Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services

Xiao-Si Wang*, Ian Herwono*, Francesco Di Cerbo†, Paul Kearney*‡, Mark Shackleton*
*Security Futures Practice, Research & Innovation, British Telecommunications plc, UK Email: {selina.wang, ian.herwono, mark.shackleton}@bt.com
†SAP Security Research, 805 av Dr Maurice Donat, 06254 Mougins, France Email: francesco.di.cerbo@sap.com
‡Cybersecurity Research Group, Birmingham City University, Birmingham, UK Email: Paul.Kearney@bcu.ac.uk

***Abstract*—Large enterprises and organizations from both private and public sectors typically outsource a platform solution, as part of the Managed Security Services (MSSs), from 3rd party providers (MSSPs) to monitor and analyze their data containing cyber security information. Sharing such data among these large entities is believed to improve their effectiveness and efficiency at tackling cybercrimes, via improved analytics and insights. However, MSS platform customers currently are not able or not willing to share data among themselves because of multiple reasons, including privacy and confidentiality concerns, even when they are using the same MSS platform. Therefore any proposed mechanism or technique to address such a challenge need to ensure that sharing is achieved in a secure and controlled way. In this paper, we propose a new architecture and use case driven designs to enable confidential, flexible and collaborative data sharing among such organizations using the same MSS platform. MSS platform is a complex environment where different stakeholders, including authorized MSSP personnel and customers' own users, have access to the same platform but with different types of rights and tasks. Hence we make every effort to improve the usability of the platform supporting sharing while keeping the existing rights and tasks intact. As an innovative and pioneering attempt to address the challenge of data sharing in the MSS platform, we hope to encourage further work to follow so that confidential and collaborative sharing eventually happens among MSS platform customers.**

Keywords—Cyber security, privacy, policy, information, data sharing, data anonymization, data sanitization, data encryption, managed security service, managed security service provider, large-scale enterprise, organization, architecture, design, component, diagram, use case, multi-tenant, cloud service

I. BACKGROUND

The enormous losses and damages due to malware attacks (e.g., WannaCry [1], NotPetya) and data breaches (e.g., Equifax Data Loss) in recent years have highlighted the importance of robust and agile cyber security. It was estimated by Detica/the UK Cabinet Office in 2011 that cybercrime costed the UK £27billion annually (about 1.8 per cent of GDP), of which £3billion came from citizens, £3billion from the government and a huge £21billion from companies [2]. The Norton report on cyber security for 2017 presents a shocking figure of £130billion cybercrime loss globally, of which £4.6billion was contributed by British internet users [3].

Sharing cyber threat information has been shown to increase the capacity of cybercrime prevention and detection. Two examples are the Flame and Conflicker malwares which were successfully tackled collaboratively by security and business enterprises [4].

However, several barriers exist that make sharing cyber security information difficult among organizations of different sizes and different functionalities. These organizations, including large-scale enterprises and small and medium sized enterprises (SMEs), are not able or not willing to share data with each other because of privacy and confidentiality concerns, contractual obligations, and legal requirements; and also because the available technologies might not be able to ensure proper access control mechanisms. Not sharing means reduced visibility and understanding of the situation and makes collaborative data analytics difficult, but how to protect confidentiality while enabling collaboration is a challenging research topic.

The project of Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP) [5], a European Commission Horizon 2020 research project, aims to address this challenge with innovative architectures and technologies. The project plans to provide a framework for secure and controlled information sharing that includes sanitization measures from anonymization up to homomorphic encryption; such framework also comprises specially crafted analytics for different cyber defense use cases. The C3ISP project considers a number of scenarios in which a common technological component or framework is applied in different scenarios. In this paper, we focus on the so-called 'Enterprise' scenario, which concerns how to enable confidential, collaborative and flexible data sharing among large-scale organizations and enterprises in both public and private sectors. This definition means that the term "Enterprise" in our paper does not include SMEs. Such large-scale entities typically outsource security services offered by 3rd party providers to defend and fight against cybercrimes. These

security services are typically referred to as Managed Security Services (MSSs) and the 3rd party providers are typically referred to as Managed Security Service Providers (MSSPs). One typical type of MSSs offered to customers is focused on monitoring and analyzing the customer's data which contain cyber threat information and in this paper we focus on such a MSS. In principle, the greater the volume and variety of data available for analysis and correlation, the higher the quality of information. Thus combining the analysis of data from multiple customers has advantages to both customers and MSSPs. In this paper, we describe a novel architecture and use case driven designs, aiming at providing a confidential and collaborative sharing capability within the Enterprise MSS environment.

Examples of such a MSS include BT Cyber Security [6], BT Security Threat Monitoring [7], SAP Enterprise Threat Detection [8], McAfee Enterprise Security Manager [9] and Alien Vault Unified Security [10]. MSSPs sometimes offer a Security Operations Centre (SOC) service to enterprises. SOC services can include a platform solution as the MSS for cyber threat monitoring and analytics for enterprises. The MSS platform is a centralized solution at the MSSP side, so it is a cloud service for the customers. Such a platform typically but not necessarily consists of a Data Lake, existing portals and tools. We consider the Data Lake as a distributed file system capable of storing huge amount of structured and unstructured data. The Data Lake which comprises data from individual customers, as well as instances of portals and tools are used by the cyber security analysts with contractual obligations at the MSSP side. In this paper, we refer to such a platform with these typical components as described above as a MSS Platform.

A typical MSS platform works in the following way. A large variety of security data sources are ingested into the platform, normalized to comply with the platform's common information model, enriched with contextualizing information and stored in the Data Lake. Data from the Data Lake are automatically/semi-automatically processed, monitored and analyzed using the Presentation & Analytics Tools (PAT) via a portal. PAT may write results back to the Data Lake, so the results data become available for further processing if required. The distinction between presentation tools and analytics tools is not hard and fast — for example, visual analytics tools combine aspects of both presentation and analytics. The results are made available to human decision-makers, who are either the MSSP personnel, referred to in this paper as Security Analyst(s) or Data Policy Officer(s) (DPOs), who are assigned to represent the interests of the customer(s) in question; or the customer personnel, referred to as Security Operation Executive(s) (SOEs). Security Analysts working on the front lines may be only using the PAT to perform investigation or analytics on behalf of customers; Security Analysts working on the non-front lines may also design and implement new features or data policies for the related platform components to meet requirements from customers. The SOEs can use PAT to monitor or analyze their own data sources, but are not allowed to write to the MSS platform components to change or add features. If SOEs have feature requirements (e.g. modifying the existing features or adding new features), the SOEs need to pass their requests to the platform Security Analysts via the customer support or account managers.

To allow collaborative and confidential data sharing using the MSS platform, a new architecture is needed and the design of the new architecture including the new components becomes a research challenge. The architecture requires novel approaches so that the current tasks can still be carried out without disruption, as well as allowing the MSS platform personnel to use the newly introduced components and functionalities for carrying out confidential and collaborative analytics.

Prior art and expertise are related to this project. As part of the same proposal call from EU Horizon 2020, another project, Proactive Risk Management through Improved Cyber Situational Awareness (PROTECTIVE) looks into how to improve cyber security incident and risk management using improved security monitoring and sharing for public domain computer security incident response teams and SMEs [11]. Coco Cloud was another EU project which aimed to allow cloud users to share data securely and privately in the cloud [12]. It was proposed that users of the cloud who are willing to share their data must consent to a Data Sharing Agreement (DSA), which requires uniform end-to-end enforcement [12]. We make use of the DSA developed by the Coco Cloud project, adapted for use within the C3ISP project.

In the following sections, we present the new system architecture of the MSS platform integrating the Collaborative and Confidential Sharing Component, referred as the C3ISP Component, and subsequently present the more detailed component designs driven by three different use cases. The C3ISP component is the important module which protects and desensitize the shared data and provides additional analytical functions the existing MSS platform does not have, but describing detailed sharing techniques and mechanisms used within the C3ISP Component is beyond the scope of this paper. The architecture and use cases we present here focus on how to connect an existing MSS platform with the C3ISP Component and how to use the MSS platform with the C3ISP Component enabled.

II. System Architecture

The system architecture incorporating the new C3ISP Component, is illustrated in Fig. 1 using the Fundamental Modeling Concepts (FMC) block diagram notation [13].

The MSS platform comprises components in three categories: the existing platform components (purple), the C3ISP Component including subcomponents (orange) and the new MSS platform software components (blue) which couple the existing platform components with the C3ISP Component.

The existing platform components are the PAT and the Data Lake storing data from different customers and have been introduced in Section I. The C3ISP Component consists of three main subcomponents: The Information Sharing Infrastructure (ISI) for data sanitization and protected storage,

the Information Analytics Infrastructure (IAI) for new and tailored analytical functions not provided by the existing MSS platform (e.g., performing operations on homomorphically encrypted data) and the Data Sharing Agreement Manager (DSAM) for defining policies for the IAI and ISI. DSAM is a powerful tool that transforms directives expressed in controlled natural language to machine-intelligible policies. A more detailed description of the C3ISP Component can be found here [14].

The new software components include the Portal, the Collaborative Task Manager (CTM) and the Data Manager (DM). CTM and DM act as "adapters" between existing components and the new C3ISP Component, in order to reconcile the expectations of existing components with the new analysis capabilities of the IAI or make use of the possibility to access sanitized data storage for shared data from participating customers. Detailed functionalities of the Portal, DM and CTM are introduced in the following subsections.

A. The Portal

The Portal is a front-end that will allow all the MSS platform users to call their respective functionalities and provide convenient links to the PAT, the CTM and the Data Sharing Agreement Manager (DSAM) within the C3ISP Component. As described earlier, the MSS platform already provides portals for users. However, the C3ISP Component being added to the platform means that new subcomponents will be added to the existing interfaces of the Portal or new interfaces of the Portal will be introduced. Hence the Portal is marked as a new component in the architecture design. The Portal will allow the Data Policy Officer (DPO) representing the customer on the MSSP side to write new data sharing policies into the DSAM or modify the existing sharing policies. It will also allow the MSS platform Security Analyst to enable or modify the configuration or task management functions provided by the CTM. From the customer side, the Portal will allow the SOEs to request the PAT but will not allow the SOEs to request CTM or the C3ISP Component; this is because the SOEs do not have the management rights on the MSS platform.

B. The Data Manager

The Data Manager (DM) mediates the interactions between the Information Sharing Infrastructure (ISI) of the C3ISP Component and other non-C3ISP components. The DM provides an Application Programming Interface (API) enabling it to match the PAT's standard data query and formatting requirements (e.g. allowing SQL (Structured Query Language) queries), also ensuring each PAT instance would operate with delegated authority. DM reads the data from the Data Lake and writes the data to ISI of the C3ISP Component or reads protected data from ISI.

The ISI is designed to protect the data (e.g. through encryption or sanitization) and to store the protected data, so it does not possess the full range of data management functionality required by the user. The IAI of the C3ISP Component, by design, requests protected data from the ISI,

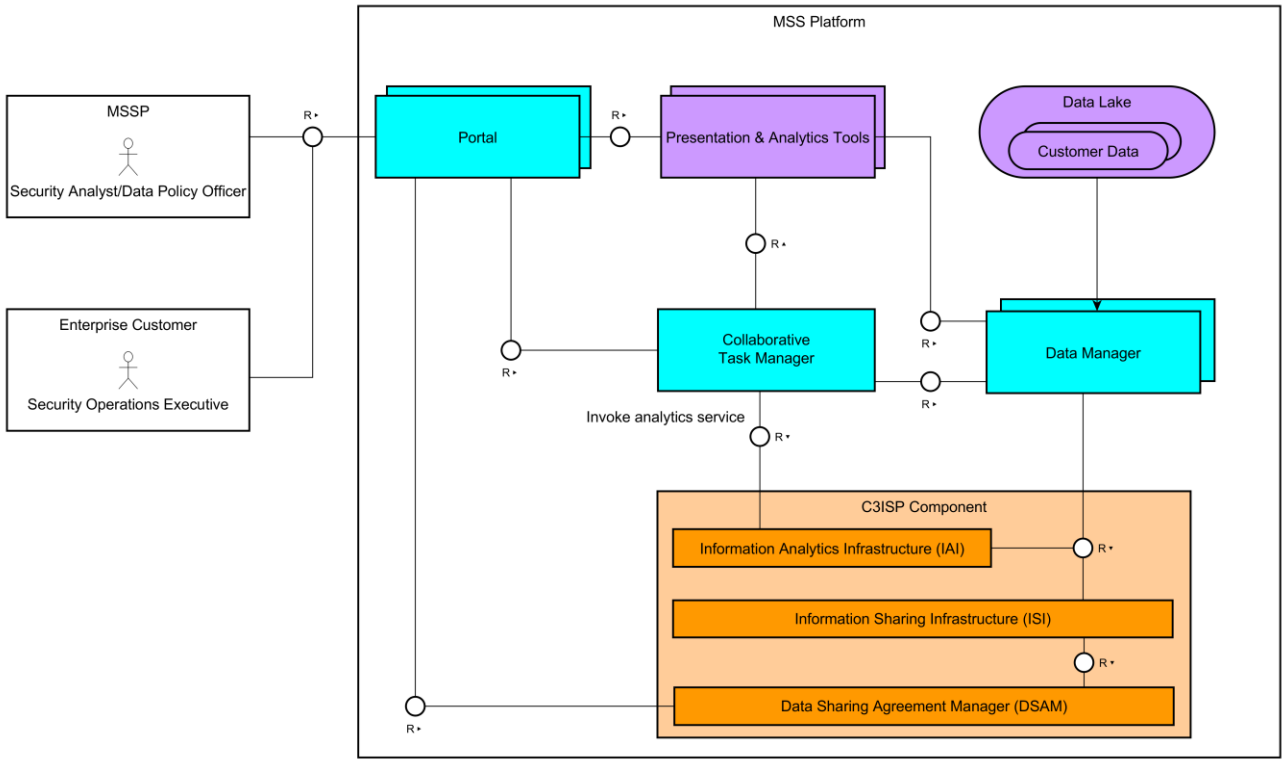

Fig. 1. System Architecture

performs analytics and returns the results to the ISI. In this case, if the user only wants to view or use the results generated previously, the user needs to request the results using PAT via the Portal and then the PAT at the back-end requests the DM to fetch the results from ISI to complete the operation.

The DM also mediates the Collaborative Task Manager (CTM) with the ISI. When the CTM receives a request to perform an analytical operation using the IAI, the CTM will request the DM to check whether the data required by the operation is available or request the data source IDs.

C. The Collaborative Task Manager

The Collaborative Task Manager (CTM) works as the controller of the IAI and the middleware between non-C3ISP components and the C3ISP Component. The CTM can receive requests from the Portal, including configuration requests or task management requests; it can request the DM to check if the data requested by the task are available and if not, then ask the DM to read the data in; it can automatically invoke the PAT to request the data after the protected data are stored in the ISI.

The CTM can work as an on-demand component. Here we give a real example to demonstrate the on-demand use of the CTM. If an enterprise requires all its shared data to be homomorphically encrypted using the C3ISP Component and then carry out algorithmic operations on the encrypted data, then the data request, the encryption request and the analytical request would be passed into the CTM through the Portal. The CTM subsequently requests DM to fetch the data. The DM then communicates with ISI to homomorphically encrypt and store the data; the CTM also requests the IAI to perform algorithmic operations on the encrypted data once the data are encrypted.

The CTM can also be programmed to perform automatic tasks without invocation. For example, if the task is to automatically display the data in the PAT every five minutes, the CTM would automatically control the data flow going through the C3ISP Component.

III. Component Designs Driven By Use Cases

In this section, detailed component architectures are described for three typical use cases of using the C3ISP Component within the Enterprise MSS platform. For clarity and simplicity, the diagrams only show the required components determined by the operational processes which are defined by the use cases. Some of the MSS platform components were not shown in the System Architecture (Fig. 1) but are shown in this section because those components are needed for a use case process, although they are not part of the C3ISP Component enabled platform design.

A. Data policy control and storage

This use case concerns a DPO from the MSSP who wants to specify sanitization and/or normalization measures, access and usage control policies and other policies in order to lower the sensitivity of the data from the customer he/she is representing. In this case, he/she needs to feed the platform with DSA so that the data are sanitized and/or normalized. Before starting this process, the DPO who is part of the MSS platform administrative personnel, has already received the data sharing policy request from the customer's own data policy personnel via the customer support or account manager.

The DPO will use the browser to log into the portal and write the data sharing agreement into DSAM within the C3ISP Component (Fig. 2). The use case represents the first step of the collaborative and confidential security information sharing proposed by the C3ISP project. This use case works as a pre-existing step for the next two use cases.

B. Security Analyst gaining insights from the shared data and subsequently transforming the operational process

Compared to the first use case, this second use case considers a more complex scenario where a Security Analyst from the MSSP discovers new knowledge from the shared

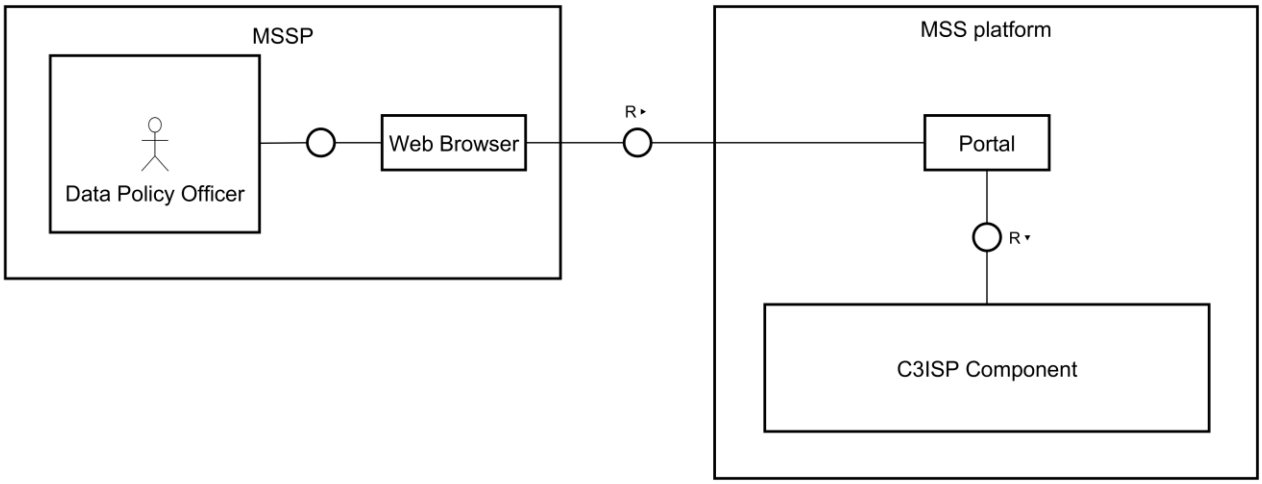

Fig. 2. Component design illustrating DPO enforcing the DSA

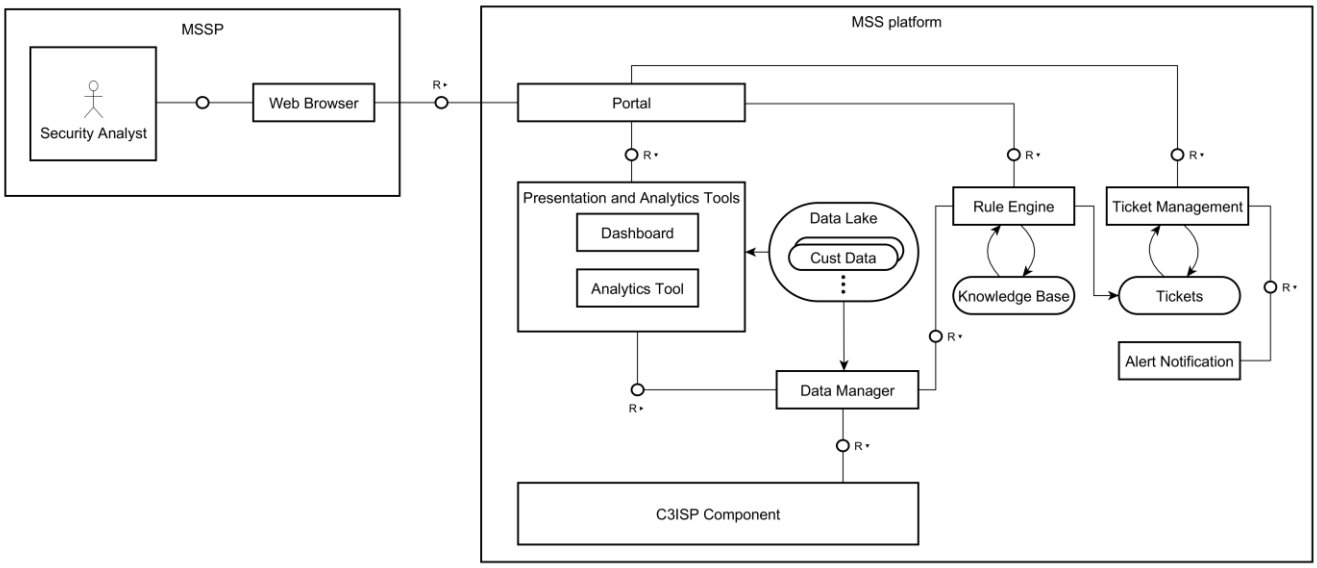

Fig. 3. Component design illustrating Security Analyst analyzing shared data and managing threat monitoring

data and subsequently transforms the threat operation. In this use case, the Security Analyst is responsible for managing multiple customers using the MSS platform with the C3ISP Component enabled. Now these customers have agreed to share their data using the C3ISP Component and the data have been protected and stored in the C3ISP subcomponents, as shown in the first use case, this particular use case does not require the analytics functions provided by the IAI of the C3ISP Component and therefore the CTM is not illustrated (Fig. 3).

The Security Analyst now starts a new process to investigate and identify actual and potential threats using the newly shared data and updates the operational process for one or more of these customers. Without the C3ISP Component, for individual customers, the analyst would use the MSS Dashboard (e.g., Kibana [15]) as part of the PAT to read the data from the Data Lake and to monitor various threat metrics (e.g., top 10 blocked source IPs) and would use the analytics tool within the PAT to further investigate threats and anomalous events. With the C3ISP Component enabled, the analyst is ready to use the shared data to monitor or further investigate active or potential threats.

The analyst uses a Web Browser to log in to the Portal and then uses the Portal to request the PAT. As described previously, the PAT will then request the DM to read the shared and protected data from the C3ISP Component. The C3ISP Component will ensure that the read operation complies with the corresponding DSA and the data are formatted correctly before passing to the DM. The analyst discovers some new knowledge from the shared data, e.g., gaining a global understanding from the shared data, noticing a commonly shared threat pattern among the sharing parties. The analyst then decides to use some of the new discoveries to transform the operational process. Compared to the system architecture, notice that the Rule Engine and the Ticket Management System are existing MSS platform components but were not previously presented as these existing components are not directly or indirectly related to the C3ISP Component embedding.

With the new insights, the analyst uses the Portal again to add a new rule into the Knowledge Base via the Rule Engine. The Knowledge Base stores the threat information or pattern which determines the operational rules (e.g. if more than a certain number of systems are reported with malware, it implies there is an important malware attack and needs to trigger an alert). The Rule Engine works as a controller of the Knowledge Base and connector of the ticketing and alerting components. The Rule Engine also needs to communicate with the DM to check if the (shared) data are relevant to any of the rules. The Rule Engine reads from and writes to the Knowledge Base and checks the data regularly through the DM to see if any rule is triggered. If a rule is indeed triggered, the Rule Engine then automatically creates a new ticket in the Tickets Database, and Ticket Management can also trigger an automatic alert with the new ticket being added via the Alert Notification system, e.g. automatic e-mail.

For new knowledge where an automatic process is not suitable, the analyst can also log into the Ticket Management system via the Portal to create a new ticket or modify an existing ticket and to alert the customer.

C. Security Operations Executive investigates the situation using the C3ISP shared data

This use case concerns a Security Operations Executive (SOE) from the customer side, who wants to use the Analytics Tool to investigate the shared data, in addition to analyzing his/her company's own data. In this use case, the investigation tasks also require usage of the analytical subcomponents of the

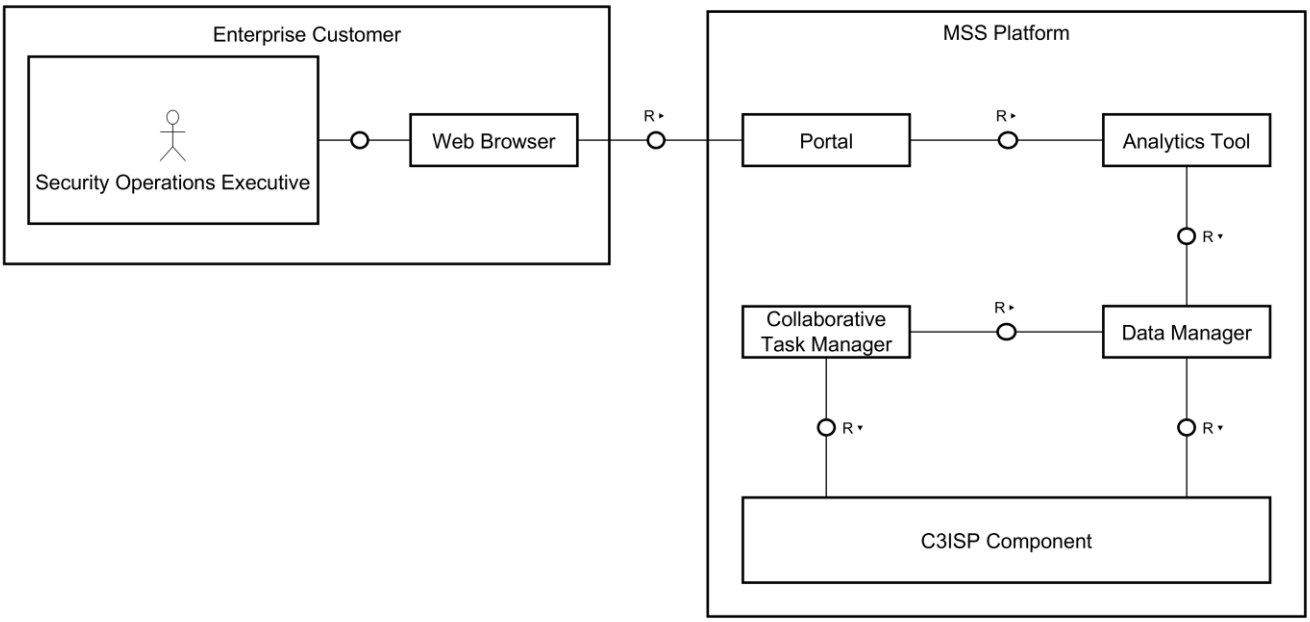

Fig. 4: Component design illustrating SOE analyzing shared data and gaining new threat knowledge

C3ISP Component (e.g., using the analytical components within IAI to use homomorphically encrypted data).

Here are the required operations before this particular use case can be applied. Before the SOE starts the new investigation, the DPO from the MSSP side has already attached the data sharing agreement to the data so that the data was protected and stored in the ISI and ready for use; the Security Analyst admin from the MSSP side has also configured the CTM so that the data can be analyzed using the C3ISP Component in an automatic process. As described before, the SOE does not control CTM, so CTM is not connected to the Portal. Figure 4 shows the FMC block diagram of this use case.

At the front end, the SOE uses a Web Browser to log in to the Portal and instructs the Analytics Tool to retrieves his/her company's own data and the shared data via the corresponding DM instance, which reads from the C3ISP Component regularly to ensure that the presented shared data is always up-to-date.

At the back-end, the CTM requests the IAI to perform the required functions on the shared and protected data from multiple enterprise customers (e.g. applies algorithmic operations on the homomorphically encrypted data) and stores the analytics results as the new protected and shared data in the ISI in an automatic manner. Any newly shared and protected data from ISI will be passed to IAI for analysis and the new data after analysis will be returned to the ISI automatically. The CTM may request specific information from DM about the customer data, e.g., requesting the IDs of different data sources.

IV. Discussion and Conclusion

This paper presents a new system architecture and detailed component designs required by different user processes for collaborative and confidential data sharing. This addresses the current gap in security information sharing within a MSS environment for large-scale enterprises and organizations.

As presented in the use cases, the possible scenarios and MSS environment are complex and therefore the way the different components are integrated also shows a certain level of complexity. The security analysts on the MSSP side and the SOE on the customer side, therefore need to develop new practices and process in order to make use of the shared data. Nevertheless, we have made every effort to simplify the complexity from an end-user experience perspective.

Another challenge in sharing data within the MSS platform environment is that the MSSP processes a large amount of data on a daily basis. How to make the best use of such data if shared would also need to be explored and experimented on.

This paper provides an innovative and concrete attempt to address the absence of architecture and designs allowing security data sharing on a MSS platform within the Enterprise environment. With an agile approach and strict privacy and confidentiality enforcement, we hope our research inspires more work in this area and makes collaborative and confidential data sharing achievable and manageable.

Acknowledgment

This work was funded by the EU H2020 project C3ISP [GA #700294]. The authors thank reviewers and Dr. Jonathan Tate for their valuable feedbacks on the manuscript. The views expressed in this paper are solely those of the authors

and do not necessarily represent the views of their employers, the C3ISP project, or the Commission of the European Union.

REFERENCES

[1] WannaCry ransomware attack. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack Last accessed: 20th February 2018.

[2] Detica (2011) The cost of cyber crime. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf Last accessed: 1st February 2018.

[3] 2017 Norton Cyber Security Insights Report. Available at: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-united-kingdom-en.pdf Last accessed: 12th February 2018.

[4] Fung, C.J., Boutaba, R., Design and Management of Collaborative Intrusion Detection Networks, 2013

[5] Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP). http://cordis.europa.eu/project/rcn/202687_en.html

[6] BT Cyber Security. https://www.globalservices.bt.com/uk/en/products/cyber-security

[7] BT Security Threat Monitoring. https://www.globalservices.bt.com/uk/en/products/security-threat-monitoring

[8] SAP Enterprise Threat Detection. https://www.sap.com/uk/products/enterprise-threat-detection.html

[9] McAfee Enterprise Security Manager. https://www.mcafee.com/us/products/enterprise-security-manager.aspx

[10] Alien Vault Unified Security. https://www.alienvault.com

[11] Proactive Risk Management through Improved Cyber Situational Awareness (PROTECTIVE). https://cordis.europa.eu/project/rcn/202674_en.html

[12] A. M. Garcia, R. S. Requena, A. Alberich-Bayarri, G. García-Martí, M. Egea and C. M. Martinez, "Coco-Cloud project: Confidential and compliant clouds," *IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*, Valencia, 2014, pp. 227-230.

[13] Fundamental Modeling Concepts (FMC) block diagram notation. http://www.fmc-modeling.org

[14] C3ISP Deliverables. http://c3isp.eu/download/deliverables-list

[15] Kibana. https://www.elastic.co/products/kibana