Retrieval of Relevant Historical Data Triage Operations in Security Operation Centers

Tao Lin[1], Chen Zhong[2], John Yen[1], and Peng Liu[1(✉)]

[1] Pennsylvania State University, University Park, PA 16802, USA
{lint,jyen,pliu}@psu.edu
[2] Indiana University Kokomo, Kokomo, IN 46904, USA
chzhong@iuk.edu

Abstract. Triage analysis is a fundamental stage in cyber operations in Security Operations Centers (SOCs). The massive data sources generate great demands on cyber security analysts' capability of information processing and analytical reasoning. Furthermore, most junior security analysts perform much less efficiently than senior analysts in deciding what data triage operations to perform. To help (junior) analysts perform better, several retrieval methods have been proposed to facilitate data triaging through retrieval of the relevant historical data triage operations of senior security analysts. This paper conducts a review of the existing retrieval methods, including rule-based retrieval and context-based retrieval of data triage operations. It further discusses the new directions in solving the data triage operation retrieval problem.

Keywords: Cyber situational awareness · Data Triage
Retrieval systems

1 Introduction

There are colossal, complex, and undetermined threats in the cyber world. As cyber attacks are happening on a daily basis and could be launched against an enterprise network at any moment, more and more organizations have established Security Operations Center (SOCs) to coordinate the defenses against cyber attacks [4].

When a security incident happens, the top three questions a SOC seeks to answer are: What attack has happened? Why did it happen? What action should be done? While a variety of software tools (e.g., security information management system, host-based security systems) and hardware equipment (e.g., network intrusion detection systems) have been deployed in today's enterprise networks to detect and correlate security-related events, real-world SOCs still rely on security analysts (and watch officers) to make decisions on "What should I do?". Due to several critical limitations (e.g., high false positive rates) of the

P. Samarati et al. (Eds.): Jajodia Festschrift, LNCS 11170, pp. 227–243, 2018.
https://doi.org/10.1007/978-3-030-04834-1_12

deployed software tools and hardware equipment, autonomous intrusion response is not yet being adopted by SOCs.

From the perspective of "data to decisions," the intrusion response decisions made by a SOC can be viewed as the main output of a particular human-in-loop data triage system. Not surprisingly, how soon the right intrusion response decisions can be made heavily depends on the efficiency (i.e., avoid performing useless data triage operations) of the system's data triage operations. Since there are a large variety of "sensors" monitoring an enterprise network, the enterprise's SOC will gather a huge amount of heterogeneous data coming from different types of data sources. Accordingly, a critical challenge faced by the SOC is that the massive data sources generate great demands on security analysts' capability of information processing and analytical reasoning.

To address this critical challenge, SOCs have been putting in a lot of effort to recruit and train security analysts. However, it is widely observed that the amount of time and effort required to train a security analyst is overwhelming. It usually takes a newly hired security analyst several years to complete his or her training and become an experienced analyst. Moreover, during the long on-job training process, it is observed that most inexperienced (junior) security analysts perform much less efficiently than senior analysts in deciding what data triage operations to perform.

To address these training challenges, several retrieval methods have been proposed to facilitate the data triage of inexperienced security analysts through retrieval of the relevant past data triage operations of experienced (senior) analysts. These research works have shown that data triage operation retrieval could help an inexperienced security analyst a lot in reducing the number of useless triage operations during his or her data triage processes.

In this article, we first conduct a review of the existing retrieval methods, including experience-based retrieval and context-driven retrieval of data triage operations. We then discuss the new directions (e.g., apply machine learning techniques) in solving the data triage operation retrieval problem.

The remainder of this paper is organized as follows. In Sect. 2, we present an overview of data triage in SOCs. In Sect. 3, we give an overview of data triage operation retrieval systems. In Sect. 4, we discuss the main challenges in developing effective triage operation retrieval systems. In Sect. 5, we conduct a review of two existing data triage operation retrieval methods, namely, experience-based retrieval and context-driven retrieval of triage operations. In Sect. 6, we discuss some future directions in building better triage operation retrieval systems. We conclude the paper in Sect. 7.

2 Triage Analysis in SOCs

We define the triage analysis as a dynamic Cyber-Human System (CHS) evolving over time in this section. We mainly describe the details of the input data sources and the analysts' operations performed by analysts in the process of triage analysis and explain the challenges faced by the analysts. The definition

of triage analysis lays the base for understanding the work of developing the knowledge retrieval systems described in the following sections.

2.1 Data Triage for Cyber SA

Figure 1 demonstrates the human-in-the-loop process of the triage analysis in a SOC. The goal of the cyber security analysts is to detect the potential attack chains. Given the data sources collected by multiple sensors, an analyst conducts a series of data triage operations to rule out the false alerts or unrelated reports. Therefore, we define the data triage process as a dynamic Cyber-Human System (CHS), which includes the following components: (1) the attack chains, (2) the network monitoring data collected from multiple sources, (3) a collection of incident reports which concludes the analysts' findings, (4) a collection of domain knowledge and experience knowledge, (5) the data triage operations performed by the analysts for accomplishing data triage, and (6) the hypotheses generated by analysts based on the existing findings about the potential attack chains (i.e., the mental model of analysts) [10]. Next, we explain the data sources and analysts' data triage operations in details.

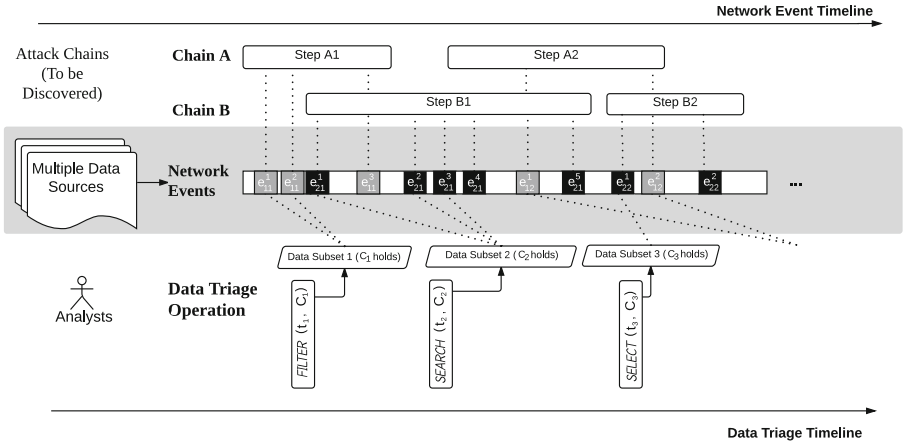

Fig. 1. Data triage operations conducted by analysts to identify and correlate the suspicious network connection events that indicate potential attack chains. [11]

2.2 Multi-Source Data in SOCs

SOCs usually deploy multiple cyber security defense technologies to protect an organization's network (such as intrusion detection systems (IDS) and firewall). The network connection activities are being monitored and controlled by these defense technologies over time. These network monitoring data collected from multiple sources usually have a high noise-to-signal ratio and are changing rapidly in the dynamic network environment. The common data sources include

the alerts generated from intrusion detection/prevention systems (IDS/IPS), firewall logs, server logs, network status reports, vulnerability scanning reports, anti-virus reports, traffic packages, and so on.

Going through the automatic data cleaning, aggregation, and correlation, the data sources will be further provided to the analysts to identify the key evidence of potential cyber attacks so that they can reason about the potential attack chains. Therefore, such multi-source data are the input of the data analysis process of human analysts.

The multi-source data collected from the cyber defense technologies can be represented by a collection of network connection events. These events can be further ordered according to their occurrence time. Therefore, the multi-source data can be represented as a sequence of network connection events, part of which are indicators of the ongoing attack activities and the remaining are the benign network activities, as it is shown in Fig. 1. Each **network connection event** can be defined by a vector that specifies the attributes of a network connection [10]:

$$e =< t, type, ip_s, port_s, ip_d, port_d, protocol, source, severity, conf, msg > \quad (1)$$

where t is the occurrence time of the event; $type$ is the type of network connection (e.g., built, teardown and deny); ip_s and $port_s$ are the IP address and port of the source, respectively; ip_d and $port_d$ are the IP address and port of the destination, respectively; $protocol$ is the network protocol; $source$ is the data source; $severity$ and $conf$ specify the level of severity and confidence of the event, respectively; msg specifies other important characteristics of the event, determined by the sensor [10].

2.3 Data Triage Operation

The data triage of the network monitoring data refers to the process where an analyst conducts a sequence of data triage operations to filter and correlate the suspicious network connection events. To accomplish a data triage task, an analyst needs to iteratively search and identify the suspicious events from the raw data, to interpret the suspicious events, and to generate hypotheses about potential attack chains based on the existing observation, and to search for supporting/denying evidence if a hypothesis needs to be further investigated [9]. There are in general three types of operations performed during data triage [11]:

- FILTER: filtering based on a condition.
- SELECT: identifying a subset of suspicious events.
- SEARCH: searching according to keywords.

As a result, the data triage analysts concludes his/her hypotheses about the possible attack chains with the evidence found in the raw data sources in the incident reports. Therefore, one main output of the triage analysis is the updates of the collection of incident reports.

3 Data Triage Operation Retrieval Systems

3.1 Difficulties in Data Triage Tasks

The primary challenge faced by most SOCs is the gap between increasing data collected by cyber defense technologies and the limited resources of expert analysts. Security analysts face several major difficulties in conducting their data triage tasks. First of all, the raw data from multiple sources has a large volume and very high noise-to-signal ratio. It has been impossible for analysts to go through all of them in details. Besides, considering the time pressure, analysts need to be highly concentrated on the task. Analysts need to decide whether or not a cyber event is suspicious or benign in minutes. Even worse, more and more cyber attacks have multiple steps to achieve their ultimate goal, which make detection harder. Last but not the least, the training of analysts always requires long-time on-the-job training. It is usually found that experts may not be able to explain the practical knowledge and their strategies precisely, although they are able to accomplish the tasks.

3.2 Experts' Knowledge of Data Triage

Analysts' experience and domain knowledge play a critical role in accomplishing data triage tasks. There have been several cognitive task analysis (CTA) studies conducted to investigate the working procedure of triage analysis. D'Amico et al. studied the main data sources and workflow of triage analysis [2]. Erbacher et al. investigated analysts' tasks, concerns, and needs for data analysis [3]. It has shown that analysts are good at interpreting data, comprehending contexts, generating hypotheses and drawing conclusions through a complicated analytical reasoning process [8,9]. Therefore, it is desirable to elicit experts' knowledge from their past data triage operations.

3.3 A Framework for Data Triage Knowledge Retrieval System Designs

A framework for data triage knowledge retrieval system designs is shown in Fig. 2. The system maintains a triage operation trace collection which manages all the data triage operations performed by experts for solving previous data triage tasks. A novice analyst is working on the triage of the incoming data sources. The analyst can directly create a query based on his/her attention of interest. Otherwise, his/her operations can be tracked in order to automatically construct a query based on the current context. Given a query, the operation retrieval engine will search for relevant operation traces in the trace collection and rank the results according to the relevance. The relevance can be determined by the similarity of the contexts. The retrieval result will then be presented to the analyst as a next-step suggestion.

The benefits of a retrieval system can be two-fold. First of all, a junior analyst can learn what could be effective data triage operations to conduct in the

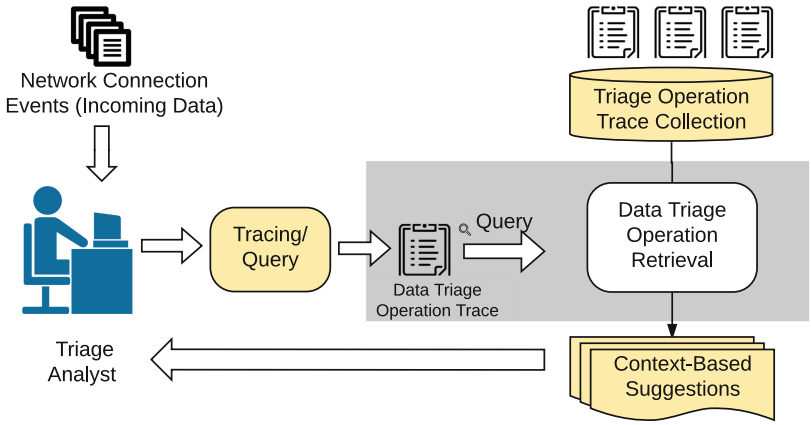

Fig. 2. The framework for the data triage knowledge retrieval systems. [10].

current context, if he/she is provided with the retrieved operations performed by other senior analysts in similar situations. Secondly, the junior analyst can learn how to interpret the suspicious network events and how to generate the valuable hypotheses for further investigation. Considering that most junior analysts are currently working under the supervision of senior analysts for guidance, a retrieval system can offer immediate and relevant suggestions in a more cost-efficient way. We have found little prior work specific to the information retrieval on data triage operations to assist analysts. However, we noted several areas of related work that are of interest in this work, which will be described in the next section.

4 Challenges in Developing Effective Data Triage Knowledge Retrieval Systems

The unique characteristics of how a SOC operates lead to several notable challenges in developing effective data triage operation retrieval systems. These challenges are as follows.

– The nature of data triage operation retrieval is Knowledge Retrieval, not Information Retrieval. Knowledge representation plays an essential role in triage operation retrieval, but not in standard information retrieval systems. Accordingly, the existing information retrieval techniques, including text retrieval and web (page) retrieval techniques, could not be directly applied to solve the data triage operation retrieval problem. The subject of the data triage operation retrieval is the practical knowledge gained by analysts from experience. Such tacit knowledge has been represented in an explicit format that a system can manage. A good representation of such knowledge needs to incorporate the key components in analysts' analytical reasoning processes.

Zhong et al. proposed a conceptual AOH model of an analyst's analytical reasoning process: (A) actions performed by the analyst to filter and correlate the provided data sources; (O) observations of suspicious network events gained by performing actions; (H) hypotheses of the potential attack chains generated based on the existing observations [9].

- The specific knowledge representation needed by data triage operation retrieval cannot be directly handled by existing knowledge retrieval systems. First, one unique characteristic of how a SOC operates is that there are a large variety of data sources (e.g., over 100 log files are collected from each host) are involved in data triage. Such amount of heterogeneity is usually not assumed in existing knowledge retrieval systems. For example, rule-based logic representations are generally used to represent knowledge, but the highly formalized structure makes this kind of representation limited to handle the aforementioned heterogeneity. Second, the data triage knowledge representation in a SOC has domain-specific characteristics which cannot be handled by generic knowledge retrieval systems.
- Data triage knowledge inherently covers a large amount of analytical reasoning conducted by security analysts, and the analytical reasoning in a SOC has domain-specific characteristics. Given that a common challenge of developing a knowledge retrieval system is to make the system domain-specific, data triage operation retrieval systems face the same challenge. This challenge will affect both knowledge representation and the retrieval algorithms. It is necessary to develop retrieval systems that can handle both the task operation information (i.e. actions and observations) and the analyst's mental processing (i.e., hypothesis).
- A new challenge which is faced by a SOC but is not addressed in other knowledge retrieval systems is that data triage operations are being retrieved in adversarial settings. That is, the attacker may purposely obfuscate their attack actions in such a way that the accuracy of triage operation retrieval could be significantly reduced. How to make the retrieval system resilient to such adversarial obfuscation is a new challenge. Since keyword-based retrieval is usually not really resilient, it is important to incorporate semantics in triage operation retrieval.

5 Current Research on Data Triage Knowledge Retrieval

In this section, we review two data triage knowledge retrieval systems that were constructed under the retrieval framework proposed in Sect. 3.3: a rule-based retrieval system and a context-based retrieval system. According to the challenges discussed in the previous section, we will mainly introduce the knowledge representation and matching algorithms of the knowledge retrieval systems.

5.1 Rule-Based Data Triage Retrieval System

Chen et al. developed a knowledge-based intrusion detection approach, which using Horn rules to illustrate experts' experience [1]. As shown in Fig. 3, a large

number of data filtered by intrusion detection systems. Coordination agents will determine the events with the potential relationship. Inference agents will decide the related events with specific rules. Most works focus on the layers rely on the results of data triage analysis. This work represented analysts' data triage knowledge of as logic rules and invented a rule relaxation approach to gain flexibility.

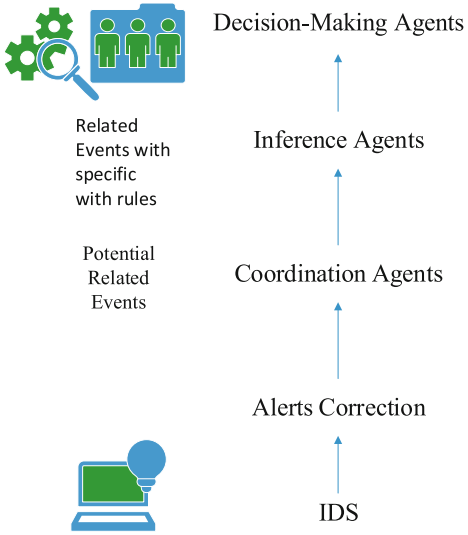

Fig. 3. Data analysis processes in SOCs.

Knowledge Representation. According to the retrieval framework (Sect. 2), analysts' data triage knowledge is managed in the triage Operation trace collection. Each knowledge piece is represented by logic rules. An **event-alert system** S is formalized as a 4-tuple (E, A, C, T), where E = E_1,...,E_m is a finite set consisting of Event Types, A = A_1,...,A_2 is a finite set consisting of Alert Types, C = C_1,...,C_o is the causality relationship hyper edges between Event Types. T = T_1,...,T_2 is links about Event Type to Alert Type. A partially observable event-alert system S is a system where all alert events are observable but may be hidden from the users. These hidden events can still be indirectly observed through context. Because alerts are observable, while events are unobservable, the runtime information is an alert sequence.

Given a partially observable event-alert system $S = (E, A, C, T)$, there is an alert sequence q = $< a_1,\ldots,a_n >$ being generated at run-time. Each instance of the alert $a_i = \ T_A, t_A, T_E, t_E \ $ contains these information:

– T_A: the alert instance's type;
– t_A: the time stamp of this alert becoming available;
– T_E: the type of the event;
– t_E: the time stamp of the hidden event occurs.

An Example of Rule-Based Representation. In this section, to help understand experiences in data triage operation retrieval, an example is provided to illustrate the core idea of hierarchical experience representation. An attack graph can be constructed to show its vulnerabilities and their dependencies. Figure 4 explains the important features from an attack graph. Firstly, the upper part of the graph is a list of alert types. These alert types are observable to analysts. In addition, each alert contains information about its triggering event. In this survey, we use dashed line to represent this relationship. The events are often hidden from the analysts. Lastly, several events are linked by their causal relationships. These causal relationships infer a typical temporal order of alerts.

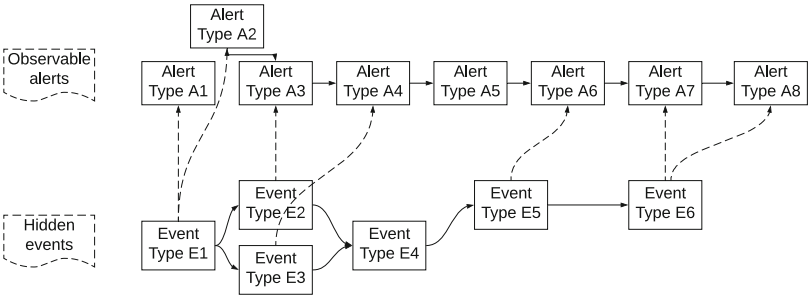

Fig. 4. The critical features in an attack graph

Knowledge Capturing. Before retrieving analyst's experience, it is necessary to capture experience to construct the knowledge base. Chen et al. identified the following important properties of cyber situation recognition:

– Events type;
– Events temporal relationships;
– Alert correlation information.

Based on them, Chen et al. use forward-changing rules stemming from Horn logic to illustrate experience patterns [1]. There are two patterns for each experience: event pattern and alert pattern. Hidden events are important clues for data triage operation retrieval. Event pattern captures the hidden events, and the temporal orders among the hidden events indicate the causal relationship. Alert pattern captures the observable alerts. They are the clues discovered by analysts.

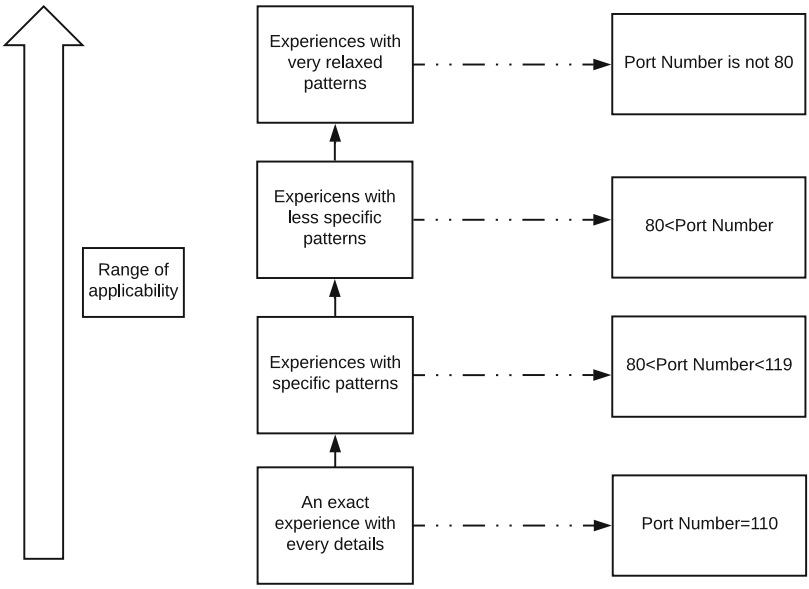

Fig. 5. Experience relaxation levels

Knowledge Matching and Rule Relaxation. Given the rule-based representation, a past incident can be described by a rule condition, which includes every specific detail at that moment, such as the time slot and the geographical location of the events. Therefore, an experience will not repeat itself with each same single details. As shown in the retrieval framework, the current context will be searched in the knowledge base. However, the rule matching requires every single detail of the rules to be matched, which may limit the usefulness of the retrieval results. To make the rule matching more flexible, Chen et al. proposed rule relaxation based on the Horn clause representation [1]. In regard to rule-based representation, researchers can relax the constraints by removing conditions from antecedents of that rule. The higher the degree to which an experience can be relaxed, the higher the possibility exists that it can be matched against a new situation. Figure 5 shows that the knowledge generated by relaxation form a hierarchy: the most specific knowledge at the bottom while the top is the most relaxed ones. Overall, upper-level experiences have better precision. While lower level experiences provide broader coverage. The entire experience hierarchy is formed through a consistent process, where each level of relaxation is defined with a specification guideline (i.e., how a higher-level experience should be relaxed into lower-level ones). All experiences on the same level will have a consistent specificity. According to Fig. 6, rule matching is performed on each piece of knowledge in the network. Rule relaxation enables a larger set of matching candidates. Meanwhile, it may influence the precision of the results.

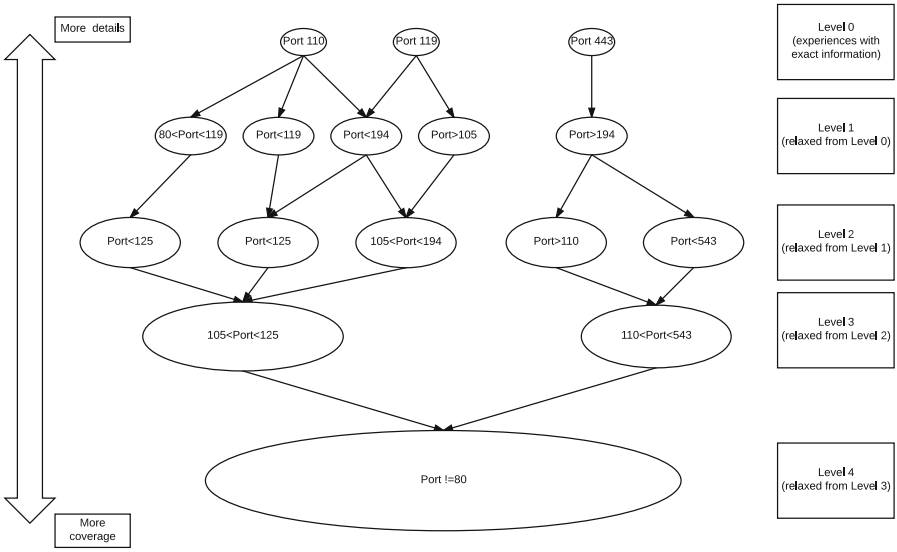

Fig. 6. Hierarchical experience networks

Case Study. The rule-based retrieval system has been implemented and evaluated in a case study. Figure 7 demonstrates the architecture of the system: the experience base is the collection of knowledge; the cyber security adapter takes in the network data (alerts); the recognizer performs the rule matching and rule relaxation by consulting the knowledge base and the rule system, and the matched results will be suggested to the user.

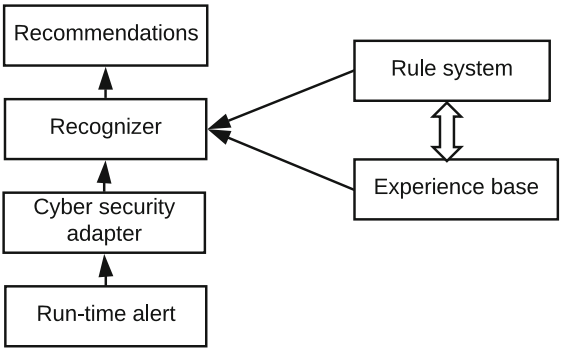

Fig. 7. The architecture of the rule-based knowledge retrieval system.

In the case study, Chen et al. evaluated the performance of the retrieval system by comparing the recommendations against the ground truth of a simulated

data set. It showed that the rule representation made knowledge capturing possible. Besides, the rule relaxation makes the retrieval system more flexible and the analysts can adjust the coverage or precision of the matching results based on their needs.

5.2 Context-Based Data Triage Knowledge Retrieval System

Zhong, et al. proposed a context-based data triage knowledge retrieval system that represents analysts' analytical reasoning processes in a tree structure [7]. Given the structure-based knowledge representation, the context of an analytical reasoning process was further defined so that the similarity between two contexts can be measured. The retrieval results were ranked according to the similarity between them with the current context.

Knowledge Representation. According to the conceptual AOH model, an analyst's analytical reasoning process in data triage contains three types of components: actions, observations, and hypotheses (Sect. 4): an action may trigger an observation; gaining an observation may let the analyst generate a hypothesis; the further investigation of the hypothesis requires further actions. Based on the conceptual model, Zhong et al. proposed a tree structure, named Experience Tree (E-Tree), to represent actions, observations, hypotheses, and their relationships [7].

The nodes of an E-Tree are the instances of actions, observations, and hypotheses, and the edges are the relationships between them. The root of an E-Tree is the initial action or observation in the analytical process. The context of a hypothesis is defined by the path in the E-Tree from the root to this hypothesis. Figure 8 demonstrates an example of E-Tree: "EU" refers to a pair of action and its resulting observation. According to the context definition, the context of "H4" consists of "Root EU1","H1", and "EU2".

Knowledge Matching. Given the definition of context, the similarity measure was proposed to determine whether two pieces of knowledge (E-Tree) matches or not. Both base matching and weighted matching are used to calculate similarity. Base Matching is the minimum criteria. For instance, Two E-Trees should come from the same data source. Weighted Matching is based on Base Matching. We can calculate the degree of matching through Weighted matching. To efficiently rank E-Trees based on similarity, Zhong et al. further proposed a Match Propagation (MP) algorithm to efficiently rank E-Trees by similarity [7].

In summary, [7] presents an AOH model to retrieve data triage operation. After representing analysts' experience as an experience tree, there are several approaches to retrieve data triage operations. For example, this work constructs indexes for retrieving efficiently.

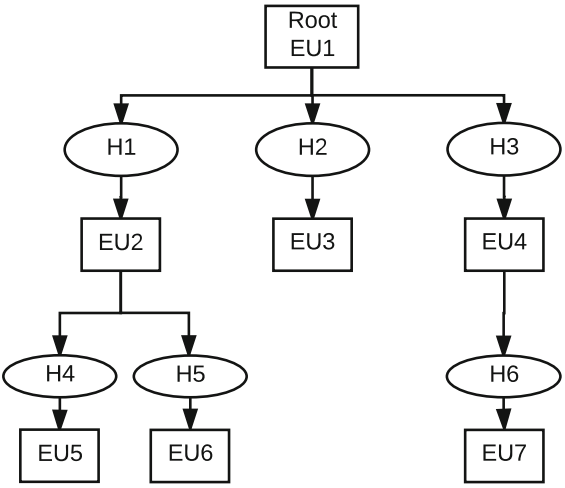

Fig. 8. An E-Tree example.

6 Future Directions in Data Triage Operation Retrieval

The existing studies introduced in the above section has demonstrated promising results for future studies. In this section, we propose several research directions for developing data triage knowledge retrieval systems.

6.1 Graph-Based Data Triage Knowledge Retrieval System

According to the conceptual AOH model, an action is a data triage operation performed by an analyst to filter or to correlate network events, which usually specify a condition on the network events to narrows down the dataset. It is through conducting a series of data triage operations enables an analyst to find the critical "indicators" of potential attack chains. Therefore, the analytical reasoning strategies used by an analyst are embedded in the relationships (both logical and temporal relationships) among the data triage operations. With this insight, a graph-based data triage knowledge retrieval system can be developed that represents and retrieves not only the analytical reasoning process but also the underlying logic and reasoning strategies used by analysts.

Knowledge Representation. Recall that there are three types of data triage operations in SOC:

- FILTER (D, C): to filter a set of events based on a constraint.
- SEARCH (D, C): to search a keyword in an events group.
- SELECT (D, C): to select a subset of events with a specific feature.

All these operations are performed to obtain a subset satisfying a specific constraint. Therefore, a constraint is a critical component in a data triage operation. A constraint specifies the characteristics of network events, indicating the analyst's focus of attention. The constraint can be multidimensional if multiple characteristics are specified. Therefore, a constraint can be represented by a predicate in disjunctive normal form.

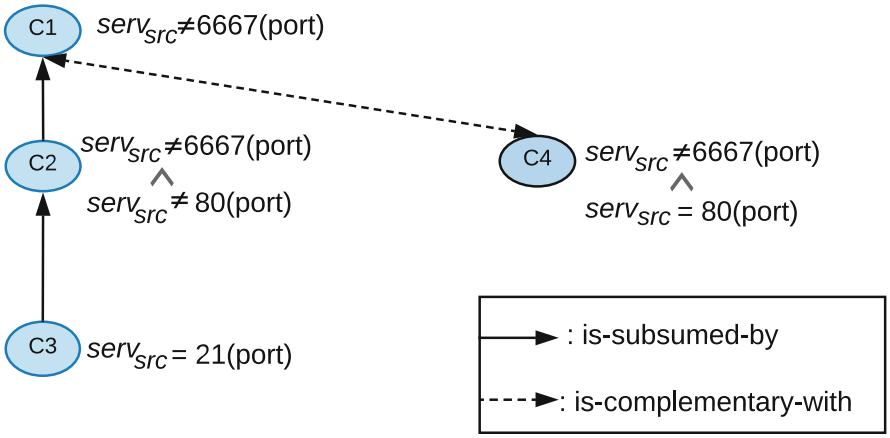

Fig. 9. An example of the logical relationships between data triage operations.

The relationships between data triage operations include both temporal and logical relationships [11]. An analyst performs data triage operations in a temporal sequence: one operation precedes the next one. The logical relationships between data triage operations are defined by the constraints specified in the operations. Let $C1$ and $C2$ be two constraints of operation $O1$ and $O2$ respectively, we have

- if $C1 \leftrightarrow C2$, $O1$ "is-equal-to" $O2$;
- if $C1 \rightarrow C2$, $O1$ "is-subsumed-by" $O2$;
- if $C2 \rightarrow \neg C2$ *and* $C2 \rightarrow \neg C1$, $O1$ "is-complementary-with" $O2$;

The examples of the "is-subsumed-by" and"is-complementary-with" relationships are demonstrated in Fig. 9. The nodes are the constraints that specify the characteristics of network events (i.e., C1, C2, C3, and C4). C2 is subsumed by C1, and C3 is subsumed by C2. C1 and C4 don't have overlap so that they are complementary with each other.

To discover an analyst's analytical reasoning process, both temporal and logical relationships need to be considered. More specifically, we are mainly interested in learning how a data triage operation is related to the previous operations. Therefore, given all the operations performed by an analyst, we identify the logical relationships between each operation and all its preceding operations and represent them in a graph structure.

Knowledge Matching and Challenges. The context of a data triage operation can be defined as all its preceding operations and their temporal and logical relationships. Given the graph structure, the context of a data triage operation is a graph. Therefore, the matching problem becomes a graph matching problem: we need to search in the knowledge base (i.e., a collection of graphs) to find the graphs/subgraphs that matches the current context of the user of the retrieval system.

The time efficiency is the main challenge for graph matching. Graph isomorphism analysis is usually time-consuming. In order to improve the time performance, it worths considering the similarity calculation based on the "centroid" of graphs: first, to develop a method for calculating the"centroid" of a graph; second, to develop a similarity measure to compare the "centroids" of two graphs; and then match the graphs based on the centroid similarity.

6.2 Machine Learning Based Retrieval of Triage Operations

Due to the following observations, machine learning could play an essential role in developing better data triage operation retrieval systems. First, the methods we have discussed in the previous sections make use of pre-determined similarity measurements when checking which historical data triage operations are most relevant to the current cyber situation. However, there is no guarantee that the pre-determined similarity metrics are the most suitable. Machine learning could be leveraged to help learn the most suitable similarity metrics. Second, data triage operation retrieval systems must be able to handle a variety of uncertainties such as the uncertainty introduced by false positives, false negatives, and incomplete information. Machine learning could be leveraged to increase retrieval systems' capability in dealing with the uncertainties.

Machine learning, especially neural networks, is a potential approach, which can be used for data triage operation retrieval in a SOC. There are a variety of artificial neural networks, such as convolutional neural networks, long short-term memory [6], and deep belief networks. Instead of providing a comparative viewpoint, below we only discuss the potential application of recurrent neural networks.

Data Triage Operation Retrieval Based on Recurrent Neural Networks. For data triage operation retrieval, the most promising neural networks approach seems to be recurrent neural networks (RNN), mainly because this type of neural network is good at dealing with sequence data. One of the most notable features in data triage operations is that security-related events are sequential. The fundamental philosophy behind RNN models is that rather than rewriting all information, each element in an RNN model updates the current state by adding new information. Accordingly, when an RNN is trained to classify the newly arrived data triage operations, the RNN can be incrementally maintained to incorporate substantial new data triaging knowledge.

But, before training and deploying any RNNs in a SOCs, the SOC should cautiously consider the potential adversaries. A new challenge which is faced by

a SOC but is not addressed in other knowledge retrieval systems is that data triage operations are being retrieved in adversarial settings. That is, the attacker may purposely obfuscate their attack actions in such a way that the accuracy of triage operation retrieval could be significantly reduced. Recently, substantial research work has shown that most existing machine learning classifiers are highly vulnerable to adversarial examples. The RNNs deployed in a SOC should be resilient to adversarial examples.

Challenges in Using Machine Learning for Data Triage Operation Retrieval. Machine learning has been playing an increasingly important role in performing various tasks in SOCs. For example, network intrusion detection systems and malware classification systems are leveraging more and more automation achieved through machine learning.

However, although machine learning is good at (dealing with) average cases, it is not easy to implement any machine learning methods for data triage operation retrieval systems, since data triage operation retrieval systems are related to worst cases. It is possible to bypass a machine learning based content filter through malicious manipulations in adversarial settings. The attacker could combine malicious samples with benign events to evade several retrieval classifiers. For example, some very small manipulations in events logs can lead to distinct opposite results in data triage operation retrieval systems. It is not an easy task to guarantee accuracy and sensitivity simultaneously. In data triage operation retrieval, because of the inherent temporal relationships between events, the adversary has the possibility to infer the similarity metrics to bypass the retrieval system.

6.3 Ontology-Based Data Triage Operation Retrieval

Ontology-based retrieval is widely used in semantic web (data) search [5]. Researchers may apply this approach to solving several relevant triage operation retrieval problems (e.g., semantics-aware retrieval of triage operations). In order to apply this approach, researchers need to map data triage operations into an ontological knowledge base. To achieve this goal, the main hurdle is the ontological annotations. After the ontological annotations are obtained, the next step of data triage operation retrieval seems to "embed" semantic features into the retrieval process.

7 Concluding Remarks

A major challenge of data triage in SOCs is the inefficient performance of junior security analysts caused by the lack of experience. It can be effectively addressed through retrieval of the relevant past data triage operations performed by the senior analysts. We conducted a review of the existing data triage knowledge retrieval methods and discussed the new directions in solving the retrieval problem in this field.

Acknowledgment. This work was supported by ARO W911NF-13-1-0421 (MURI) and ARO W911NF-15-1-0576.

References

1. Chen, P.C., Liu, P., Yen, J., Mullen, T.: Experience-based cyber situation recognition using relaxable logic patterns. In: 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 243–250. IEEE (2012)
2. D'Amico, A., Whitley, K.: The real work of computer network defense analysts. In: Goodall, J.R., Conti, G., Ma, K.L. (eds.) VizSEC 2007. Mathematics and Visualization, pp. 19–37. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78243-8_2
3. Erbacher, R.F., Frincke, D.A., Wong, P.C., Moody, S., Fink, G.: A multi-phase network situational awareness cognitive task analysis. Inf. Vis. **9**(3), 204–219 (2010)
4. Ganame, A.K., Bourgeois, J., Bidou, R., Spies, F.: A global security architecture for intrusion detection on computer networks. Comput. Secur. **27**(1), 30–47 (2008)
5. Lukasiewicz, T.: Ontology-based semantic search on the web. Ann. Math. Artif. Intell. **65**(2–3), 83–121 (2011)
6. Palangi, H., et al.: Deep sentence embedding using long short-term memory networks: analysis and application to information retrieval. IEEE/ACM Trans. Audio Speech Lang. Process. (TASLP) **24**(4), 694–707 (2016)
7. Zhong, C., et al.: RankAOH: context-driven similarity-based retrieval of experiences in cyber analysis. In: 2014 IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 230–236. IEEE (2014)
8. Zhong, C., Yen, J., Liu, P., Erbacher, R., Etoty, R., Garneau, C.: ARSCA: a computer tool for tracing the cognitive processes of cyber-attack analysis. In: 2015 IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 165–171. IEEE (2015)
9. Zhong, C., Yen, J., Liu, P., Erbacher, R., Etoty, R., Garneau, C.: An integrated computer-aided cognitive task analysis method for tracing cyber-attack analysis processes. In: Proceedings of the 2015 Symposium and Bootcamp on the Science of Security, p. 9. ACM (2015)
10. Zhong, C., Yen, J., Liu, P., Erbacher, R.F., Garneau, C., Chen, B.: Studying analysts' data triage operations in cyber defense situational analysis. In: Liu, P., Jajodia, S., Wang, C. (eds.) Theory and Models for Cyber Situation Awareness. LNCS, vol. 10030, pp. 128–169. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-61152-5_6
11. Zhong, C., Yen, J., Liu, P., Erbacher, R.F.: Automate cybersecurity data triage by leveraging human analysts' cognitive process. In: 2016 IEEE 2nd International Conference on Intelligent Data and Security (IDS), 2nd edn., pp. 357–363. IEEE (2016)