, improve the ability to detect and prevent threats, and enhance collaboration and coordination.
- Global data: This refers to the data available from public or official sources that provide varying degrees of breadth and detail about cyber threats and current trends. Defined as **Social Media** and **Threat Intelligence**, it includes news articles, blog posts, social media posts, announcements from government agencies and public administrations, as well as OSINT feeds from organisations and communities. Global data can help an organisation

Table 1
Knowledge sources to be utilised for data-driven collaboration in CS-AWARE-NEXT

Knowledge source	Description
Social Media	Discussions about security relevant aspects by relevant people in the security community or from relevant discussion groups/channels. Social media often provides the first discussions about novel attacks that slowly spread among organisations. Social media discussions can help pinpoint and identify abnormal behaviour observed, without necessarily being able to derive mitigation measures from such conversations.
Threat Intelligence	Threat intelligence represents structured or semi-structured information about threats and attacks, often including detailed information about how to detect such threats or attacks (indicators of compromise) and mitigation actions (courses of action). Threat intelligence is often provided by authorities like CERTs/CSIRTS, by commercial threat intelligence providers, or by open communities.
Organisational Cybersecurity Knowledge	This is a novel type of knowledge not available in this form outside of CS-AWARE. This knowledge is created for each organisation using CS-AWARE based on socio-technical analysis, and it contains knowledge items for each asset that range from general (e.g., human-readable description) to very specific (e.g., asset inventory).
Organisational Incident History	In addition to detailed knowledge about an organisation, an incident history for each past incident is available, containing knowledge items like the incident timeline and, ultimately, the mitigation mechanisms applied to resolve the incident.
Ecosystem Knowledge	The ecosystem knowledge that can be created through CS-AWARE-NEXT is not yet fully defined since the project is still in its early stages at the time of writing. However, CS-AWARE-NEXT will facilitate the creation of knowledge items relating to ecosystem collaboration that are not available through other sources. It will include: • An ecosystem map similar to the system dependency graph in organisations. It will be able visually to represent a local/regional ecosystem and its relevant dependencies. The ecosystem elements will be formed around organisations and services supplied or consumed by organisations. • A history of collaboration within the ecosystem, both for cybersecurity issues that span across multiple organisations in the local supply ecosystem, and for cybersecurity incidents for which an individual organisation seeks knowledge and collaboration within the ecosystem in order to resolve the incident. • A general history of experiences and stories that collaborators on the ecosystem might want to share to help other organisations in similar situations.

stay informed about latest cyber incidents and developments, understand the motivations and objectives of threat actors, and identify emerging threats and vulnerabilities.

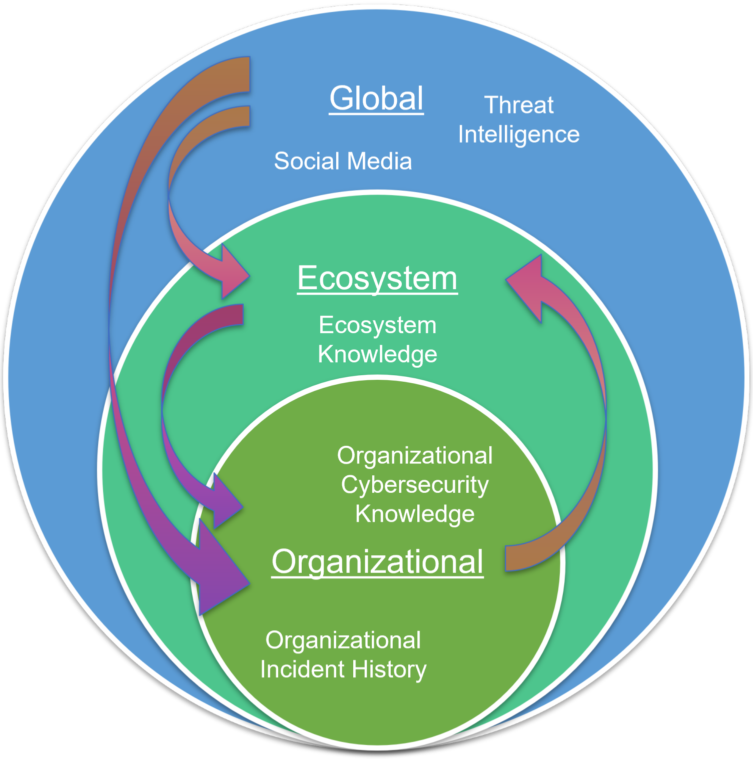


Figure 1: Knowledge sources from Table 1 assigned to their respective level. Global data serves as input for all levels, while organisations and their ecosystems can mutually exchange their data

3.3. Organisational Policies for Sharing Data

Having defined the knowledge sources and the different levels of data to be shared, one problem remains: The sharing policies of individual organisations. Organisations are reluctant to share internal data with others for various, albeit legitimate, reasons. The disclosure that they have been the victim of a cyber-attack could be damaging to their reputation, and the sharing of internal network topology data could raise new security concerns due to lack of trust. In addition, organisations may be reluctant to participate in information sharing activities due to legal challenges or confidentiality concerns.

Organisations can implement organisational data sharing policies that outline the rules and principles of what data can be shared with other organisations to address these concerns and facilitate data sharing for cybersecurity awareness and collaboration. A key aspect is pseudonymization, anonymization, and selective selection of data fields to share. Compliance with applicable laws and regulations is also important.

By incorporating shared internal data from others, as well as data from the global level, and using it to correlate and enrich their own data, organisations can increase their understanding of cyber incidents and anomalies in their network. This can improve their awareness of cybersecurity and their ability to collaborate with other organisations in their industry or supply chain, as well as with government authorities.

To facilitate information sharing, HCI issues should be considered in designing user-friendly interfaces for organisations to share their data according to their needs, to access data from different ecosystems and at the global level, and to communicate and collaborate with other organisations and authorities.

Organisations can improve cybersecurity awareness and collaboration while protecting sensitive information by addressing these concerns, developing effective organisational policies, and incorporating HCI principles for user-friendly data sharing and communication.

4. AI-based Data Analysis Pipeline

As described in the previous sections, cybersecurity awareness is enabled by information sharing. As described in Section 3.2 data are shared at different levels; organisations can exchange information with each other, or the CS-AWARE platform can broadcast information gathered from external sources, such as social media or threat intelligence feeds. However, to be effective, the information that is shared must be reliable.

To this aim, the goal is to develop an effective and efficient AI pipeline that can operate within the multi-level European cybersecurity framework to ensure the quality of data used by the AI at the time it is collected. This will be done by using an appropriate data preparation pipeline that, by means of normalization and cleaning components, can filter relevant data and identify and correct errors and inconsistencies. In this way, it is possible to build a high-quality input dataset that is analysed with AI/ML-based models. Such analyses go from simple tasks such as finding outliers, to more complex activities such as correlation or prediction of anomalous events detected within organisations. In particular, the analysis pipeline is composed of the following steps:

1. *Data collection and cataloguing*: The design of a proper data lake architecture is a prerequisite for the ingestion of internal and external sources that will be described in the data catalogue, and the effective use of modern AI models applicable to the CS-AWARE-NEXT context.
2. *Data preparation and quality assurance*: We define it as the set of pre-processing operations performed in early stages of a data analysis pipeline. Data preparation includes many different cleaning and normalization components, and users often experience difficulties in selecting the pre-processing methods that can optimize the final results. For this reason, data preparation is often performed by using the most commonly used data standardization and cleaning techniques to guarantee a certain data quality level. Building on previous experience with application-aware data quality (DQ) assessment, the definition of the data preparation pipeline will be driven by the socio-technical analysis provided in other parts of this project to support the proposed pre-processing and DQ activities.
3. *AI data correlation models*: Building on the data quality assurance and cataloguing activities, the AI models for data correlation and contextualisation can rely on effective and efficient access to the data via a data-lake interface with the use of AI technologies such as deep learning and reinforcement learning for anomaly and threat detection, contextualization with threat intelligence, and to support the design of mitigation and self-healing

strategies (including disaster recovery and business continuity) tailored to individual organisational set-ups.

A reference implementation of AI based data quality assessment and correlation framework, as well as its operational integration, will be provided in the context of the CS-AWARE platform.

5. CS-AWARE-NEXT Architecture

The CS-AWARE approach relies on two main user interfaces for awareness and collaboration to allow the users to interact with the data collected and analysed by the CS-AWARE AI, and to perform the processes designed by CS-AWARE to allow for effective and efficient handling of cybersecurity incidents within organisations and in the context of local/regional ecosystems. Both interfaces follow a human centric approach, facilitating knowledge creation and knowledge management by key stakeholders, and supporting them in their activities through automation in a natural and intuitive way.

CS-AWARE platform UI: Is designed to create cybersecurity awareness based on a socio-technical and data driven approach within individual organisations, and provides cybersecurity incident management procedures that assist the relevant stakeholders in an organisation to resolve or mitigate incidents efficiently and effectively.

CS-CONNECT: Is designed to allow data-driven collaboration and knowledge creation/ knowledge management by facilitating topical discussions to resolve cybersecurity problems within individual organisations, or more complex incidents spanning multiple organisations of an ecosystem.

In the following, we are introducing the core concepts that define the user interaction in CS-AWARE and CS-CONNECT.

5.1. CS-AWARE Platform UI

The CS-AWARE platform UI is designed around the knowledge created through socio-technical analysis of an organisation. CS-AWARE focuses on a novel approach to socio-technical cybersecurity management in organisations, following a data-driven approach to create awareness by, in a first step, working with the only people able to understand how an organisation really works; the people working in an organisation and with organisational IT services, systems and networks on a daily basis. CS-AWARE has developed a novel socio-technical system and dependency analysis methodology based on the tried and proven soft systems methodology, (SSM) [7] in order to generate an organisational knowledge repository relating to cybersecurity relevant assets. In the CS-AWARE approach, as depicted in Figure 2, the results of this analysis are prepared in a machine-readable form through the CS-AWARE platform, in order to collect all this multi-stakeholder knowledge in one single place, and to be able to act on this information in an automated way in order to create awareness and deal with incidents.

The CS-AWARE platform provides automation to monitor identified assets, and detect and contextualise incidents using the data sources and AI capabilities described in previous sections. In this Section we focus on how the platform UI supports users once an anomaly or incident has been brought to the attention of the user. While the platform UI has several usage scenarios,

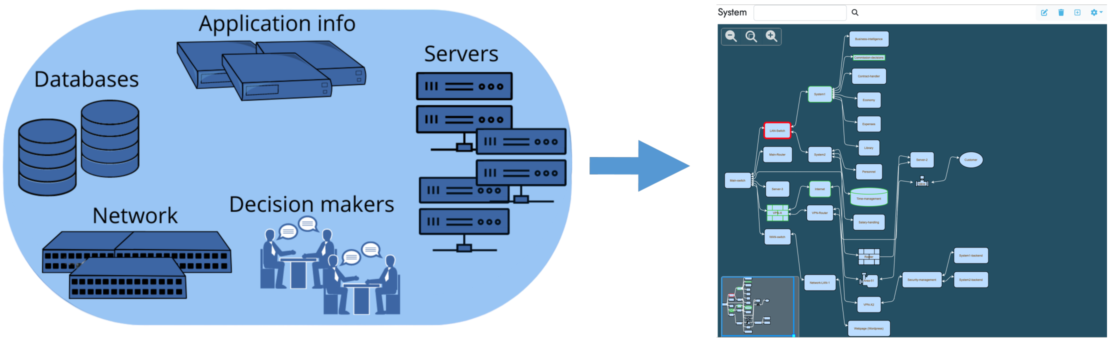


Figure 2: The CS-AWARE soft systems analysis process

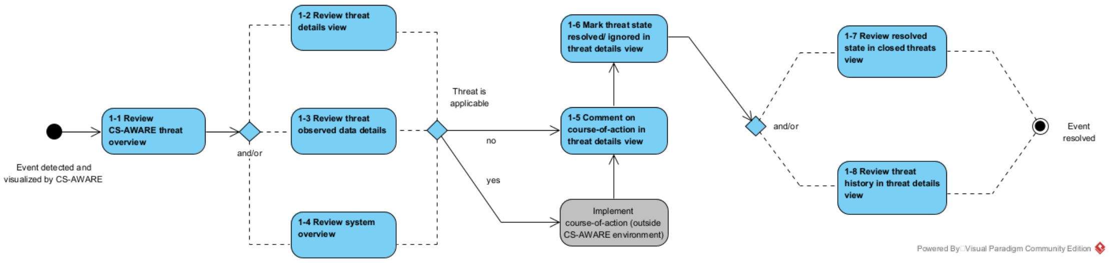

Event detected and visualized by CS-AWARE
1-1 Review CS-AWARE threat overview
and/or
1-2 Review threat details view
1-3 Review threat observed data details
1-4 Review system overview
Threat is applicable
no
yes
1-5 Comment on course-of-action in threat details view
1-6 Mark threat state resolved/ ignored in threat details view
Implement course-of-action (outside CS-AWARE environment)
and/or
1-7 Review resolved state in closed threats view
1-8 Review threat history in threat details view
Event resolved
Powered By: Visual Paradigm Community Edition

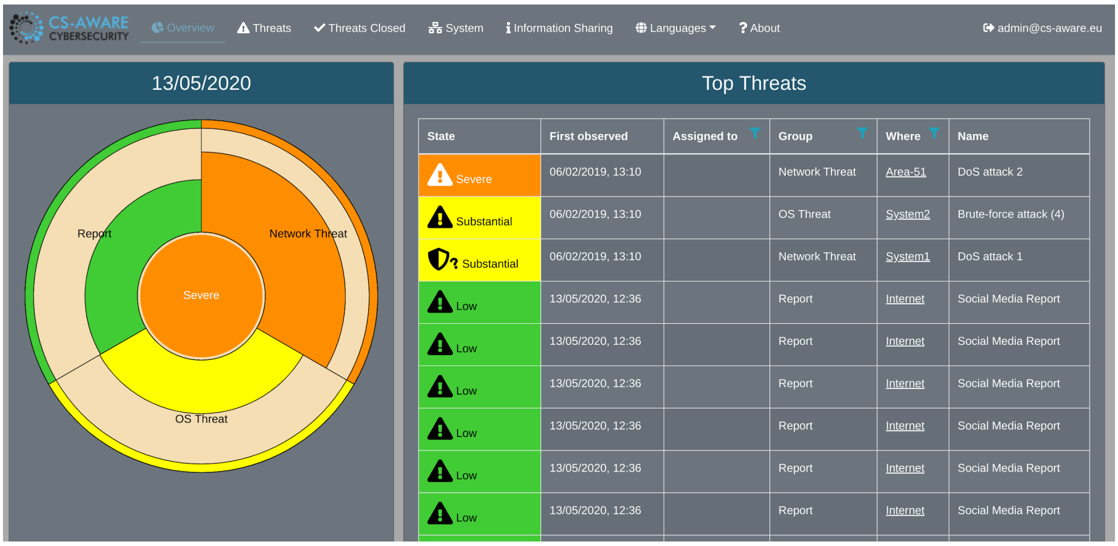
Figure 3: CS-AWARE usage scenario - managing a cybersecurity incident

we will focus on the simplest one as illustrated in Figure 3, a user is made aware of an incident, understands how to resolve the issue, implements a resolution, and adds to the organisational knowledge by commenting on the resolution. Figure 3 illustrates 8 steps that can be taken by the CS-AWARE platform user to resolve an issue (Steps 1-1 to 1-8).

In Step 1-1, the user is made aware of threats detected by the CS-AWARE platform (Figure 4). 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.

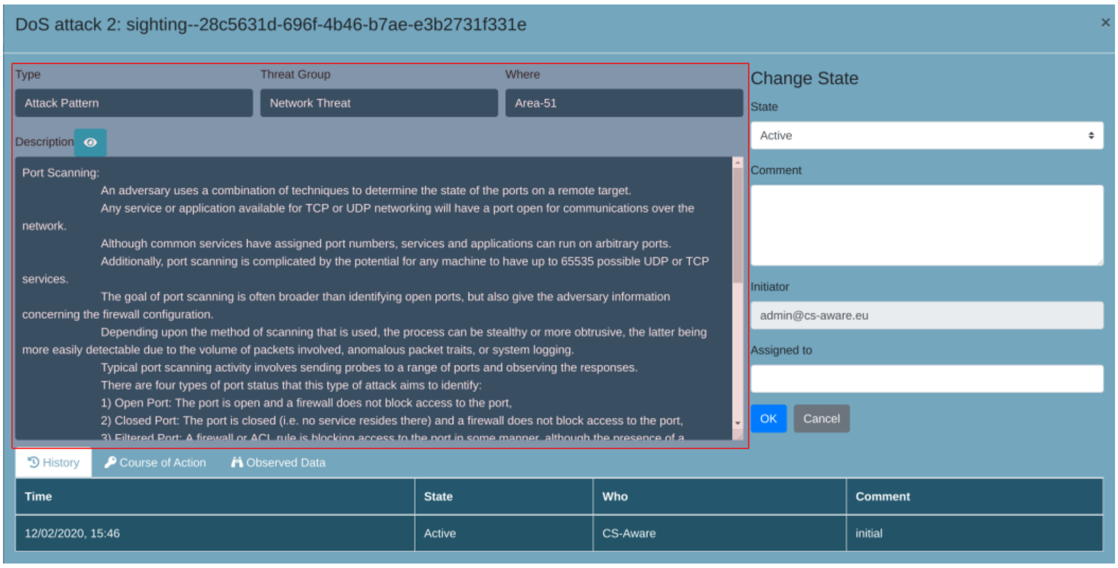
In step 1-2, the user can review the threat details and context (Figure 5). Each threat event has a detailed view that is accessible by clicking on the event in the CS-AWARE threat overview. The information given in this view includes the type of threat, the general threat group, the location within the system and a detailed description that can contain context as well as potential mitigation options to address the threat.

In Step 1-3, the user can review detailed information about the observed threat (Figure 6). 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.



State	First observed	Assigned to	Group	Where	Name
Severe	06/02/2019, 13:10		Network Threat	Area-51	DoS attack 2
Substantial	06/02/2019, 13:10		OS Threat	System2	Brute-force attack (4)
Substantial	06/02/2019, 13:10		Network Threat	System1	DoS attack 1
Low	13/05/2020, 12:36		Report	Internet	Social Media Report
Low	13/05/2020, 12:36		Report	Internet	Social Media Report
Low	13/05/2020, 12:36		Report	Internet	Social Media Report
Low	13/05/2020, 12:36		Report	Internet	Social Media Report
Low	13/05/2020, 12:36		Report	Internet	Social Media Report
Low	13/05/2020, 12:36		Report	Internet	Social Media Report

Figure 4: The CS-AWARE threat overview



DoS attack 2: sighting--28c5631d-696f-4b46-b7ae-e3b2731f331e

Type: Attack Pattern

Threat Group: Network Threat

Where: Area-51

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying open ports, but also give the adversary information concerning the firewall configuration.
Depending upon the method of scanning that is used, the process can be stealthy or more obtrusive, the latter being more easily detectable due to the volume of packets involved, anomalous packet traits, or system logging.
Typical port scanning activity involves sending probes to a range of ports and observing the responses.
There are four types of port status that this type of attack aims to identify:
1) Open Port: The port is open and a firewall does not block access to the port,
2) Closed Port: The port is closed (i.e. no service resides there) and a firewall does not block access to the port,
3) Filtered Port: A firewall or ACL rule is blocking access to the port in some manner, although the presence of a

State: Active

Comment:

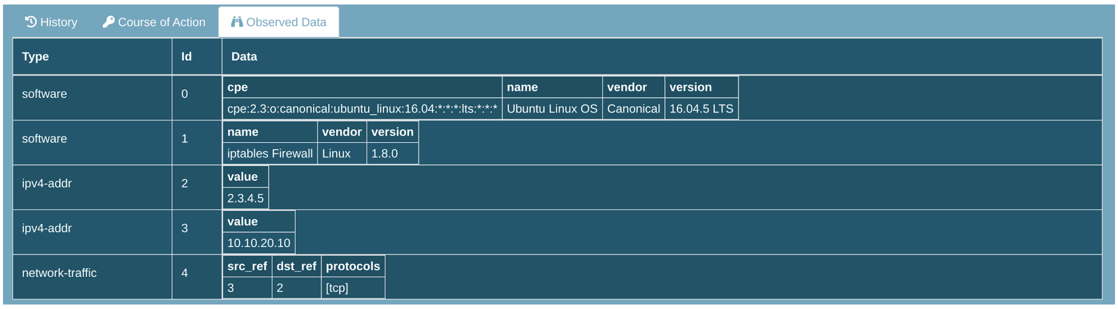
Initiator: admin@cs-aware.eu

Assigned to:

Time	State	Who	Comment
12/02/2020, 15:46	Active	CS-Aware	initial

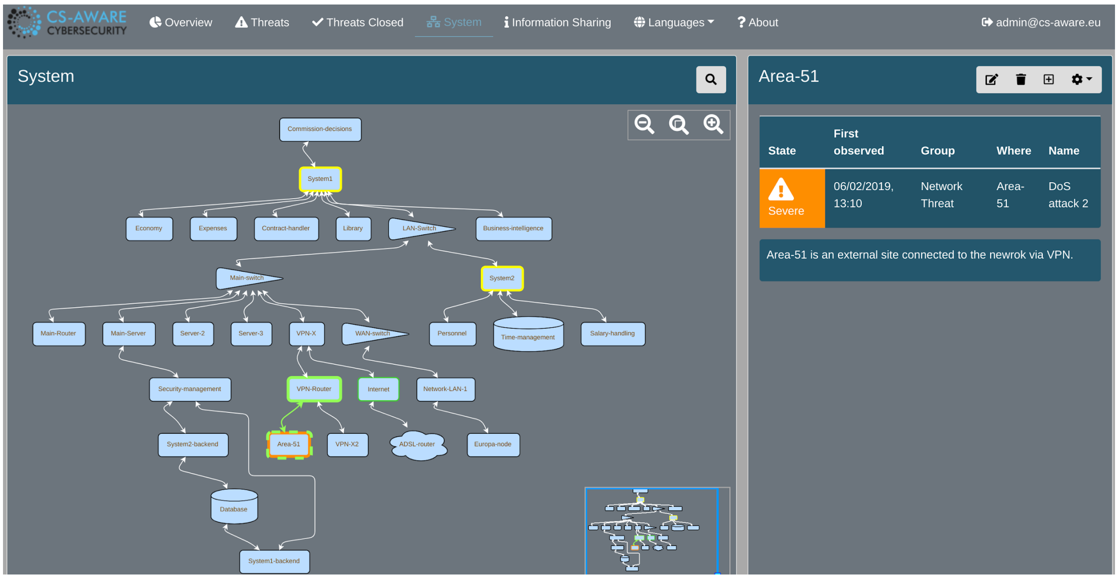
Figure 5: Review threat details

In Step 1-4, the user can review the system overview (Figure 7), the representation of organisational assets and dependencies created together with organisational stakeholders during socio-technical analysis. 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.



<table>
<tr><th>Type</th><th>Id</th><th>Data</th></tr>
<tr><td>software</td><td>0</td><td><table><tr><th>cpe</th><th>name</th><th>vendor</th><th>version</th></tr><tr><td>cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*</td><td>Ubuntu Linux OS</td><td>Canonical</td><td>16.04.5 LTS</td></tr></table></td></tr>
<tr><td>software</td><td>1</td><td><table><tr><th>name</th><th>vendor</th><th>version</th></tr><tr><td>iptables Firewall</td><td>Linux</td><td>1.8.0</td></tr></table></td></tr>
<tr><td>ipv4-addr</td><td>2</td><td><table><tr><th>value</th></tr><tr><td>2.3.4.5</td></tr></table></td></tr>
<tr><td>ipv4-addr</td><td>3</td><td><table><tr><th>value</th></tr><tr><td>10.10.20.10</td></tr></table></td></tr>
<tr><td>network-traffic</td><td>4</td><td><table><tr><th>src_ref</th><th>dst_ref</th><th>protocols</th></tr><tr><td>3</td><td>2</td><td>[tcp]</td></tr></table></td></tr>
</table>

Figure 6: Review threat observed details



State	First observed	Group	Where	Name
Severe	06/02/2019, 13:10	Network Threat	Area-51	DoS attack 2

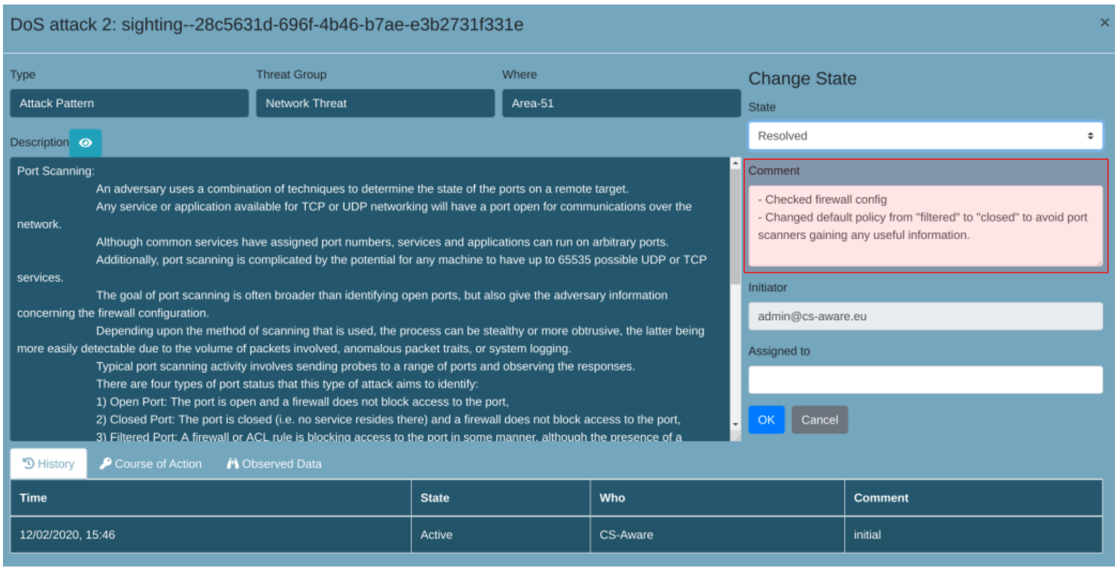
Area-51 is an external site connected to the newrok via VPN.

Figure 7: Review system overview

At this point, the user has reviewed all the awareness and context information provided by the CS-AWARE platform to help the user implement measures to mitigate the incident. If the user is not yet confident in their ability to resolve the issue using the information available to them, they can seek additional help and expertise outside the CS-AWARE platform, e.g., through the collaborative cybersecurity features provided by CS-CONNECT, as described in Section 5.2. After an incident has been handled or mitigated satisfactorily, CS-AWARE offers reporting functionality to add to the organisational knowledge in order to be able to handle similar incidents more efficiently in future.

In step 1-5, the user can comment on the state of the threat (Figure 8). For later reference, a comment about the course-of-action taken to resolve an issue outside the CS-AWARE environment can be given.

To conclude threat handling in step 1-6, a user can mark a threat "resolved" if the appropriate course of action could be taken, or "ignored" if the threat has been considered not relevant to



DoS attack 2: sighting--28c5631d-696f-4b46-b7ae-e3b2731f331e

Type: Attack Pattern

Threat Group: Network Threat

Where: Area-51

Description:

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying open ports, but also give the adversary information concerning the firewall configuration.
Depending upon the method of scanning that is used, the process can be stealthy or more obtrusive, the latter being more easily detectable due to the volume of packets involved, anomalous packet traits, or system logging.
Typical port scanning activity involves sending probes to a range of ports and observing the responses.
There are four types of port status that this type of attack aims to identify:
1) Open Port: The port is open and a firewall does not block access to the port,
2) Closed Port: The port is closed (i.e. no service resides there) and a firewall does not block access to the port,
3) Filtered Port: A firewall or ACL rule is blocking access to the port in some manner, although the presence of a

Change State

State: Resolved

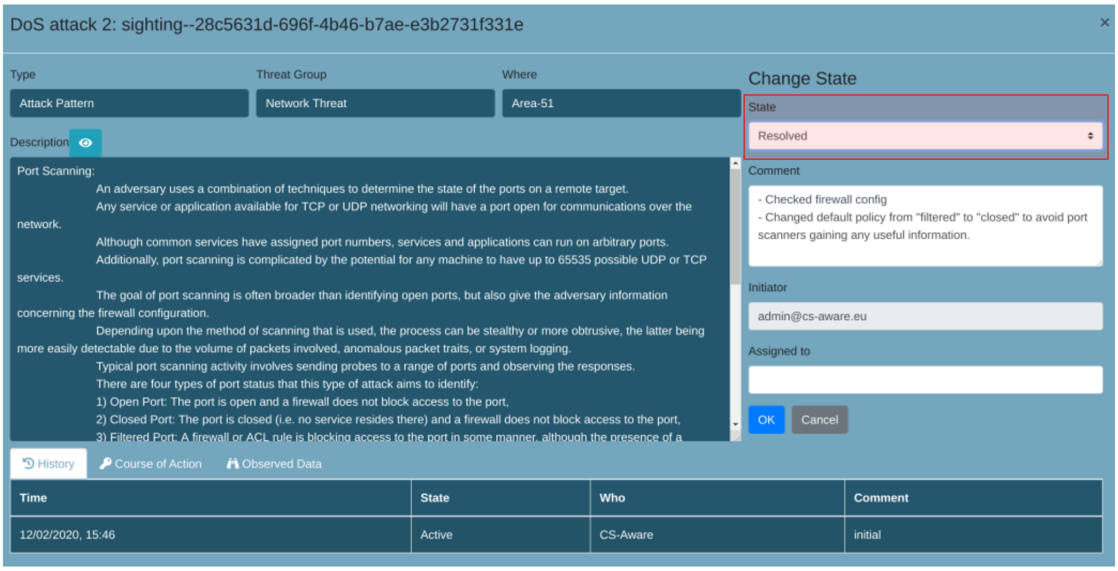
Comment:
- Checked firewall config
- Changed default policy from "filtered" to "closed" to avoid port scanners gaining any useful information.

Initiator: admin@cs-aware.eu

Assigned to:

Time	State	Who	Comment
12/02/2020, 15:46	Active	CS-Aware	initial

Figure 8: Comment on course-of-action in threat details view



DoS attack 2: sighting--28c5631d-696f-4b46-b7ae-e3b2731f331e

Type: Attack Pattern

Threat Group: Network Threat

Where: Area-51

Description:

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying open ports, but also give the adversary information concerning the firewall configuration.
Depending upon the method of scanning that is used, the process can be stealthy or more obtrusive, the latter being more easily detectable due to the volume of packets involved, anomalous packet traits, or system logging.
Typical port scanning activity involves sending probes to a range of ports and observing the responses.
There are four types of port status that this type of attack aims to identify:
1) Open Port: The port is open and a firewall does not block access to the port,
2) Closed Port: The port is closed (i.e. no service resides there) and a firewall does not block access to the port,
3) Filtered Port: A firewall or ACL rule is blocking access to the port in some manner, although the presence of a

Change State

State: Resolved

Comment:
- Checked firewall config
- Changed default policy from "filtered" to "closed" to avoid port scanners gaining any useful information.

Initiator: admin@cs-aware.eu

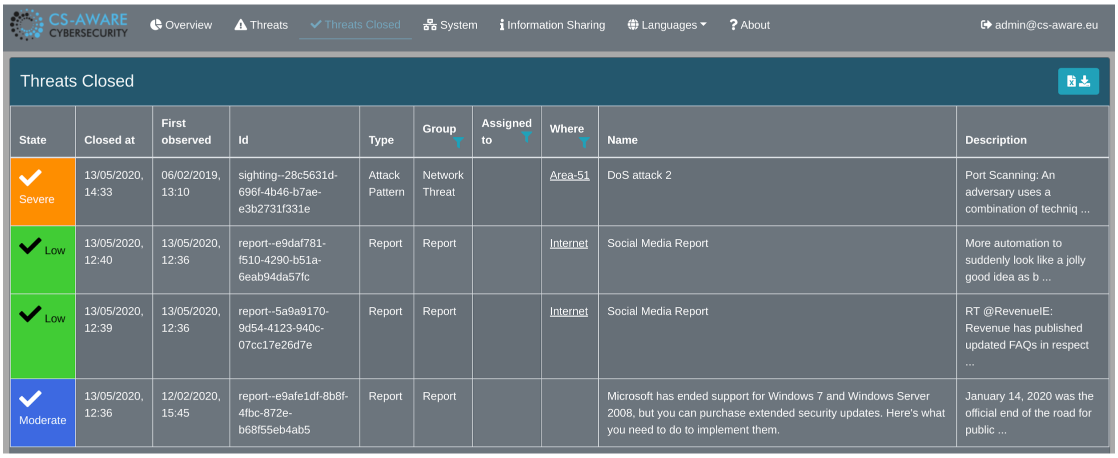
Assigned to:

Time	State	Who	Comment
12/02/2020, 15:46	Active	CS-Aware	initial

Figure 9: Mark threat state resolved/ignored in threat details view

the specific context (Figure 9).

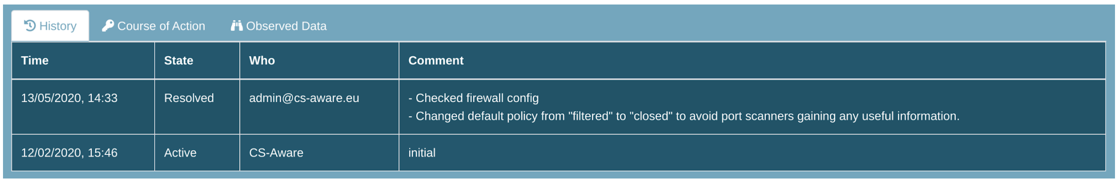
As optional steps 1-7 and 1-8, users can review closed threats and their incident handling details, as depicted in Figure 10 and Figure 11 respectively. An organisation's incident history is an important element of the organisational cybersecurity knowledge repository in order to be able to handle similar incidents more effectively in future, and it is also an important cybersecurity management indicator, allowing to reason about an organisation's cybersecurity



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 ...

Figure 10: Review resolved threats in "threats closed" view



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

Figure 11: Review threat history in threat details view

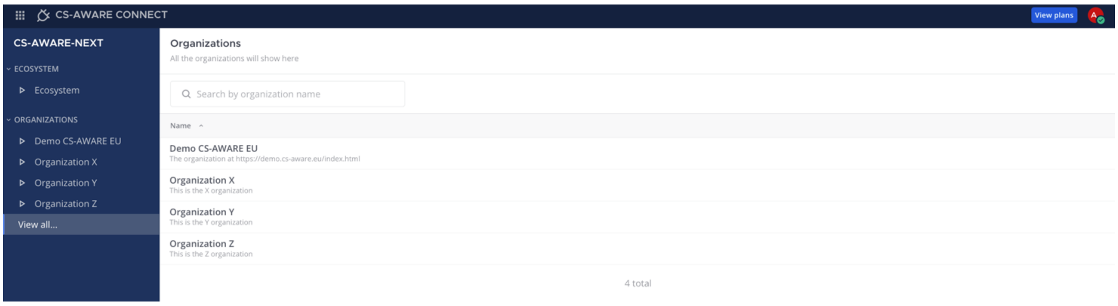
management performance.

5.2. CS-CONNECT

Collaboration is an important element in resolving cybersecurity issues. CS-CONNECT is designed to bring together stakeholders from ecosystems that belong together, e.g., by sharing the same goals, culture, or contextual knowledge to be able to help resolve cybersecurity issues efficiently and effectively within the community. To this end, CS-CONNECT follows a data-driven approach to collaboration, providing the ability to group context information about an incident (and relevant stakeholders from the community) together to discuss about incidents and find solutions that work in each specific context.

Following the same usage scenario as in the previous section, will show how CS-CONNECT can assist a CS-AWARE platform user to discuss an incident that was detected by the CS-AWARE platform, because the user was not able to resolve the incident on their own by just relying on the context information provided by the CS-AWARE platform. In this scenario, the user is able to provide all the relevant contextual information in CS-CONNECT and ask community users for assistance to resolve the issue. Please keep in mind that CS-CONNECT is currently still in active development, and this section describes an early maturity state of the tool.

The CS-CONNECT functionality is built on top of the Mattermost collaboration platform



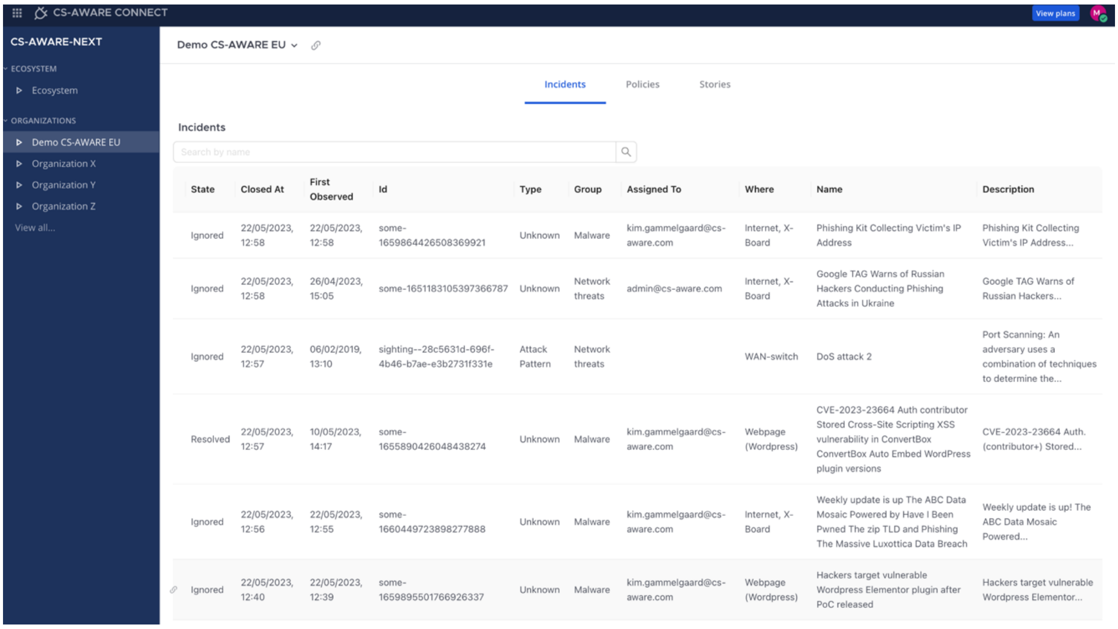
Organizations

All the organizations will show here

Name
Demo CS-AWARE EU The organization at https://demo.cs-aware.eu/index.html
Organization X This is the X organization
Organization Y This is the Y organization
Organization Z This is the Z organization

4 total

Figure 12: Organisations in the CS-CONNECT dashboard



Incidents

State	Closed At	First Observed	Id	Type	Group	Assigned To	Where	Name	Description
Ignored	22/05/2023, 12:58	22/05/2023, 12:58	some-1659864426508369921	Unknown	Malware	kim.gammelgaard@cs-aware.com	Internet, X-Board	Phishing Kit Collecting Victim's IP Address	Phishing Kit Collecting Victim's IP Address...
Ignored	22/05/2023, 12:58	26/04/2023, 15:05	some-1651183105397366787	Unknown	Network threats	admin@cs-aware.com	Internet, X-Board	Google TAG Warns of Russian Hackers Conducting Phishing Attacks in Ukraine	Google TAG Warns of Russian Hackers...
Ignored	22/05/2023, 12:57	06/02/2019, 13:10	sighting--28c5631d-696f-4b46-b7ae-e3b2731f331e	Attack Pattern	Network threats		WAN-switch	DoS attack 2	Port Scanning: An adversary uses a combination of techniques to determine the...
Resolved	22/05/2023, 12:57	10/05/2023, 14:17	some-1655890426048438274	Unknown	Malware	kim.gammelgaard@cs-aware.com	Webpage (Wordpress)	CVE-2023-23664 Auth contributor Stored Cross-Site Scripting XSS vulnerability in ConvertBox ConvertBox Auto Embed WordPress plugin versions	CVE-2023-23664 Auth. (contributor+) Stored...
Ignored	22/05/2023, 12:56	22/05/2023, 12:55	some-1660449723898277888	Unknown	Malware	kim.gammelgaard@cs-aware.com	Internet, X-Board	Weekly update is up The ABC Data Mosaic Powered by Have I Been Pwned The zip TLD and Phishing The Massive Luxottica Data Breach	Weekly update is up! The ABC Data Mosaic Powered...
Ignored	22/05/2023, 12:40	22/05/2023, 12:39	some-1659895501766926337	Unknown	Malware	kim.gammelgaard@cs-aware.com	Webpage (Wordpress)	Hackers target vulnerable Wordpress Elementor plugin after PoC released	Hackers target vulnerable Wordpress Elementor...

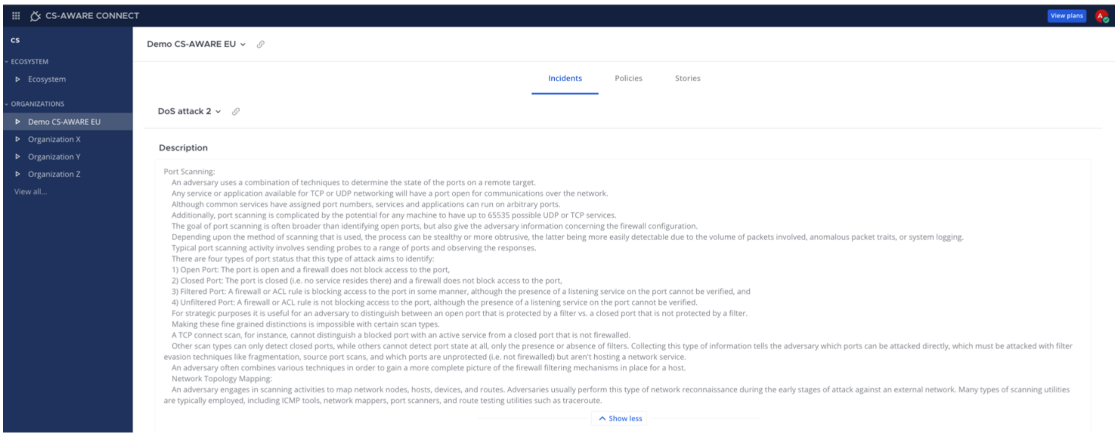
Figure 13: Incident overview in the CS-CONNECT dashboard

[1] and inherits all its collaboration and team management features. The CS-CONNECT functionalities to enable data-driven collaboration are implemented as plug-ins to Mattermost. In CS-CONNECT we have multiple organisations that are part of the ecosystem. To access them, the platform provides users with a dashboard where all the data of all organisations can be accessed (Figure 12).

By clicking on any of organisation, users can access the incident overview for an organisation (Figure 13) displaying data similarly to CS-AWARE threat overview in Figure 4.

The detailed view of each incident (Figure 14 and Figure 15) can be accessed by clicking on the corresponding row in the CS-CONNECT incident overview. This view provides information such as the incident description, a network representation of the organisation's system where

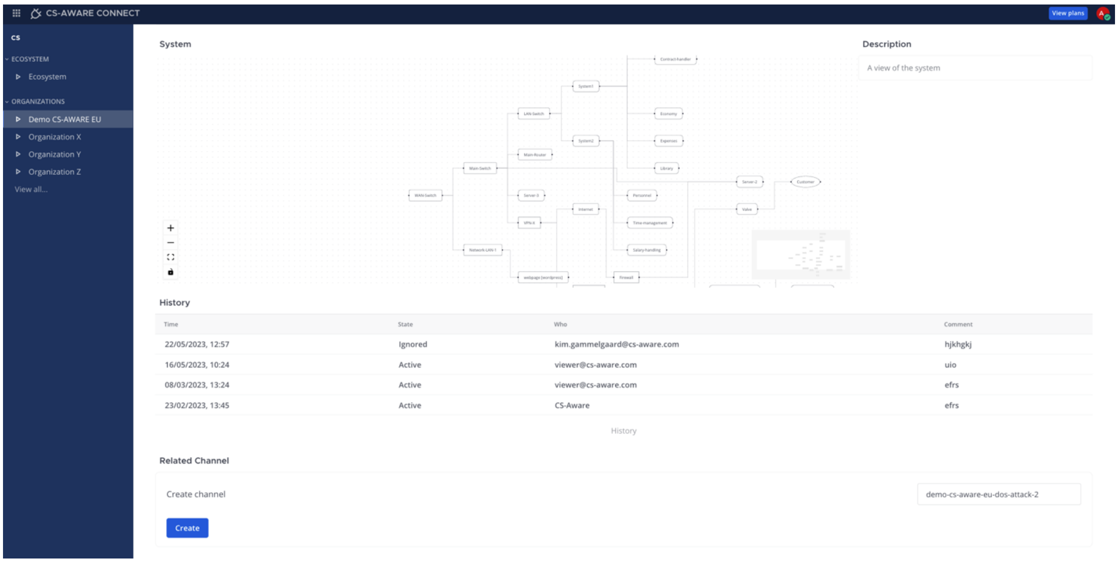
[1] https://github.com/mattermost/mattermost



Description

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying open ports, but also give the adversary information concerning the firewall configuration.
Depending upon the method of scanning that is used, the process can be stealthy or more obtrusive, the latter being more easily detectable due to the volume of packets involved, anomalous packet traits, or system logging.
Typical port scanning activity involves sending probes to a range of ports and observing the responses.
There are four types of port status that this type of attack aims to identify:
1) Open Port: The port is open and a firewall does not block access to the port,
2) Closed Port: The port is closed (i.e. no service resides there) and a firewall does not block access to the port,
3) Filtered Port: A firewall or ACL rule is blocking access to the port in some manner, although the presence of a listening service on the port cannot be verified, and
4) Unfiltered Port: A firewall or ACL rule is not blocking access to the port, although the presence of a listening service on the port cannot be verified.
For strategic purposes it is useful for an adversary to distinguish between an open port that is protected by a filter vs. a closed port that is not protected by a filter.
Making these fine grained distinctions is impossible with certain scan types.
A TCP connect scan, for instance, cannot distinguish a blocked port with an active service from a closed port that is not firewalled.
Other scan types can only detect closed ports, while others cannot detect port state at all, only the presence or absence of filters. Collecting this type of information tells the adversary which ports can be attacked directly, which must be attacked with filter evasion techniques like fragmentation, source port scans, and which ports are unprotected (i.e. not firewalled) but aren't hosting a network service.
An adversary often combines various techniques in order to gain a more complete picture of the firewall filtering mechanisms in place for a host.
Network Topology Mapping:
An adversary engages in scanning activities to map network nodes, hosts, devices, and routes. Adversaries usually perform this type of network reconnaissance during the early stages of attack against an external network. Many types of scanning utilities are typically employed, including ICMP tools, network mappers, port scanners, and route testing utilities such as traceroute.

Figure 14: Incident's description in the incident overview in CS-CONNECT



Description

A view of the system

History

Time	State	Who	Comment
22/05/2023, 12:57	Ignored	kim.gammelgaard@cs-aware.com	hjkhgkj
16/05/2023, 10:24	Active	viewer@cs-aware.com	uio
08/03/2023, 13:24	Active	viewer@cs-aware.com	efrs
23/02/2023, 13:45	Active	CS-Aware	efrs

History

Related Channel

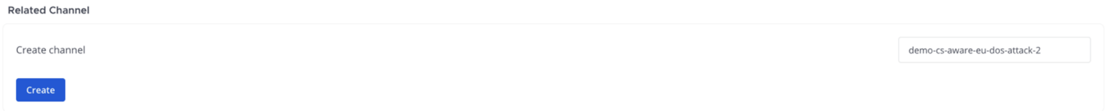
Create channel: demo-cs-aware-eu-dos-attack-2

Figure 15: Incident's system and history in the incident overview in CS-CONNECT

the incident occurred, and the incident history. In CS-CONNECT, each incident is associated with a network because the platform manages multiple organisations, unlike CS-AWARE which only manages a single organisation.

At the end of the detailed view, users have the option to either create a new channel to collaborate on the incident, (Figure 16) or access the existing channel dedicated to the incident (Figure 17). Clicking on either the create channel or existing channel option will redirect the user to the corresponding channel, where they can initiate collaboration with other users. This functionality enables seamless communication and collaboration around the incident among users within the platform.

When users access the channel, they will be presented with the Mattermost channel view,



Related Channel

Create channel

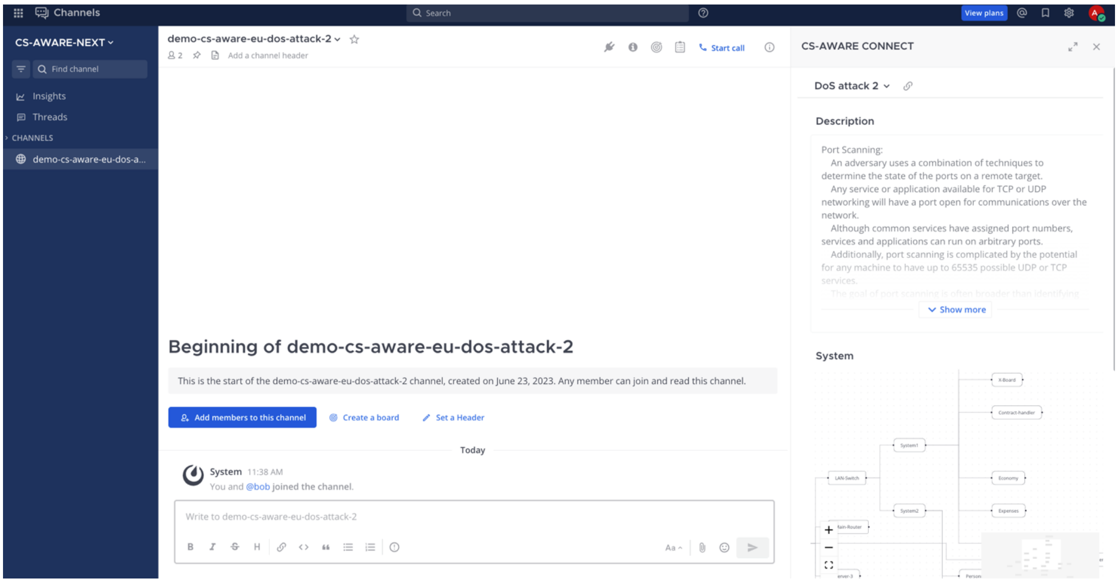
demo-cs-aware-eu-dos-attack-2

Figure 16: Incident's related channel creation in CS-CONNECT

Related Channel

demo-cs-aware-eu-dos-attack-2

Figure 17: Incident's related channel in CS-CONNECT



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

Today

System 11:38 AM
You and @bob joined the channel.

Write to demo-cs-aware-eu-dos-attack-2

Description

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying

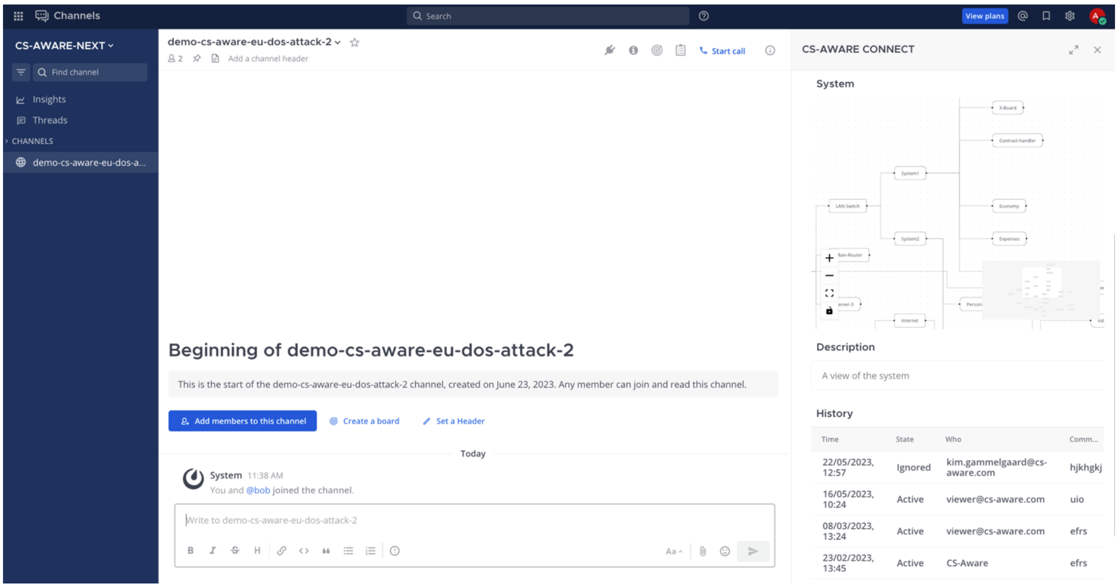
System

Figure 18: Incident's channel view and sidebar in CS-CONNECT

enhanced by the CS-CONNECT right-handed sidebar (Figure 18 and Figure 19). This sidebar includes all the information available in the incident detailed view, allowing users to easily access it during their discussions. The sidebar can be expanded by clicking on the expand icon (the first icon from the left in the top-right corner) or closed by clicking on the close icon (the second icon from the left in the top-right corner). If the sidebar is closed, it can be reopened by clicking on the CS-CONNECT icon, which is the first icon in the channel header.

Moreover, from this view, users can also return to the CS-CONNECT dashboard (Figure 20). They can do so by clicking on the icon in the top-left corner of the Mattermost channel view and selecting "CS-AWARE-CONNECT" to access the dashboard. This allows users to seamlessly navigate between the channel view and the CS-CONNECT dashboard for a comprehensive collaboration experience.

In the channel, users can actively engage in discussions regarding the incident (Figure 21). To illustrate the platform's collaborative capabilities, we will now present an example discussion



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

System 11:38 AM
You and @bob joined the channel.

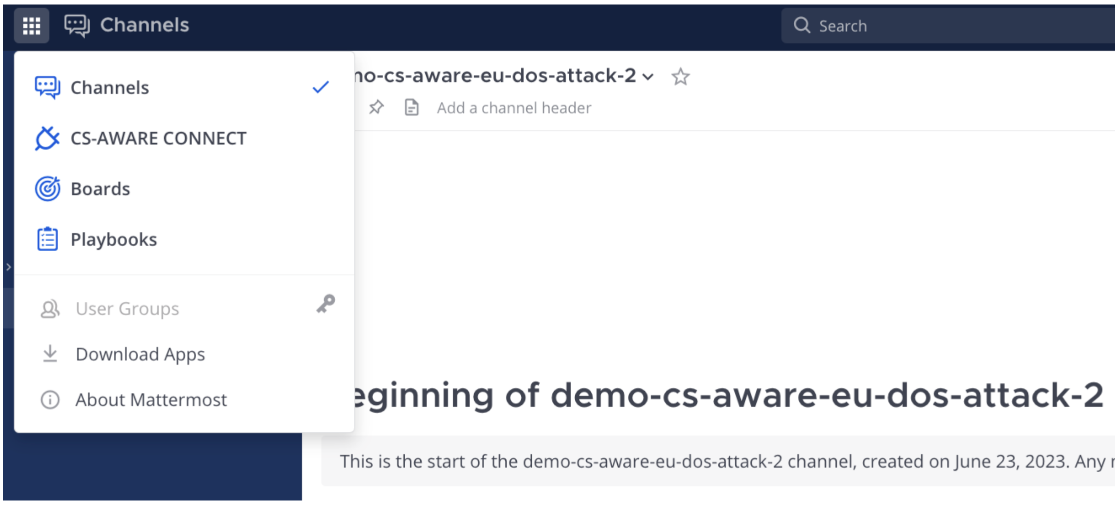
Description

A view of the system

History

Time	State	Who	Comm...
22/05/2023, 12:57	Ignored	kim.gammelgaard@cs-aware.com	hjkhgkj
16/05/2023, 10:24	Active	viewer@cs-aware.com	uio
08/03/2023, 13:24	Active	viewer@cs-aware.com	efrs
23/02/2023, 13:45	Active	CS-Aware	efrs

Figure 19: Incident’s channel view and sidebar in CS-CONNECT (2)



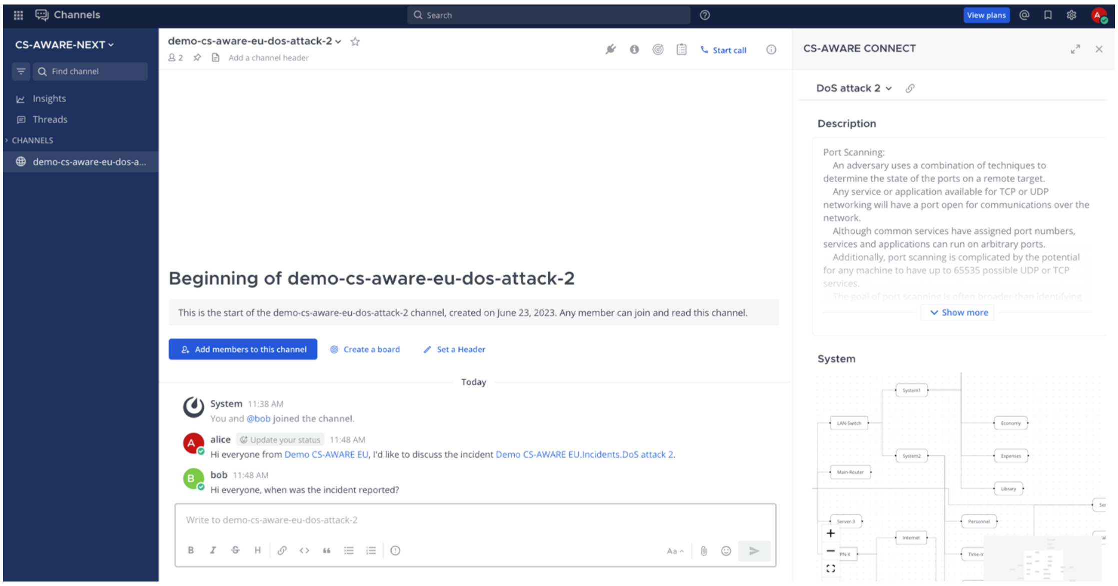
eginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any r

Figure 20: Access the CS-CONNECT dashboard from incident’s channel

between two users, Alice and Bob, regarding the DoS attack 2 incident in the DEMO-CS-AWARE-EU organisation. The purpose of this discussion is to showcase how the platform facilitates collaboration among users in addressing the incident.

The discussion begins with Alice initiating the conversation by requesting other users (in this case, only Bob) to discuss the DoS attack 2 incident in the DEMO-CS-AWARE-EU organisation. Notably, in Alice’s initial message, there are two hyperlinks: “Demo CS-AWARE EU” and “Demo CS-AWARE EU.Incidents.DoS attack 2.” A hyperlink is a unique reference to an information



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

System 11:38 AM
You and @bob joined the channel.

alice Update your status 11:48 AM
Hi everyone from Demo CS-AWARE EU, I'd like to discuss the incident Demo CS-AWARE EU.Incidents.DoS attack 2.

bob 11:48 AM
Hi everyone, when was the incident reported?

Description

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying

Figure 21: Users discussing the incident

in the platform. These hyperlinks are generated by Alice using the platform's hyperlinking mechanism, which allows users to easily locate and share data within the platform through a few clicks or by typing hyperlinks in the chat. The first hyperlink directs the user to the incident overview for the organisation, while the second hyperlink redirects the user to the incident's detailed view.

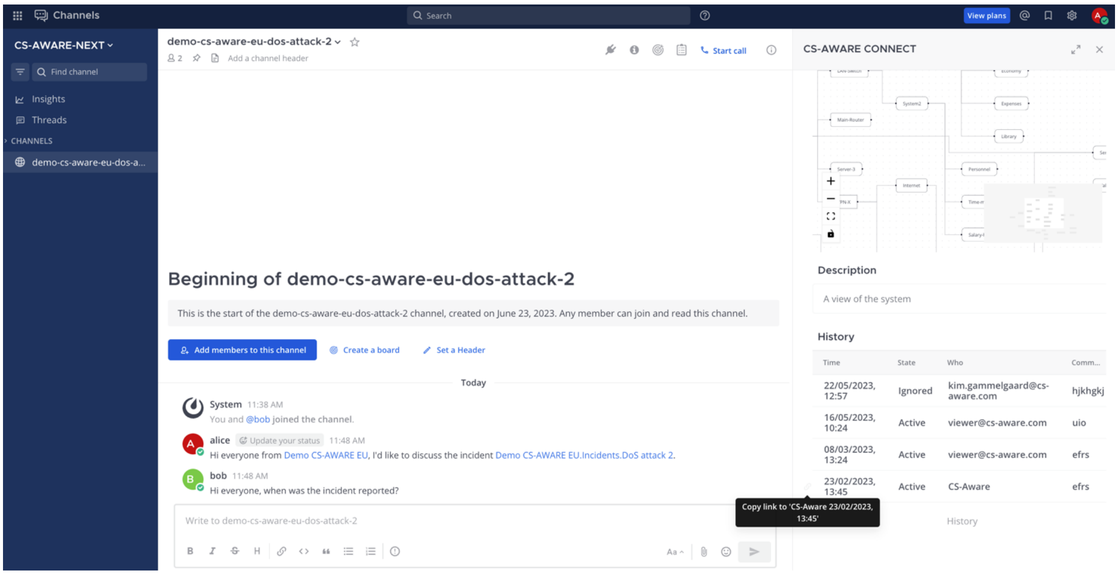
In response to Alice's message, Bob asks about the date when the incident was initially reported.

In response to Bob's question, Alice wants to provide the information that the incident was reported on 23/02/2023 at 13:45, as indicated in the history table. Alice aims to make this information easily accessible to Bob. To accomplish this, Alice utilizes a hyperlink to the specific row corresponding to the reporting date of the incident.

By hovering over the row in the history table, a dedicated icon (Figure 22) appears, allowing Alice to generate a hyperlink directly to that row. Once the hyperlink is generated, it is automatically copied to Alice's clipboard, enabling them to easily paste it into their message and share it in the chat (Figure 23). This ensures that Bob can quickly access the relevant information with a simple click on the hyperlink provided by Alice.

Once the message containing the hyperlink is sent in the chat, the platform renders the hyperlink in a human-readable format to ensure that the message remains easily readable for users. When a user, such as Alice, clicks on the hyperlink (Figure 24), the platform highlights the hyperlinked data, bringing it to the user's attention. This allows the user to quickly access the discussed data and easily comprehend the context of the conversation. By providing this functionality, the platform facilitates efficient information retrieval and enables users to respond within the relevant context of the discussion.

After receiving Alice's message, Bob examines the incident and starts to suspect that the



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

System 11:38 AM
You and @bob joined the channel.

alice Update your status 11:48 AM
Hi everyone from Demo CS-AWARE EU, I'd like to discuss the incident Demo CS-AWARE EU.Incidents.DoS attack 2.

bob 11:48 AM
Hi everyone, when was the incident reported?

Write to demo-cs-aware-eu-dos-attack-2

Description

A view of the system

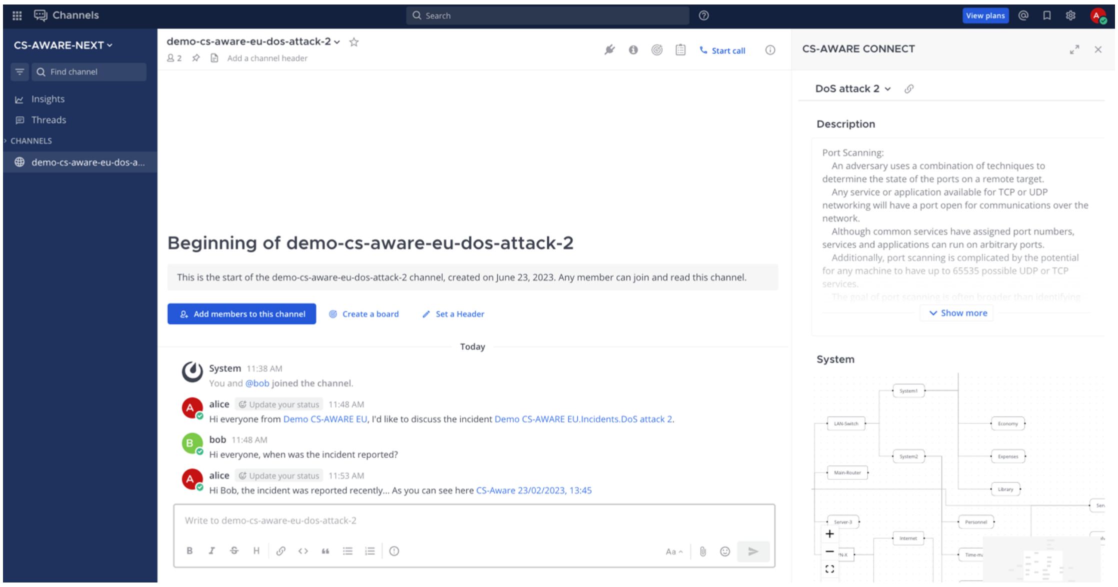
History

Time	State	Who	Comm...
22/05/2023, 12:57	Ignored	kim.gammelgaard@cs-aware.com	hjkhgkj
16/05/2023, 10:24	Active	viewer@cs-aware.com	uio
08/03/2023, 13:24	Active	viewer@cs-aware.com	efrs
23/02/2023, 13:45	Active	CS-Aware	efrs

Copy link to 'CS-Aware 23/02/2023, 13:45'

History

Figure 22: Generating a hyperlink via the user interface



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

System 11:38 AM
You and @bob joined the channel.

alice Update your status 11:48 AM
Hi everyone from Demo CS-AWARE EU, I'd like to discuss the incident Demo CS-AWARE EU.Incidents.DoS attack 2.

bob 11:48 AM
Hi everyone, when was the incident reported?

alice Update your status 11:53 AM
Hi Bob, the incident was reported recently... As you can see here CS-Aware 23/02/2023, 13:45

Write to demo-cs-aware-eu-dos-attack-2

DoS attack 2

Description

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying

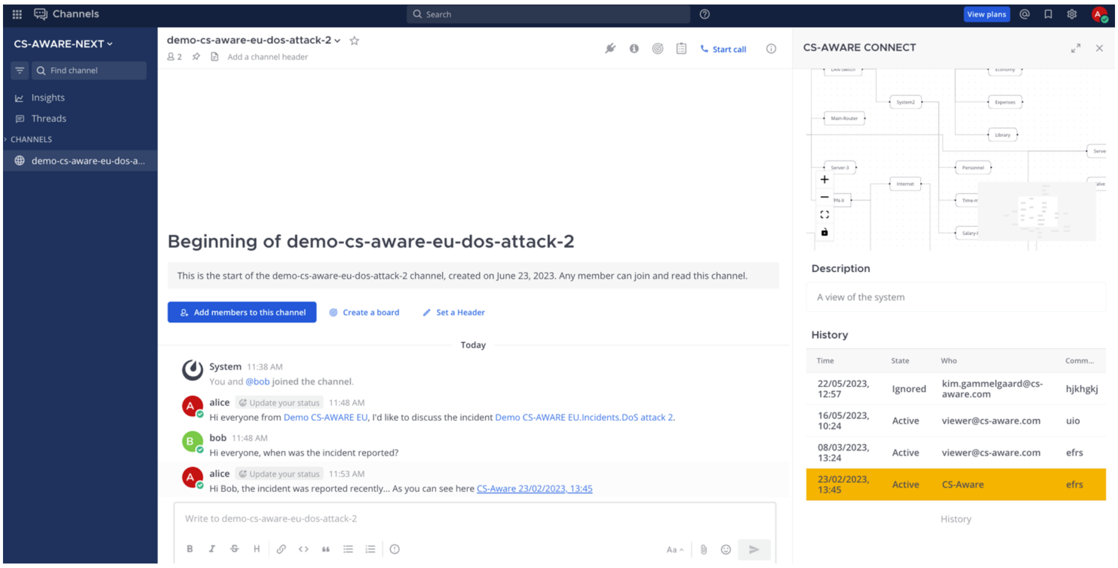
Show more

System

Figure 23: Hyperlink rendered as a human-readable message in chat

firewall component in the organisation's system is involved. Bob wants to share this opinion with Alice and decides to generate a hyperlink to the component in the incident's system for easy reference. Bob has two options for generating the hyperlink: clicking on the component in the system data view or typing the reference in the chat.

Bob chooses to type the reference in the chat. To generate a hyperlink through typing, Bob



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

System 11:38 AM
You and @bob joined the channel.

alice Update your status 11:48 AM
Hi everyone from Demo CS-AWARE EU, I'd like to discuss the incident Demo CS-AWARE EU.Incidents.DoS attack 2.

bob 11:48 AM
Hi everyone, when was the incident reported?

alice Update your status 11:53 AM
Hi Bob, the incident was reported recently... As you can see here CS-Aware 23/02/2023, 13:45

Description

A view of the system

History

Time	State	Who	Comm...
22/05/2023, 12:57	Ignored	kim.gammelgaard@cs-aware.com	hjkhgkj
16/05/2023, 10:24	Active	viewer@cs-aware.com	uio
08/03/2023, 13:24	Active	viewer@cs-aware.com	efrs
23/02/2023, 13:45	Active	CS-Aware	efrs

History

Figure 24: Hyperlink effect in channel view

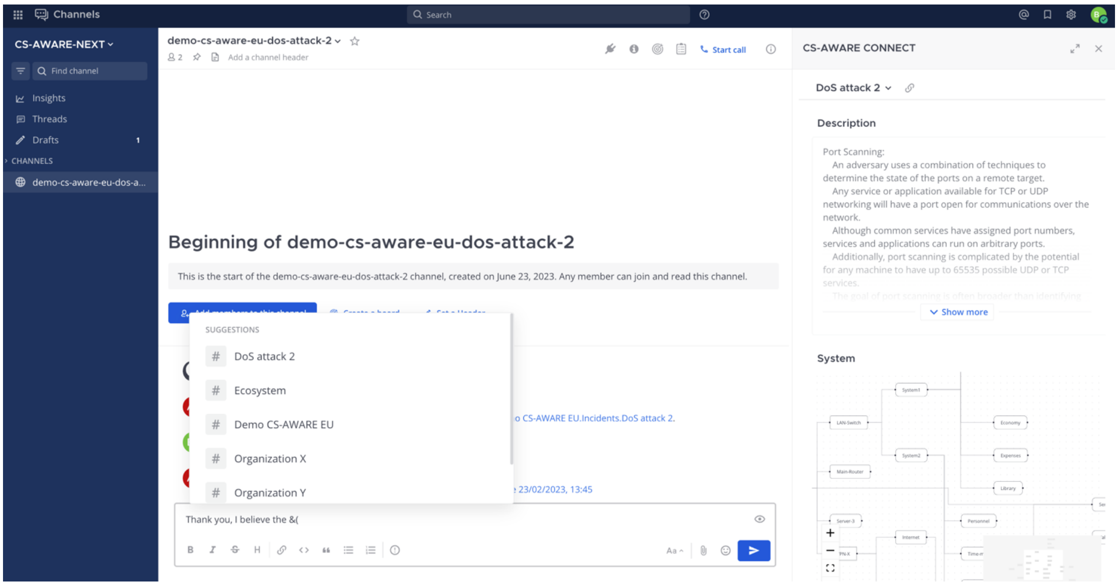
uses the “&” character, which indicates that a hyperlink should be generated using the reference provided within the parentheses. In this case, Bob wants to reference the firewall component in the incident’s system, so the reference is constructed as follows: the incident’s name followed by a dot, then the desired incident’s data (system), followed by a dot, and finally the desired information in the data (firewall). The resulting reference is &(DoS attack 2.System.Firewall). When the message is sent, this reference is converted into a hyperlink (Figure 27).

While typing the reference, the platform assists Bob by providing suggestions based on the context (Figure 25) and the content already typed (Figure 26). In Figure 25, Bob is provided with suggestions related to the discussed incident (DoS attack 2) and the organisations managed by CS-CONNECT. These suggestions serve as starting points for constructing the hyperlink, and for each piece of information, the platform provides further suggestions based on the available data. This functionality applies to any information within the platform, including organisations, incidents, and their respective data.

When Alice receives Bob’s message, they click on the hyperlink (Figure 28), and in the same way it happened for the history, the firewall component is highlighted in the system and brought to Alice’s attention.

6. Related Work

As mentioned in [8], “Information sharing between national stakeholders but even in cross country cases is one important aspect for cyber security. Knowledge on tackling cyber-attacks, incident response, mitigation measures, and preparatory controls can be shared between the relevant stakeholders”. The automation of the cybersecurity information exchange process in the context of incident and risk management for organisations is still in its infancy, and an



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

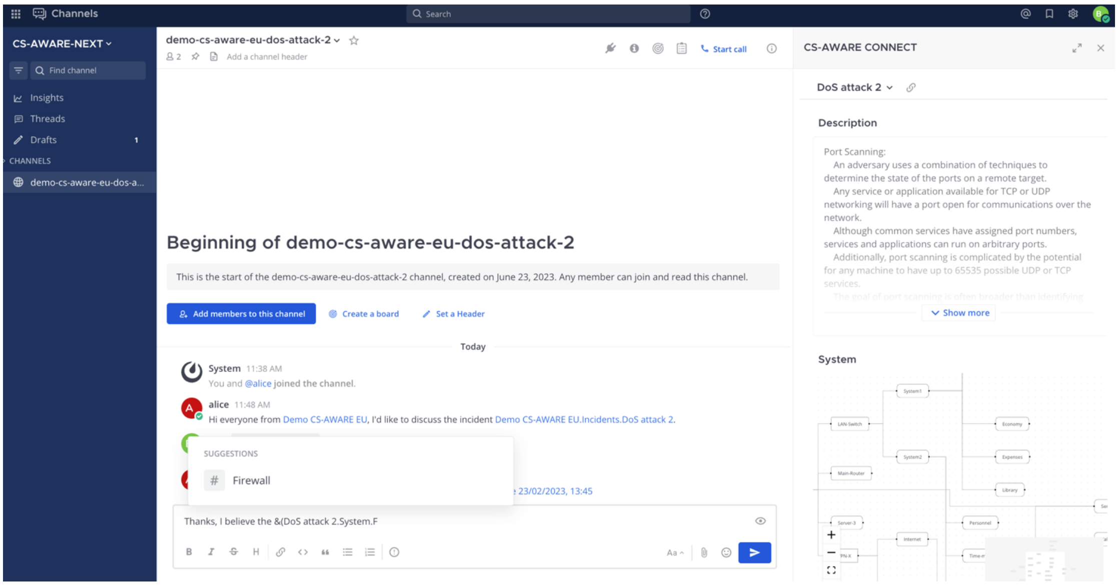
o CS-AWARE EU.Incidents.DoS attack 2.

23/02/2023, 13:45

Thank you, I believe the &(

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying

Figure 25: Suggestions when generating hyperlinks in chat



Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

System 11:38 AM
You and @alice joined the channel.

alice 11:48 AM
Hi everyone from Demo CS-AWARE EU, I'd like to discuss the incident Demo CS-AWARE EU.Incidents.DoS attack 2.

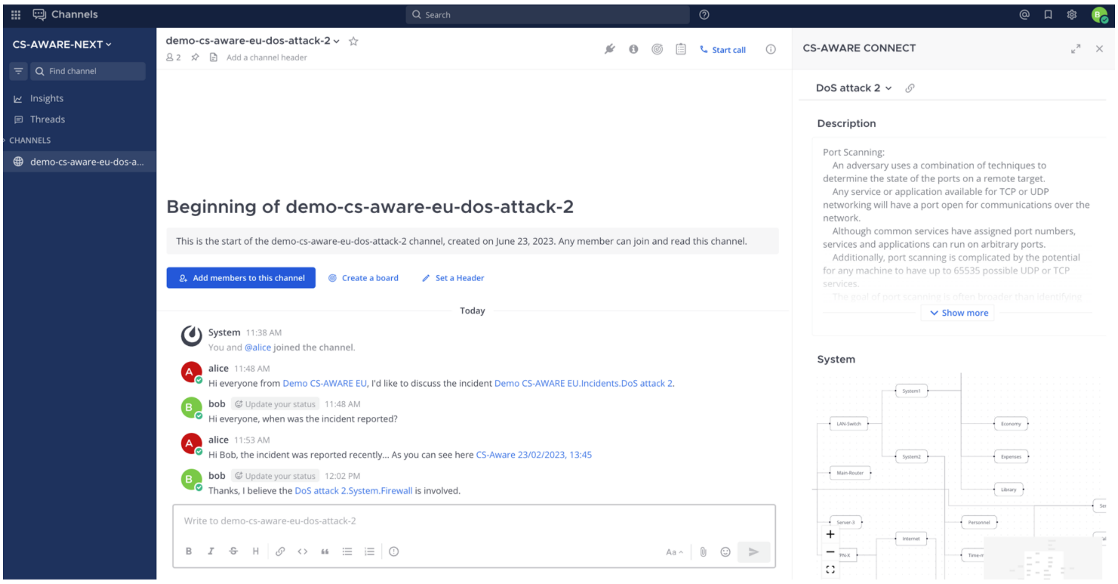
23/02/2023, 13:45

Thanks, I believe the &(DoS attack 2.System.F

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying

Figure 26: Suggestions based on user input when generating hyperlinks in chat

integration with modern and dynamic incident and risk management platforms like CS-AWARE has great potential for increasing the efficiency of information sharing through automation. In fact, collaboration and information sharing is already operational to some extent on the European and national levels (e.g., between competent authorities, CSIRTs). Still, when it comes to utilization of threat intelligence by individual organisations and local/regional networks in



demo-cs-aware-eu-dos-attack-2

Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

Today

System 11:38 AM
You and @alice joined the channel.

alice 11:48 AM
Hi everyone from Demo CS-AWARE EU, I'd like to discuss the incident Demo CS-AWARE EU.Incidents.DoS attack 2.

bob Update your status 11:48 AM
Hi everyone, when was the incident reported?

alice 11:53 AM
Hi Bob, the incident was reported recently... As you can see here CS-Aware 23/02/2023, 13:45

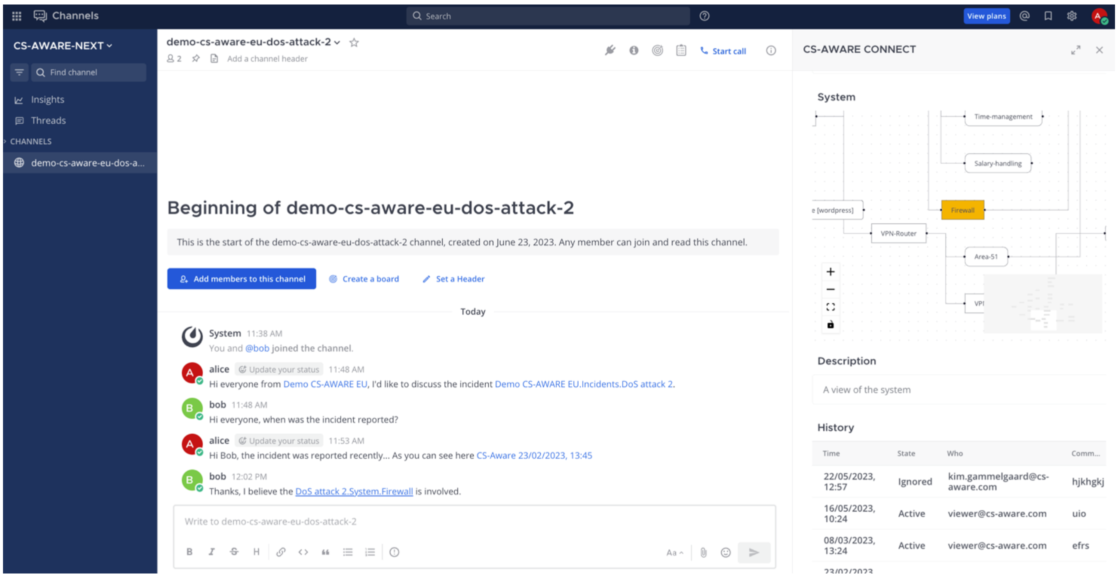
bob Update your status 12:02 PM
Thanks, I believe the DoS attack 2.System.Firewall is involved.

Description

Port Scanning:
An adversary uses a combination of techniques to determine the state of the ports on a remote target.
Any service or application available for TCP or UDP networking will have a port open for communications over the network.
Although common services have assigned port numbers, services and applications can run on arbitrary ports.
Additionally, port scanning is complicated by the potential for any machine to have up to 65535 possible UDP or TCP services.
The goal of port scanning is often broader than identifying

System

Figure 27: Hyperlink generated via chat



demo-cs-aware-eu-dos-attack-2

Beginning of demo-cs-aware-eu-dos-attack-2

This is the start of the demo-cs-aware-eu-dos-attack-2 channel, created on June 23, 2023. Any member can join and read this channel.

Today

System 11:38 AM
You and @bob joined the channel.

alice Update your status 11:48 AM
Hi everyone from Demo CS-AWARE EU, I'd like to discuss the incident Demo CS-AWARE EU.Incidents.DoS attack 2.

bob 11:48 AM
Hi everyone, when was the incident reported?

alice Update your status 11:53 AM
Hi Bob, the incident was reported recently... As you can see here CS-Aware 23/02/2023, 13:45

bob 12:02 PM
Thanks, I believe the DoS attack 2.System.Firewall is involved.

System

Description

A view of the system

History

Time	State	Who	Comm...
22/05/2023, 12:57	Ignored	kim.gammelgaard@cs-aware.com	hjkhgkj
16/05/2023, 10:24	Active	viewer@cs-aware.com	uio
08/03/2023, 13:24	Active	viewer@cs-aware.com	efrs
23/02/2023			

Figure 28: Effect of the hyperlink generated via chat

their day-to-day cybersecurity incident and risk management, there is currently little awareness and supporting procedures/tools available to streamline the process. The information sharing framework builds on the results of the CS-AWARE project [2], which integrates threat intelligence in a central way for dynamic cybersecurity management in organisations, and offers the technical

[2] https://cordis.europa.eu/project/id/740723

means to share cybersecurity information/evidence with relevant authorities in the multi-level cybersecurity environment. Other European projects investigated the issues related to information sharing and collaboration. For instance, H2020 ROUTE-TO-PA [3] aims to improve collaboration and transparency in the public sector. The SPOD platform was developed in this project as a collaborative and social place for discussion and problem resolution. Collaboration has been thoroughly discussed also in [9], which provides an elaborated analysis of what it means to collaborate, particularly in educational contexts. The cybersecurity context has been considered in [10]: the authors review the cybersecurity information-sharing literature, categorizing the identified papers based on their main focus and methodological approaches implemented to the cybersecurity information-sharing problem. [11] instead highlighted the importance of organisations relying on cyberspace as a mission-critical asset requiring advanced situational awareness to maintain a tactical advantage over emerging threats. In the paper, a new cyber–situational awareness framework relies on the OODA (observe, orient, decide, act) cycle to provide near real-time cognitive mapping for corporate environments. Several contributions can then be considered for data analysis. In the context of European projects, it is relevant to cite the CRIMSON project [4] that proposed an innovative AI framework to handle real-time image collection and analysis. Despite the context of the application being profoundly different, the variety and sensitive nature of the data remains. CS- AWARE-NEXT will use similar algorithms (Deep and transfer learning) and methods for data collection and processing. In the paper [12], the authors present a comprehensive view on "AI-driven Cybersecurity" that can play an important role for intelligent cybersecurity services and management. This paper highlighted that several works focused on deep learning have recently been studied in the field. For example, methods of detection of network attacks based on deep learning techniques are studied in [13][14][15]. The social media analysis will take instead inspiration from the results of the SSIX [5] project that provided a tool for analysing and understanding social media users' interest and sentiment for any given topic. To this end an advanced Big Data pipeline has been deployed to analyse millions of social media conversations using machine learning and NLP. CS-AWARE-NEXT will build on this experience by adopting social media listening and analysis components, including NLP techniques for multi-language text interpretation.

7. Conclusions and Future Work

Smart collaboration about cybersecurity data in our proposal requires intelligent selection of data, adapted to the goals of the collaborative scenario, as well as object oriented interfacing, allowing users an easy way to include and select particular data types during their online interaction. Collaboration about particular data, used as evidence or as resource for discussion, necessarily has to take place online, because of the opportunistic nature of data selection in such interaction.

One of the recommendations of a study conducted for the European Commission regarding 'Simulation, visualisation and visual computing technologies: EU position and future potential'

[3] https://cordis.europa.eu/project/id/645860
[4] https://cordis.europa.eu/project/id/101016923
[5] https://cordis.europa.eu/project/id/645425

concerned the development of what was named as 'next generation digital companions capable to provide assistance to users and to communicate with them in a natural way within mixed reality scenarios' [16]. What mainly we see as a part that we should concentrate our future research and development activities for the improvement of our platform are mainly related to the improvement of the user experience and bringing closer if not together HCI and AI aspects.

For example, moving from the concept of CS-AWARE as-a-platform to its constituent enabling technologies, one may see the need to promote the design of what one might call as a 'next generation of personal assistants'. In fact, and although personal assistants, virtual companions or avatars are certainly not a novelty within the human-computer interaction landscape, however, technologies developed so far were affected by severe usability restrictions, and at a great part because of limited language and / or poor semantic understanding capabilities. Nonetheless, over the last few years, language technologies have progressed to such an extent that the idea of being able to develop virtual companions capable to provide assistance to users and to communicate with them in a natural way, is now within reach not only by the research community but also by a large amount of general users in a variety of organisations. An example of advancement of language technologies is the very recent developments with the proliferation of ChatGPT and the deployment of large language models [17], something not possible only few years ago.

From the current research work perspective, the above has not been given priority in our agenda so far, as we aimed to build a fully operational system that could be adopted by public administrations which has been the initial target audience, and in particular local authorities, while later on we extended this to address also end-users from critical NIS sector such as health and water management, as well as SMEs. What we see as an important issue here is not only how realistic but also how trustworthy will be the behaviours of such companions or assistants within cybersecurity or other forms of emergency management scenarios.

Another important aspect for consideration in our future research agenda relates to the use and deployment of advanced data analytics platforms and infrastructures applying, amongst others, distributed learning and artificial intelligence approaches to query and aggregate efficiently, effectively, and securely data from multiple sources for multiple use cases. In our current planning, we have foreseen a core set of use cases related to organisational cybersecurity awareness, cybersecurity collaboration through information sharing and, what we preferred to call, system self-healing [18].

For each of these three core Use Cases we have identified aspects where our technology and business readiness levels need to improve, like for instance the visualisation components, so that these shall allow to visualize incidents in the particular organisational system and dependency set-up and provide mitigation options and cybersecurity management features to address each particular incident.

However, again, what we may have failed to identify and may now need to pursue as a priority, is the need to capitalise on new approaches towards better sharing and integration and use of cybersecurity-related real-world and research data to improved decisions. To this, there are two ways of sharing data: According to the first, data are 'handed out' in terms of pseudonymised or even if necessary, fully anonymised data from multiple sites (in our case this may be the customers' base of CS-AWARE) in order to allow for central analysis procedures to take place on the integrated dataset. This is also called 'bring-the-data-to-the-analysis' and was historically the way an analysis taking data from multiple locations into account has been performed. As sharing of retrospective data from organisations without informed consent is not allowed to take place, this ‘traditional’ data pulling method will not be utilised for analysing retrospective incident data. This is why infrastructures supporting a distributed analysis have been developed in recent years. Their goal is to keep the data within institutional borders, analyse these data partitions separately, and finally combine the individual results by either sequentially updating the final model with results from single institutions, or eventually merging the intermediate results. Such infrastructures follow the principle ‘bring-the-analysis-to-the-data’ leading to federated learning. This approach comes with privacy-by-design, since no individual data are shipped outside the particular organisations that own the data.

Acknowledgments

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101069543.

References

[1] A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis, A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis, Publication Office/CORDIS, European Commission, 2017. URL: https://cordis.europa.eu/project/id/740723.

[2] CS-AWARE, CS-AWARE, 2023. URL: https://cs-aware.com, [Online; accessed 23. Apr. 2023].

[3] European Commission, High Representative of the Union, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001, [Online; accessed 23. Apr. 2023].

[4] C. European Commission, Directorate-General for Communications Networks, Technology, The EU’s Cybersecurity Strategy for the Digital Decade, 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018&qid=1682286372218, [Online; accessed 23. Apr. 2023].

[5] Directive (EU) 2022/2555, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022L2555, [Online; accessed 23. Apr. 2023].

[6] Directive (EU) 2022/2557, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, 2022. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022L2557, [Online; accessed 23. Apr. 2023].

[7] V. Kupfersberger, T. Schaberreiter, C. Wills, G. Quirchmayr, J. Röning, Applying soft systems methodology to complex problem situations in critical infrastructures: The cs-

aware case study, International Journal on Advances in Security 11 (2018) 191–200. URL: http://eprints.cs.univie.ac.at/5904/.

[8] ENISA, Information Sharing and Analysis Center (ISACs) - Cooperative models, 2017. URL: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models, [Online; accessed 23. June. 2023].

[9] J. Andriessen, M. Baker, On Collaboration: Personal, Educational and Societal Arenas, Educational Research E-Books Online, Collection 2020, ISBN: 9789004407381, Brill | Sense, 2020. URL: https://books.google.it/books?id=VTBGzQEACAAJ.

[10] A. Pala, J. Zhuang, Information sharing in cybersecurity: A review, Decision Analysis 16 (2019) 172–196. URL: https://doi.org/10.1287/deca.2018.0387. doi:10.1287/deca.2018.0387.

[11] V. Lenders, A. Tanner, A. Blarer, Gaining an edge in cyberspace with advanced situational awareness, IEEE Security Privacy 13 (2015) 65–74. doi:10.1109/MSP.2015.30.

[12] I. Sarker, M. Furhad, R. Nowrozy, Ai-driven cybersecurity: An overview, security intelligence modeling and research directions, SN COMPUT. SCI. 2 (2021) 173. URL: https://doi.org/10.1007/s42979-021-00557-0. doi:10.1007/s42979-021-00557-0.

[13] Y. Wu, D. Wei, J. Feng, Network attacks detection methods based on deep learning techniques: a survey, Security and Communication Networks 2020 (2020) 1–17.

[14] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, Journal of Information Security and Applications 50 (2020) 102419.

[15] D. S. Berman, A. L. Buczak, J. S. Chavis, C. L. Corbett, A survey of deep learning methods for cyber security, Information 10 (2019) 122.

[16] E. Commission, D.-G. for the Information Society, Media, R. De Amicis, G. Conti, D. Taglioni, I. Facchin, VISION, VIsualization SImulation and visual cOmputing techNologies : EU position and future potential : executive summary, Publications Office of the European Union, 2013. doi:doi/10.2759/83607.

[17] Y. Liu, T. Han, S. Ma, J. Zhang, Y. Yang, J. Tian, H. He, A. Li, M. He, Z. Liu, Z. Wu, D. Zhu, X. Li, N. Qiang, D. Shen, T. Liu, B. Ge, Summary of chatgpt/gpt-4 research and perspective towards the future of large language models, 2023. arXiv:2304.01852.

[18] T. Schaberreiter, J. Roning, G. Quirchmayr, V. Kupfersberger, C. Wills, M. Bregonzio, A. Koumpis, J. E. Sales, L. Vasiliu, K. Gammelgaard, Alex, R. Papanikolaou, K. Rantos, A. Spyros, A Cybersecurity Situational Awareness and Information-sharing Solution for Local Public Administrations Based on Advanced Big Data Analysis: The CS-AWARE Project, River Publishers, Denmark, 2019.