Using Extensible Metadata Definitions to Create a Vendor-Independent SIEM System

Prof. Dr. Kai-Oliver Detken[1], Dr. Dirk Scheuermann[2], Bastian Hellmann[3]

[1] DECOIT GmbH, Fahrenheitstraße 9, 28359 Bremen, Germany, detken@decoit.de
[2] Fraunhofer Institute for Secure Information Technology, Rheinstrasse 75, 64295 Darmstadt, Germany, dirk.scheuermann@sit.fraunhofer.de
[3] University of Applied Sciences and Arts of Hanover, Ricklinger Stadtweg 120, 30459 Hanover, Germany, bastian.hellmann@hs-hannover.de

Abstract. The threat of cyber-attacks grows up, as one can see by several negative security news and reports [8]. Today there are many security components (e.g. anti-virus-system, firewall, and IDS) available to protect enterprise networks; unfortunately, they work independently from each other – isolated. But many attacks can only be recognized if logs and events of different security components are combined and correlated with each other. Existing specifications of the Trusted Computing Group (TCG) already provide a standardized protocol for metadata collection and exchange named IF-MAP. This protocol is very useful for network security applications and for the correlation of different metadata in one common database. That circumstance again is very suitable for Security Information and Event Management (SIEM) systems. In this paper we present a SIEM architecture developed during a research project called SIMU. Additionally, we introduce a new kind of metadata that can be helpful for domains that are not covered by the existing TCG specifications. Therefore, a metadata model with unique data types has been designed for higher flexibility. For the realization two different extensions are discussed in this paper: a new *feature model* or an additional *service identifier*.

Keywords: Security Information and Event Management (SIEM), anomaly detection, IF-MAP, metadata schema, Trusted Computing, feature model

1 Introduction

Security Information and Event Management (SIEM) systems are seen as an important security component of company networks and IT infrastructures. These systems allow to consolidate and to evaluate messages and alerts of individual components of an IT system. At the same time messages of specialized security systems (firewall-logs, VPN gateways etc.) can be taken into account. However, practice showed that these SIEM systems are extremely complex and only operable with large personnel effort. Many times SIEM systems are installed but neglected in continuing operation.

SIEM systems are typically only suitable for the use in huge enterprise environments, mainly because of the following reasons:

a. Deficient scalability to small and medium-sized networks.
b. High costs for installation and maintenance because new components (collectors) of IT infrastructure have to be installed, configured and maintained.
c. High costs for the operation due to the necessity of extensive expert knowledge for the policy and rule definition as well as for the correct analysis and the right interpretation of the output of SIEM systems.

Therefore, the main goal of the SIMU project is the development of a system, similar to SIEM, which significantly improves IT security in a corporate network without making great effort. In addition to its simple integration into IT infrastructures of SME and its easy traceability of relevant events and processes in the network, it is to be realized without great effort of configuration, operation and maintenance. On the functional level SIMU works like common SIEM systems, which means it monitors processes and events within the corporate network and automatically initiates proactive real-time measures to improve security. [1]

The remainder of this paper is organized as follows: Section 2 gives a short definition of SIEM systems, followed by the overall architecture of the SIMU research project in section 3, including a short introduction into the IF-MAP specification of the Trusted Computing Group. Section 4 describes the general requirements on extensible metadata models and the process of publishing them in the context of already given specifications, worked out within the ESUKOM project [9]. The specific and abstract metadata defined in the ESUKOM research project, implementing the requirements from section 4 as well as their mapping to IF-MAP is then shown in section 5. In section 6 we wind up our findings by creating and publishing own metadata definitions and by explaining how they allow creating an open-source based SIEM system as in SIMU.

2 A Definition of SIEM Systems

The acronyms SEM, SIM, and SIEM are often used in the same context, although correctly the term SIEM is a combination of the other two. The first area provides long-term storage, analysis and reporting of log data and is known as Security Information Management (SIM). The second area deals with real-time monitoring, correlation of events, notifications and console views and is commonly known as Security Event Management (SEM) [3]. Both areas can be combined differently to set-up a SIEM system.

SIEM technology provides in detail real-time analysis of security alerts, which have been generated by network hardware and applications. SIEM can be used as software, appliances or managed services, and is also applied to log security data and generate reports for compliance purposes. The objective of SIEM is to help companies respond faster to attacks and organize mountains of log data.

The term Security Information and Event Management (SIEM) has been published by Mark Nicolett and Amrit Williams of Gartner in 2005[4] and describes the product capabilities of gathering, analyzing and presenting information from network and security devices. Further features are identity and access management applications, vulnerability management and policy compliance tools, operating system, database

and application logs, and external threat data. A key focus is to monitor and help manage user and service privileges, directory services and other system configuration changes, as well as providing log auditing and review and incident response.

A complete SIEM system consists of different modules (e.g. event correlation, anomaly detection, identity mapping). These modules are responsible for the "intelligence" of a SIEM system, determining the complexity of events to be detected by the system.

3 The SIMU Research Project

The architecture of the SIMU research project, as shown in Figure 1, uses the IF-MAP protocol as central mechanism to exchange metadata between different security components. Besides the used and adapted open source tools, two German vendor solutions from NCP (VPN) and macmon (NAC) have been integrated.

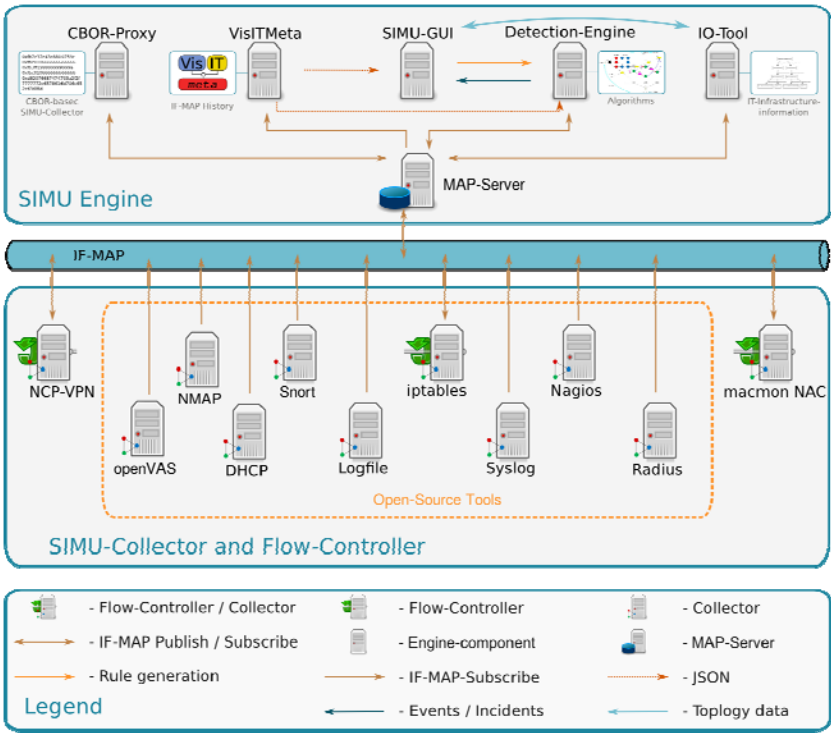

Figure 1. SIEM architecture of the project SIMU

The architecture is divided into two layers, which are connected by the IF-MAP protocol:

a. The *SIMU collector* and *flow-controller layer*, where the components are responsible for data collection and enforcement.

b. The *SIMU engine*, which includes the components for central data and knowledge storage, the data correlation, aggregation, and visualization of data, as well as interfaces to other protocols.

The SIMU engine is the processing and presenting component of the architecture. It includes the MAP server as the central communication point for information exchange, the VisITMeta (a software and research project aiming at storing and visualizing IF-MAP graph data [10]) component for data storage and metadata graph visualization, the correlation engine for situation detection and policy checking and the SIEM-GUI – a graphical user interface which presents the analysis results and according incidents to the administrator in an understandable manner. The IO-Tool (Interconnected-asset Ontology) [7] works on ontology basis and extends the database with further asset information of the network infrastructure to enable a correlation later on. The CBOR (Concise Binary Object Representation) protocol (RFC-7049) is a data exchange protocol, which focuses on multiple design goals including small code and message size, and extensibility. CBOR is used in this architecture as an alternative to SOAP/XML as used within IF-MAP. It can help to address performance problems and facilitate the usage of IF-MAP. That is especially important for small bandwidth scenarios with mobile devices.

The SIMU engine presents the results of the data analysis by the SIEM-GUI. Therefore the graphical user interface (GUI) has to communicate with the detection engine and VisITMeta directly and with the IO toolset indirectly. The SIEM-GUI has to show the events obviously and send understandable notes to the administrator. Therefore, the SIEM-GUI is of central importance.

3.1 The Interface for Metadata Access Points (IF-MAP)

IF-MAP is an open standard, client-server based protocol by the Trusted Computing Group (TCG) for sharing arbitrary metadata across arbitrary entities. Its intended purpose was to enable network devices to share security sensitive information with the goal to integrate arbitrary tools (such as NAC solutions, firewalls, IDS, etc.), thus easing their configuration and extending their functionality. However, it turns out that IF-MAP can also provide benefit to other use cases that do not have anything to do with network security. That is why the TCG decided to separate the use case independent base protocol [6] (current version 2.2) from the use case dependent metadata specifications. This ensures that new metadata specifications can easily be developed without touching the base protocol specification. Currently, there is one official specification that specifically defines standard metadata types for the field of network security: TNC IF-MAP Metadata for Network Security [5].

Trusted Network Connect (TNC) is the TCG approach for Network Access Control (NAC) solutions. TNC is the reference architecture for NAC that defines the necessary entities and the interfaces through which they are communicating in an interoperable way. IF-MAP is part of the TNC framework.

The base specification defines the two roles – client and server – and three different operations: publish, search and subscribe to distribute and access information. In addition, the basic data model is defined, consisting of identifiers (entities) and metadata, which can be attached either to the identifiers directly or connect two iden-

tifiers as a kind of relationship, called link. Thereby, an undirected information graph originates. Both metadata and identifiers provide specified instruments to use them for arbitrary domains.

IF-MAP can provide the following benefits:

a. Integration of existing security systems by a standardized, interoperable network interface
b. Avoidance of isolated data silos within a network infrastructure
c. Extended functionality of existing security tools (e.g. automatic responses on detected intrusions, identity-based configuration of packet filters)
d. Vendor independence

3.2 Collector and Flow Controller Components

Flow controller and collectors are typical security components and services in a network infrastructure. They collect information or manage the network behavior. Several clients have been adopted to support integration into an IF-MAP environment, e.g. providing the IF-MAP data model with their information or using IF-MAP information for decisions. The following IF-MAP client collectors for the architecture of SIMU have been implemented (as shown in Fig. 1):

a. **DHCP collector:** extracts metadata of actual IP leases from the lease file.
b. **RADIUS collector:** delivers metadata regarding user logins and the user itself (groups, authority).
c. **Syslog collector:** delivers metadata regarding the status of arbitrary syslog clients - hosts and services (e.g. CPU load or false logins).
d. **Nagios collector:** publishes extracted metadata from Nagios regarding the status of hosts and services (i.e. availability of the network).
e. **Icinga REST collector:** works as an alternative for Nagios and has the same functionality.
f. **Snort collector:** translates Snort alerts in IF-MAP metadata.
g. **NMAP:** Network Mapper integration into the IF-MAP environment. Detects devices, server, services, etc.
h. **OpenVAS:** publication of the scan results obtained by the vulnerability scanner. Allows for periodic or regularly triggered scans and can automatically respond to requests for investigation.
i. **Log-file collector:** generic collector for analysis of arbitrary log-files and translation of the log information in IF-MAP metadata.
j. **Android collector:** delivers metadata regarding the status and behavior of an Android smartphone (e.g. firmware, kernel, build number, traffic on different network interfaces, CPU load).
k. **LDAP collector:** manages a connection to the directory service and delivers according IF-MAP metadata.

Furthermore the architecture includes the following flow-controller components, which partly have also collector functionality:

a. **iptables flow-controller:** makes automated set-up of firewall rules possible as a reaction to special metadata events and publishes these metadata also as enforcement reports for the MAP server.

b. **macmon NAC flow-controller:** This network access control system from macmon publishes different information of connected endpoint-devices, especially authorization information of well-known end-devices, the location in the network (e.g. physical port, WLAN-AP), and further device characteristics (e.g. operating system, open ports).
c. **NCP-VPN flow-controller:** This virtual private network solution of NCP can deliver several relevant metadata to the server, such as authorization, IP address, data throughput, and connection time of a user. Enforcement is possible on the VPN layer.
d. **OpenVPN flow-controller:** SSL-based alternative VPN solution with similar features.

All these components combined present the sensors of a SIEM system and collect data from the network. The key feature of a SIEM system is to correlate these data efficiently and usefully to find out which event is an anomaly and which is not. Therefore, it is necessary to analyze a data basis of the same format. IF-MAP can handle this with its extensible metadata definition.

4 Requirements and Strategies for Metadata Definition

Metadata plays an important role for securing network applications. The TCG already established specifications providing large amounts of standardized metadata and identifiers useful for network security. However, the existing standard data schemes often do not provide appropriate types for all data objects relevant for a certain application like a desired SIEM system. The design of new applications often requires the definition of additional and domain-specific metadata. The German research project ESUKOM [9] addressed the problem of real-time security for enterprise networks. The general approach was to establish a metadata model allowing the discovery of anomalies and unwanted situations in a network by consolidation of metadata. With the ESUKOM project and its covered use cases and prototype developments as an example, we want to outline the process of building use-case specific data models and looking for appropriate data types and possible enlargements of the existing TCG specifications.

4.1 Scientific and Technical Goals of ESUKOM

The ESUKOM project aimed to develop a real-time security solution for enterprise networks that is based on the correlation of metadata. The ESUKOM approach focused on the integration of available and widely deployed security measures based upon the Trusted Computing Group's IF-MAP specification. The idea was to operate on a common data pool that represents the current status of an enterprise network. Currently deployed security measures were integrated and able to share information as needed across this common data pool. This enables the ESUKOM solution to realize real-time security measures. All data shared across the common pool were formulated according to a well-defined data model.

In order to achieve this goal, the following tasks were accomplished:

a. Implementation of IF-MAP software components
b. Development of an advanced metadata model
c. Development of correlation algorithms
d. Integration of deployed security tools

For this paper, especially the metadata model approach is interesting. The IF-MAP specification currently defines a model for metadata that specifically targets use cases in the area of network security. The metadata model of IF-MAP has been extended and refined for ESUKOM to get the possibility to add new types of metadata as well as to improve drawbacks of the current metadata model.

4.2 Problem Description

Within the SIMU research project, the main goal was to design and develop a real-time security SIEM system for networks of small and medium-sized enterprises (SME). The mobility of modern endpoints such as smartphones, tablets and notebooks and their corresponding threats to the overall network security were especially considered while developing the system.

Several user scenarios and use cases have been defined within the project ESUKOM before. For a detailed data model specification and a final development of a client-server application, a generic scenario has been developed for which the following relevant key features appeared:

a. **Anomaly Detection:** recognition of illegal system states by detection of abnormal behavior. Such behavior could be excessive use of network resources or unusual usage, and must be considered within contextual information like time or location.
b. **Mobile Device Awareness:** recognition of devices as mobile devices and application of corresponding policies. Smartphone specific policies could, for example, allow to ensure the non-use of sensors.
c. **Location-based Services:** providing services depending on detected position of devices. For example, a device could be allowed to access data only when it is present at a specific location, and is denied access when outside this location.
d. **Detection of critical attacks on vulnerable components:** When known attacks are detected within the network on a component that has a known vulnerability in one of its provided services, it must be recognized instantly and appropriate countermeasures need to be taken.
e. **Real-time Enforcement:** If abnormal behavior or malicious endpoints are detected within the network, an immediate reaction must occur. Therefore information about the detection has to be made available to enforcement components as soon as they appear.

The security solution to address all key features uses metadata, i.e. information gathered about the network – like the participating components and their capabilities – and the actions that occur within. These metadata can be generated by different components of the network itself, which allows using already existing components of today's networks, like DHCP servers, flow controllers or intrusion detection systems (IDS). Thus, the specific view of each component on traffic and endpoints in the net-

work can be used. The idea within the project was to gather all this separated information in such a way, that the information could be used by any other component. Therefore, the information itself had to be gathered and stored in a uniform way, both regarding the exchange over the network and the data model itself.

4.3 Requirements for the Data Model

The following requirements for a data model suitable for the key features were found:

a. **Integration of arbitrary metadata:** Metadata from multiple different domains must be used within the new data model. As different components have a specific view onto a network, the data model has to be flexible and non-restrictive in terms of what values can be expressed.
b. **Technology independence:** The model itself has to be independent of any concrete technology. An implementation of the data model, i.e. a mapping to a concrete technology, will then have to ensure that all needed components to solve the key features can exchange the data in a platform independent way.
c. **Allowing enlargements:** To allow the use of our model in future use cases and scenarios, the model itself has to be extensible. Thus, the definition of data has to be done in a flexible way.
d. **Covering all intended use cases:** All previously identified concepts and key features need to be represented by the model. The model has to be able to include all metadata that is needed to solve the key features.

This abstract data model allows defining all metadata that are needed to implement all key features within the ESUKOM project.

4.4 Strategies for Additional Data Definition

To embed the functionality of the data model developed within the ESUKOM project into the already existing specifications by the TCG, several strategies can be followed:

1. **Additional vendor specific data:** A simple strategy is to use already existing functionality for extension within a specification. Although this would leave the specification as it is, it will not be appropriate for future standard applications, as they would also have to use the ESUKOM specific – and thus not standard- definitions. Interoperability with non-ESUKOM components would be a problem.
2. **Enlargement of specification:** The original specification can be extended by the types and attributes of the data model. This process usually takes a long time, as changing a specification involves multiple rounds of review by the corresponding working group, and has the disadvantage that it cannot always be done (e.g. new data definitions are to use-case specific).
3. **Define a standardized way to enhance metadata specifications:** A third strategy and kind of compromise of the two previous suggestions is to encourage the specification work group to adjust their own policies for enlargement so that additions like the ones of the ESUKOM project can be easily added to the specifica-

tion. That way third-party vendors can also use the then more powerful metadata definitions of other research projects, companies etc.

The requirements for the ESUKOM metadata model must now be realized in a concrete metadata model, suitable for all use cases and scenarios. Afterwards, this metadata model has to be mapped onto an existing technology that defines both a data model, which is flexible enough to adapt the requirements of the ESUKOM data model, as well as a communication protocol and architecture to gather and exchange the metadata.

5 Data Model for Non-Proprietary SIEM Systems

In the last sections, we have identified the major properties of the IF-MAP protocol and general requirements for data models as well as possible strategies. The ESUKOM project now took the approach to design an IF-MAP based data model based on these aspects. In this section, the ESUKOM data model will be presented and it is exemplified how the model can be mapped onto entities within the IF-MAP scope.

5.1 General Data Model

The general scope of the model is to cover the following aspects:

a. **Specification of data objects:** Identifiers shall be defined for instances publishing and subscribing data as well as formats for the exchanged data (metadata).
b. **Specification of anomalies:** Abnormal system states shall be represented by combinations of certain data values.
c. **Specification of policies:** Actions shall be taken if certain system states, including anomalies, are detected.

First of all, the following basic data components are defined to cover the intended data objects. Later on, they will be mapped onto identifiers and metadata in compliance with [5] and [6]:

a. **Feature (F)**: A feature represents an elementary unit of the metadata model containing a measured value inside the application.
b. **Category (C)**: A category represents a collection of features belonging to the same group. Nested structures are possible, i.e. a category may also represent a collection of subcategories.
c. **Context Parameter (Ctx-P)**: Context parameters provide additional information connected with a feature describing the closer context, in particular information about time, location and connected devices.

On the way to the detection of anomalies, the following components are defined to represent certain system states:

a. **Context (Ctx):** A context is a Boolean combination of Ctx-Ps as mentioned above. Independent of certain features, it just gives out Boolean information that a certain set of Ctx-Ps values fulfill certain conditions.

b. **Signature (Sig):** A signature represents a pattern describing a certain system state. It consists of a set of feature instances with corresponding values. Optionally, a signature instance may also contain a set of context instances (see above).
c. **Anomaly (A):** An anomaly represents a system state deviating from normal system's behavior. It is composed of so called hints, each one describing a feature deviating from its expected value range. As well as signatures, anomalies may also optionally contain sets of context instances. The major difference to signatures consists in the fact that anomalies are not directly visible by exact feature values but must be determined with a more complex analysis.

After specification of data objects and system states, the next step is the definition of policies how to react to certain system states, in particular anomalies, by certain action. In our model, a policy (P) consists of a collection of rules (R) whereby a rule is represented by a statement of the form "if condition do action". A condition is represented by a Boolean combination of contexts, signatures and anomalies, and an action consists of a creation, deletion or modification of features. Figure 2 shows the overview of the components of the ESUKOM model.

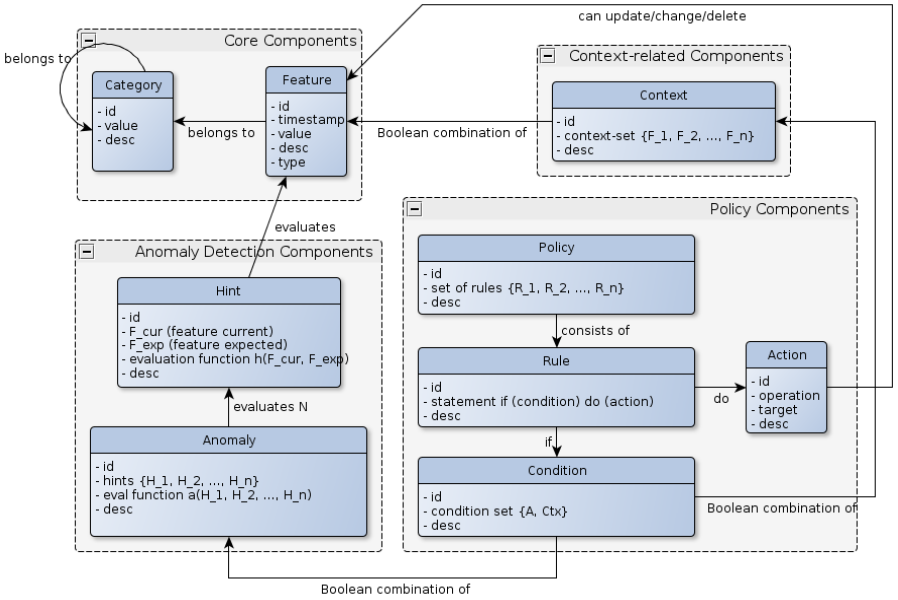

Figure 2. ESUKOM model as a whole

5.2 Identification of Domain Instances

Before looking for a formal description of the data model components described above, ESUKOM first looks for concrete data objects needed for the key features of the project listed in section 4.2. This resulted in sets of so called domain instances including categories, features, signatures, policies etc. with assigned values. Figure 3 shows the domain instances used to represent the key feature needed to detect suspi-

cious login attempts (many false attempts in a short time or nearly simultaneously login attempts of the same user at different locations) or abnormal network traffic. The grey rectangles define the categories with their logical structure: the user with a corresponding login history and the collection of dataflow parameters. All yellow rectangles represent the features. For all other key features within ESUKOM, different sets of domain instances were defined. Some of them work in conjunction with domain instances of other key features. As an example, domain instances that define a smartphone with its operating system version, its apps, the apps permissions, and so on, can also be used to detect anomalies in the behavior of a device.

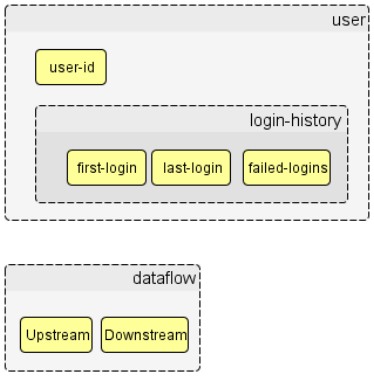

Figure 3. Domain instances for anomaly detection

5.3 Mapping onto IF-MAP

After the definition of the abstract data model, the basic data components have to be mapped onto data objects provided by IF-MAP, by using the common methods of extension. As already indicated in the last subsection, specific needs for the ESUKOM key features shall be considered:

a. **Mapping of categories (C):** In our data model, categories work as structuring elements and do not contain any metered values. Therefore, they are mapped onto identifiers according to [6]. An identifier of type o*ther* is used, whereby the *other-type-definition* attribute is set to the type of the category. For handling the hierarchy of categories, a new metadata type *subcategory-of* without any further contents or attributes is defined. Publishing this metadata type as a link between two categories indicates their subcategory relation.
b. **Mapping of context parameters (Ctx-P):** Context parameters represent information directly applied to feature data. Therefore, they are mapped onto XML attributes. For this purpose, a new attribute group *contextParameters* is defined that covers the attribute values intended to be used for the context information (time, location and connected devices).
c. **Mapping of features (F):** It is pretty obvious that features are represented by metadata according to [5]. These metadata are published by identifiers representing categories, and they contain attribute groups representing context parameters. However, the exact approach how to map features onto metadata

types is not as straightforward as the mapping concept for categories and context parameters.

First of all, it seems to be reasonable to search for appropriate standard metadata and to only define new vendor specific data if none of the data types already specified within [5] fits to the data objects specified for the key features. However, this approach appeared as problematic for the following reasons, in particular with respect to the concrete domain instances identified for our key features:

a. A lot of new data types, currently not provided by [5] are needed for our key features. The few cases with existing usable standard data types appeared as exceptional cases. Sometimes, data types generally fitting to the feature exist but not with right structure (either with missing or superfluous components).
b. According to TCG policies, standard metadata types must not be equipped with additional attribute groups, and existing attribute groups must not be enlarged with additional attributes or replaced by other attribute groups, although this would be compliant with the present XML syntax of the specification. As far as enlargements are foreseen, they are to be done exclusively by the TCG. This condition provides a major problem for the mapping of context parameters onto attributes as foreseen by our model.

Therefore, the decision was to specify a new (vendor specific) metadata type feature and to use this unique data type for all features identified within the ESUKOM features. The name of the feature is contained within an id attribute of the data type, and the values are classified by a type attribute that can be quantitative (concrete metered value), qualitative (enumeration) or arbitrary (any string). The metadata value itself is represented by a value attribute. Additionally, it can be enriched by context parameters like time or location as described above. Listing 1 shows the XML structure of the new feature type.

```
<xs:element name="feature">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="id" type="xs:string">
      </xs:element>
      <xs:element name="type">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="quantitive"/>
            <xs:enumeration value="qualified"/>
            <xs:enumeration value="arbitrary"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="value" type="xs:string">
      </xs:element>
    </xs:sequence>
    <xs:attributeGroup ref="ifmap:multiValueMetadataAttributes"/>
    <xs:attributeGroup ref="contextParameters"/>
  </xs:complexType>
</xs:element>
```

Listing 1. XML definition of „Feature“

By this way, our model gets very flexible, and no general changes on the abstract model or the definition of new data types are needed if new necessary features for

new applications like new SIEM systems are detected. This new metadata type is then to be published by identifiers representing categories as described before.

The strategies of the ESUKOM project regarding the data model design were also continued within the follow-up project SIMU. Here another extension was developed, where a new identifier called service was introduced to describe services running on a device. Together with new link-metadata and new identifiers for vulnerabilities and implementations, a sub-graph for a service within a network and its concrete implementation on a device (e.g. measured by nmap) as well as its detected vulnerabilities (e.g. measured by OpenVAS) can be described. This can then be used to correlate detected attacks that aim at a specific CVE with actually running services that are vulnerable to this exact CVE.

6 Conclusions

SIEM systems are complex solutions and consist of different modules, security components, and interfaces. With the use of SIEM systems there are much installation and service efforts associated. That is the reason why in small and medium-sized enterprises (SME) these kinds of systems are still not represented. The developed system in SIMU focuses on SME scenarios and includes an easier implementation strategy than other SIEM systems today. By the use of the protocol IF-MAP it is possible to receive the log-information from different security components on the same data format. Thereby, it is possible to collect these data in a common database and correlate this information base to find out anomalies or vulnerability.

After the identification of use cases and corresponding data objects, several strategies for an enlargement of the present IF-MAP standard metadata were discussed. Finally, it was decided to uniquely use the newly defined data type feature, which gives a high flexibility in case of further enlargements for other use cases.

Despite the good practical results, the ESUKOM data model also shows up some weaknesses when strictly used this way for any future applications. One weakness is provided by the fact that the new feature type represents a non-standard data type whereas some client developers do not need additional metadata beyond the existing specifications and therefore are not designed for usage of any other ones. But in summary, it can be recommended to partially use the ESUKOM model by always preferring standard metadata types but always having the option to use the feature data type as well as the new context attributes together with any metadata type.

Furthermore, the grouping of features into categories should be possible, but not mandatory. As a final result, a proposition for a TCG-driven enhancement of the IF-MAP specifications can be given by adopting the new feature type as a standard type. Furthermore, the newly developed attribute group contextParameters should be adopted as a new attribute group type optionally available for all standard types in order to have a unique format for time and location information as well as information about connected devices. In addition, a new identifier type should be defined for the optional categories. A realization of this proposition would always give client developers the option to make use of the ESUKOM data model within the IF-MAP standards, but its usage would not be mandatory.

This *feature model* approach makes it possible to create a flexible data model if needed. The data model of the SIMU project is based on the work of ESUKOM, although no immediate need for the *feature type* occurred. It is recommended to also include the *service identifier* (specified within the SIMU project) into future versions of the TCG specifications, given that it is as basic as the other standard identifier types, such as *ip-address* or *device*, when describing the state of a network with IF-MAP. As a final conclusion, it is recommended to use the existing specification description of the TCG regarding interoperability with other IF-MAP components. If an extension is needed it would be useful to integrate this definition also into the standard specification. If that is not possible the solution of ESUKOM can be used. But that includes interoperability lacks between different IF-MAP components and will work only in proprietary environment.

Acknowledgements

The authors give thanks to the German Ministry of Education and Research (BMBF) [2] for the financial support as well as to all other partners involved into the research projects ESUKOM [9] and SIMU [1] for their great collaboration. The projects consist of the industrial partners DECOIT GmbH, NCP engineering GmbH, macmon secure GmbH, and the research partners Fraunhofer SIT, and University of Applied Sciences and Arts of Hanover.

References

1. SIMU project website, http://www.simu-project.de
2. Federal Ministry of Education and Research, http://www.bmbf.de/en/index.php
3. Jamil, A.: The difference between SEM, SIM and SIEM. 29th July (2009)
4. Williams, A.: The Future of SIEM – The market will begin to diverge. 1st January (2007)
5. TCG: TNC IF-MAP Metadata for Network Security. Trusted Network Connect, Specification Version 1.1, Revision 8, Trusted Computing Group (2012)
6. TCG: TNC IF-MAP Binding for SOAP. Trusted Network Connect, Specification Version 2.2, Revision 9, Trusted Computing Group (2014)
7. Birkholz, H., Sieverdingbeck, I., Sohr, K., Bormann, C.: IO: An interconnected asset ontology in support of risk management processes. IEEE Seventh International Conference on Availability, Reliability and Security, Page 534-541 (2012)
8. M. Shahd, M. Fliehe: Fast ein Drittel der Unternehmen verzeichnen Cyberangriffe. BITKOM news release from 11th of March 2014, CeBIT, Hanover (2014)
9. ESUKOM project website, http://www.esukom.de
10. Ahlers, V., Heine, F., Hellmann, B., Kleiner, C., Renners, L., Rossow, T., Steuerwald, R.: Replicable security monitoring: Visualizing time-variant graphs of network metadata. Joint Proceedings of the Fourth International Workshop on Euler Diagrams (ED 2014) and the First International Workshop on Graph Visualization in Practice (GViP 2014) co-located with Diagrams 2014, number 1244 in CEUR Workshop Proceedings, pages 32-41 (2014)