Integration of a System for Critical Infrastructure Protection with the OSSIM SIEM Platform: A dam case study

Luigi Coppolino[1], Salvatore D'Antonio[2],
Valerio Formicola[2], and Luigi Romano[2]

[1] Epsilon S.r.l., Naples, Italy
luigi.coppolino@epsilonline.com
[2] University of Naples "Parthenope", Department of Technology, Italy
{salvatore.dantonio,valerio.formicola,luigi.romano}@uniparthenope.it

Abstract. In recent years the monitoring and control devices in charge of supervising the critical processes of Critical Infrastructures have been victims of cyber attacks. To face such threat, organizations providing critical services are increasingly focusing on protecting their network infrastructures. Security Information and Event Management (SIEM) frameworks support network protection by performing centralized correlation of network asset reports. In this work we propose an extension of a commercial SIEM framework, namely OSSIM by AlienVault, to perform the analysis of the reports (events) generated by monitoring, control and security devices of the dam infrastructure. Our objective is to obtain evidences of misuses and malicious activities occurring at the dam monitoring and control system, since they can result in issuing hazardous commands to control devices. We present examples of misuses and malicious activities and procedures to extend OSSIM for analyzing new event types.

Keywords: Critical Infrastructure Protection, SIEM, dam, OSSIM.

1 Introduction

Misuses and malicious activities occurring at systems for Critical Infrastructure Protection (CIP) can have catastrophic consequences, such as financial losses and danger for life [1]. We refer to misuses as unintentional incorrect uses of the system: for example, unintentional violations of the operating procedures guaranteeing safety for users, staff and people in general. Instead, we refer to malicious activities as conscious activities aimed at compromising the correct operation of the system: for example, cyber attacks to communication networks supporting the critical infrastructures.

In recent years the monitoring and control devices in charge of supervising the critical processes of Critical Infrastructures have been victims of cyber attacks [2][3]. Typically the supervision of critical processes (i.e. key processes for

F. Flammini, S. Bologna, and V. Vittorini (Eds.): SAFECOMP 2011, LNCS 6894, pp. 199–212, 2011.

the critical infrastructure operation and for providing services) is realized by means of devices able to measure and modify process state parameters (namely sensors and actuators). Particularly the attacks have turned into intrusions, by exploiting the vulnerabilities of the Commercial-Off-The-Shelf (COTS) components, such as the legacy Supervisory Control And Data Acquisition (SCADA) systems: the SCADA systems are hardware and software solutions widely used to perform monitoring and control operations.

In such a scenario, the organizations that provide critical services, such as energy, water, oil, gas distribution, transportation, have to face several challenges: avoid regulation, policy and procedure violations; protect their network infrastructure from cyber attacks; guarantee proper operation of monitoring and control systems for the safeguard of population, staff and users.

To provide network protection, currently adopted solutions are based on management tools that assess the global level of security of the network infrastructure. Particularly interesting from this perspective are frameworks based on Security Information and Event Management (SIEM) systems, since they are able to analyze in a single point the reports produced by several kinds of devices deployed over the network infrastructure. Specifically the analysis of the SIEM framework is based on gathering and correlating the operating and security reports (also called "events") generated by Information and Communication Technology (ICT) appliances, applications and security tools, finally producing detailed and concise reports about the security level of the occurred events.

In this work we propose an extension of a commercial SIEM framework, namely OSSIM by AlienVault, to perform the analysis of the events reported by the components responsible for monitoring, controlling and protecting the processes and the operation of a critical infrastructure, specifically a dam. Our objective is to obtain evidences of malicious activities and misuses on the dam monitoring and control system, since they can result in issuing hazardous commands to the control devices.

We present our work in three main tasks. (1) We provide some examples of misuses and malicious activities that could result in issuing hazardous commands to the dam control devices. (2) We show how to extend the SIEM framework to process events generated by security, monitoring and control devices of the dam infrastructure (such as structural and environmental sensors): we have adopted the open source product OSSIM, developed and maintained by the AlienVault company, since it is extensible and highly customizable and allows to build components able to analyze new kinds of events. (3) We show how to implement new correlation rules in OSSIM in order to exploit the information of the events generated by security and process control systems and obtain evidences of misuses and malicious activities.

In Section 2 we present related works about most advanced technologies for dam and critical infrastructure monitoring and to supervise systems for CIP by means of SIEM based tools. In Section 3 we give more details about the dam monitoring and control systems. In Section 4 we describe the SIEM framework technology and the OSSIM product. In Section 5 we provide some examples of misuses and malicious activities and give details about the implementation of rules and plugins in OSSIM.

2 Related Work

This section shows that works proposing innovative approaches and technologies to monitor and control dam infrastructures do not address security issues [4] [5] [6]. On the other hand, works proposing to enforce the security of systems for CIP by means of SIEM based frameworks, give no relevance to the events related to critical process domain.

2.1 Use of SIEMs for Critical Infrastructure Protection

The DATES (Detection and Analysis of Threats to the Energy Sector) project, sponsored by the National Energy Technology Laboratory (NETL) of the U.S. Department of Energy, develops several intrusion detection technologies for control systems [7]. DATES adopts the commercial SIEM ArcSight to detect a network "traversal" attack to a corporate or enterprize network: the paper describes how to detect, by means of a SIEM framework, the attempt of controlling the system managing the critical processes; the attack is described as sequential violation of machines on the network hosting the field monitoring and control devices. The SIEM correlates intrusion events related to the hosts on the field network: anomaly based Intrusion Detection Systems are in charge of revealing attack attempts by looking at deviations from the normal behavior of field devices. In [8] is presented a joint work of Universidad ICESI and Sistemas TGR S.A. to implement the Security Operations Center (SOC) Colombia product. The system extends the OSSIM SIEM to evaluate reports produced by two different kinds of physical devices, specifically a fire alarm panel and an IP surveillance camera. Moreover it introduces a new interface to facilitate the creation of new correlation rules.

2.2 Advanced Monitoring and Control for Dam Infrastructure

In [4], the Korean Water Resource Corporation (Kwater) multi-purpose dam safety management system (KDSMS) has been proposed. KDSMS implements a workflow to coordinate the surveillance activities of dam field engineers, dam staff located in headquarter offices and experts in remote research centers. The framework manages different personnel profiles: each identity is responsible for transmitting reports, approving and notifying actions and for correlating different kinds of evidences or to require proper controls at the dam infrastructure.

In [5] a work by the Technical University of Lisbon is presented. The paper presents the prototype of a knowledge-based system to support engineers responsible for dam safety assessment. The system, named SISAS, is composed of a centralized management tool in charge of analyzing sensor data to evaluate the dam health, by comparing the measures with alert thresholds computed from reference models. The final diagnosis is reported to the operator by means of graphical interfaces, providing suggestions to recover from dangerous situations.

In [6], is presented a work financed by the Swiss Nation Center of Competence in Research (NCCR) Mobile Information & Communication Systems (MICS) and the European FP6 Wirelessly Accessible Sensor Populations (WASP) project. SensorScope faces the issue of effective monitoring in harsh weather conditions by means of wireless sensors. The prototype is composed of a sink station box and a wireless sensor network made of TinyOS based devices. The framework is in charge of retrieving measures of meteorological and hydrological parameters, such as wind speed and direction.

3 Dam Monitoring and Control

Dam infrastructure is designed to provide services related to the usage of water reservoirs: food water supplying, hydroelectric power generation, irrigation, water sports, wildlife habitat granting, flow diversion, navigation are just some examples.

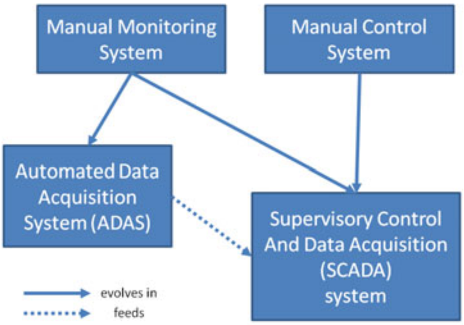

Manual Monitoring System
Manual Control System
Automated Data Acquisition System (ADAS)
Supervisory Control And Data Acquisition (SCADA) system
evolves in
feeds

Fig. 1. Automation evolution in dam monitoring and control systems

Since dam infrastructure has large geographical extension, monitoring and control operations must be performed in distributed fashion. In addition, some critical controls need to be orchestrated among several remote sites: for example the mechanisms related to the production of hydroelectric power require to control the reservoir discharges feeding the downriver plants. To monitor and control such a complex system, a large number of devices are deployed. Typically these devices are technologically heterogenous and present several levels of automation: old control systems require heavy manual interaction with human operators; more advanced systems allow real-time environmental analysis and perform automatic control procedures. In Figure 1 we show the evolution trend for these systems: the Automated Data Acquisition System (ADAS) is designed to acquire measures and data from sensor devices deployed over the dam infrastructure and store and transmit them to personal computers for assessment.

Typically personal computers are placed next to sensor devices or in remote locations. In addition to automatic acquisition of measures, the Supervisory Control And Data Acquisition (SCADA) systems are designed to supervise and control the processes, by issuing commands to configure the actuator operations. Since ADAS is designed to perform monitoring operations, its components can be adapted to the SCADA system: for example, sensors can provide measures to the SCADA devices. As a matter of fact, currently deployed ADASs include devices able to perform control operations autonomously.

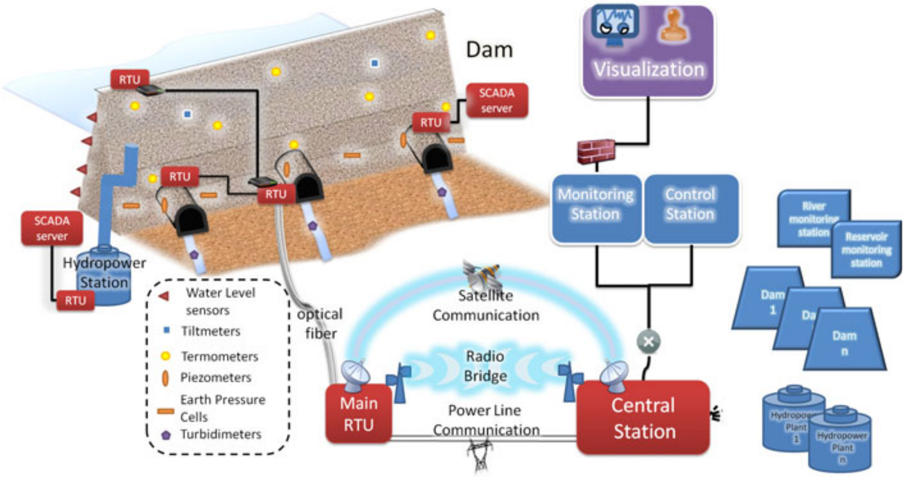


Fig. 2. Deployment of the dam monitoring and control system

Figure 2 shows some components of a SCADA-based dam monitoring and control system. We have not represented the ADAS, since its functionalities are implemented by the SCADA system. Both SCADA systems and ADASs include instruments to measure geotechnical parameters related to dam structure, water quality, water flows, environment, mechanism states, device states [9] [10]. In the context of automated monitoring, the instrumentation is based on sensors producing analog or digital signals. Measures are collected by devices placed next to or inside the dam facilities: Remote Terminal Units (RTUs) in the context of SCADA systems, and Remote Monitoring Units (RMUs) in the context of the ADASs. RTUs are in charge of converting sensor signals to digital data and sending them to remote SCADA system components or master RTUs (Main RTUs). Similarly, RMUs are in charge of transferring the measures to local or remote personal computers. Typical RMU devices are the Data Loggers.

ADASs include Monitoring and Control Units (MCUs) able to perform control operations autonomously. Similarly, more advanced RTUs and the Programmable Logic Controllers (PLCs) are able to control actuator devices.

Typically the ADAS parameter assessment is performed by application specific softwares installed on general purpose personal computers. PCs can be hosted in dam facilities or in remote locations. The SCADA system adopts a supervisor server (SCADA server) displaced next to the monitored process or in remote locations. Typically the SCADA server manages the dynamic process database, system logics, calculations, alarm database. The SCADA system includes client applications (SCADA clients) hosting process specific Human Machine Interfaces (HMIs). In figure 2 the Monitoring station represents the machine hosting the SCADA client; the Control station hosts the SCADA server and other components such as storage units and databases.

To realize short distance connections (for example RTU-main RTU, RTU-local SCADA server, RMUs-PCs), both SCADA systems and ADASs rely on several kinds of solutions: typically Local Area Networks based on fiber optic, telephone and Ethernet cables. For long distance connections Wide Area Networks based on power line communications, radio bridges, satellite links, cellular networks, telephone lines.

Central stations host SCADA components in charge of orchestrating the monitoring and control operations of several infrastructures using the water reservoirs. As shown in the figure, the Central station supervises several dams, hydropower plants, flow monitoring stations and other remote monitoring and control sites. The Visualization stations are public access zones, deployed to show the dam "health" to population living near to the reservoir or at downriver. Visualization station and some components of the Monitoring, Control and Central stations are composed of typical ICT devices like routers, firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, Web Server, Databases, Storage Units, Application servers, Gateways, Proxies. Moreover, identification devices perform access control to the SCADA units.

3.1 Dam Sensors

Physical sensors are adopted to monitor the operating environment conditions of the dam: monitoring some parameters is necessary to guarantee safe execution of critical processes, avoid hazardous controls and prevent possible critical failures or damages to the dam infrastructure. To monitor environmental parameters, several instruments and sensor devices exist. We provide a short list of them and a brief explanation of their principal usage in Table 1.

Table 1. Dam instrumentation

Instrument	*Parameter or physical event*
Inclinometer/Tiltmeter	Earth or wall inclination or tilt
Crackmeter	Wall/rock crack enlargement
Jointmeter	Joint shrinkage
Piezometer	Seepage or water pressure
Pressure cell	Concrete or embankment pressure
Turbidimeter	Fluid turbidity
Thermometer	Temperature

With regards to the most advanced technologies, we mention the smart sensors. These devices have increased the capabilities of the metering process in several aspects. Indeed, smart sensors have introduced the possibility to process the measures on the sensor boards, sending alarm messages in case of suspect environmental conditions. Other kinds of smart devices, such as the sensors of the Wireless Sensor Network (WSN), have provided capabilities in terms of protection mechanisms able to isolate faulted and misbehaving nodes (also named "motes").

4 SIEMs Overview

Security Information and Event Management (SIEM) systems are tools in charge of assessing the security level of the network infrastructure, by processing the reports generated by ICT applications, appliances and security devices deployed over the network. One of the most negative aspects of currently deployed security systems is the generation of too false positives: this limits their effectiveness since some relevant events pass unnoticed to the administrator behind the multitude of events. Main objective of the SIEM is to reduce this high false positive rate and emphasize the occurrence of events otherwise unnoticed. Its main functionality is to centralize the event analysis and produce a detailed and effective report by a multi-step correlation process.

Follows a description of the SIEM framework components.

Source Device is the component producing information to feed the SIEM; reports of normal or suspicious activities are generated by applications (Web Server, DHCP, DNS,...), appliances (router, switch,...) or operating systems (Unix, Mac OS, Windows,...). Even if not strictly part of the SIEM architecture, the Source is a fundamental component for the SIEM framework. Typically, most of the reports are logs in application specific format.

Log Collection component is responsible for gathering logs from Source Devices. It works adopting push or pull based paradigm.

Parsing and Normalizing component is in charge of parsing the information contained in the logs and to traduce this from the native format to a format manageable by the SIEM engine. Moreover, the Normalization component is in charge of filling the reports with extra information required during the correlation process.

Rule and Correlation Engines trigger alerts and produce detailed reports; they work on the huge amount of logs generated by the Source Devices. The Rule engine raises the alert after the detection of a certain number of conditions, while the Correlation Engine correlates the information within the evidences to produce a more concise and precise report.

Log Storage component stores logs for retention purposes and historical queries; usually the storage is based on a database, a plain text file or binary data.

Monitoring component allows the interaction between the SIEM user and the SIEM management framework. Interactions include report visualization, incident handling, policy and rule creation, database querying, asset analysis, vulnerability view, event drilling down, system maintaining.

As we will see soon, these components are all implemented and customizable in the OSSIM SIEM.

4.1 OSSIM

OSSIM (Open Source Security Information Management)[11] is an open source SIEM released under the GPL licence and developed by AlienVault [12]. OSSIM does not aim at providing new security detection mechanisms but at exploiting already available security tools. OSSIM provides integration, management, and visualization of events of more then 30 [13] open source security tools. More important, OSSIM allows the integration of new security devices and applications in a simple way.

All the events collected by OSSIM undergo a process of normalization in order to be managed by the SIEM core. After the normalization, OSSIM performs event filtering and prioritization by means of configurable policies.

OSSIM provides capabilities in terms of event correlation, metric evaluation and reporting. Indeed, OSSIM performs per event risk assessment and correlation process. Correlation process produces events more meaningful and reliable than those generated by single security tools. The objective of the correlation is to reduce the number of false positives to produce less reports for human operator.

OSSIM performs three types of correlations:

Inventory Correlation. performs event filtering by assessing the possibility that a given attack may affect a specific kind of asset (i.e. a Windows threat to a Linux box).

Cross Correlation. re-evaluates the event "reliability" by comparing each event with the result of the vulnerability analysis (i.e. if an event reports an attack to an IP and that host is vulnerable to that attack, the event reliability raises).

Logical Correlation. executes the correlation directives defined by condition trees. Conditions are built on Boolean logic expressed in hierarchical structures. Correlation directives are customizable and configurable by the user.

Architecture. OSSIM architecture is based on software components that can be deployed in several ways across many networks: in this way, OSSIM can be used to monitor different network domains. Main components of OSSIM are represented in Figure 3:

Detector: it is any tool that supervises the assets. Detectors are in charge of reporting operating or security-related "events". OSSIM is already enabled to be connected with a huge number of Detector tools and the Collectors of these tools come already packaged within the framework. Other Detectors can be added to OSSIM by developing new Collectors enabling OSSIM to accept new types of events.

Collector: it is the component in charge of: (1) gathering events form different sensors; (2) parsing and normalizing the events; (3) forwarding the

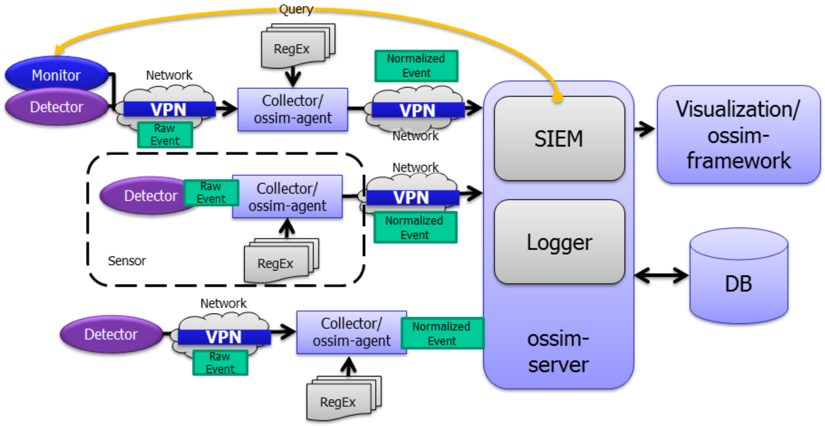


Fig. 3. Deploymnet of OSSIM components

normalized events to the Server component. The software component that implements these tasks is the OSSIM-Agent. Event collection is organized in a plugin based system. Each different source of events is associated with a plugin able to parse and normalize a specific data format. Event parsing and normalization is performed using Python style regular expressions.

Monitor: this component is very similar to the Detector, but it's activated only after a request (query) by the Server. Monitors generate "indicators". The OSSIM server can query a Monitor to gather additional information and perform a more precise correlation process. Indicators reach the Server by means of the same mechanisms used for the "events".

Sensor: it is the combination of the Detector tool and the related Collector.

Server: the OSSIM-Server component implements the intelligence of the SIEM. The Server component has two main functionalities: SIEM and Logging. The SIEM subsystem performs risk assessment, correlation, and real-time monitoring; moreover, it allows mechanisms for vulnerability scanning. The SIEM behavior is totally configurable through policies. Polices are used to set up event management and alert creation. The Logger subsystem is used to store raw events for forensic analysis. All the events are provided with a digital signature that allows their use for legal evidence. OSSIM supports encrypted channels from event source to Data Logger component.

Database: the OSSIM-Database is a MySQL database used to store both configurations (handled by means of the web interface) and the asset inventory.

Web interface: it is implemented in the OSSIM-Framework software. It provides the visualization interface of the entire framework. It allows the handling of all the events and alarms generated by Sensors and OSSIM-Server. The Web interface is used to configure policies, to perform network scanning, to query the database. The web interface is implemented in PHP and HTML code and runs on a Python daemon process.

Figure 3 represents a typical architecture of the OSSIM framework. Detectors can be deployed either along with their Collectors or separately. In the latter case the raw events produced by Detectors must reach the Collector through the network. To transfer these events, OSSIM adopts several protocols: Rsyslog, FTP, SAMBA, SQL, OSSEC, SNARE among others. Collector components can be deployed together with the OSSIM-Server or remotely. In the latter case, to protect the Collector-Server communication, Virtual Private Networks are set up. Monitors are deployed just like Detectors, but are triggered by the Server.

5 Changing the SIEMs to Provide Safety

As seen, OSSIM actions can be described in the following steps: extract information from events (or indicators) generated by the Source Devices deployed over the network infrastructure; apply a policy and execute the correlation process to perform risk assessment; finally, raise an alert message (and a *ticket*) to the administrator. Our main idea is to detect misuses and malicious actions (such as cyber attacks) occurring at the monitoring and control system of the dam infrastructure. We correlate reports produced by ICT appliances and applications, monitoring and control devices (physical sensors, SCADA servers, PLCs, RTUs, RMUs), security devices and applications (identification, authentication mechanisms,...). We describe how to implement new plugins for the OSSIM-Agent and write new correlation rules (*directives*) to detect misuses and malicious activities.

5.1 Examples of Misuses and Malicious Activities on the Dam Monitoring and Control System

In this section we provide some examples of misuses and malicious activities occurring at the dam monitoring and control system. Moreover we indicate some possible events to be correlated by the SIEM. We remark that this list is far from being exhaustive and is a hint for future considerations about the safety and cyber security relationship in systems for CIP.

Alteration of Measurement Data: Physical sensors measure unexpected values: for example the piezometer measures water levels out of the structural range or expected profile (in specific environmental conditions). The SIEM framework correlates this event with events or indicators produced by security Source Devices and evaluates the probability of sensor device tampering. Examples of security events are: changes in the sensor devices' Operating System fingerprint, traffic profile anomalies on the field network, connection attempts to the machines controlling the sensors. Altering measurement data is dangerous because parameters out of range can trigger automatic control procedures.

Malicious Control Commands: Parameters have sudden changes further to controls operated by actuators. The SIEM correlates this physical event with events reporting controls issued by the SCADA server. Moreover the SIEM verifies if the control issued by the SCADA is consequence of a predefined behavior, like a scheduled operation or a change in the automatic control procedure. In the latter case the SIEM correlates these events with security events related to the SCADA system components.

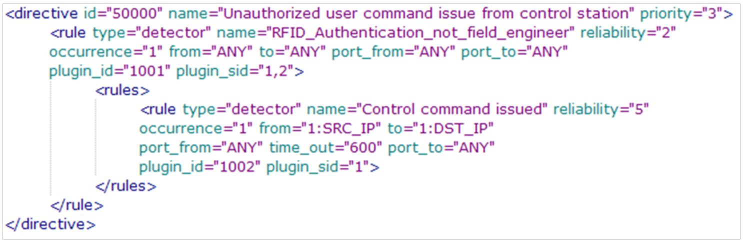
Missing Control Commands: Sensors measure physical parameter values inside the expected ranges and/or the sensor supervisor unit does not report any alerting event (or reports a normal event). In case of critical conditions for the infrastructure, altered measures or missing reports can result in missing safety controls causing damages to the dam infrastructure (”dam failures”). Events about malicious activities against the SCADA system components can be correlated with the analysis of model-based physical predictors.

Control Station Hacking: The control station issues control commands modifying the procedures of the RTU or PLC systems. Controls or changes are issued by an operator enabled to access the control station, but not to perform these operations, as reported by the identification procedure. The identification procedure can be realized by means of Radio Frequency IDentification (RFID) or by biometric recognition devices.

5.2 Customizing OSSIM to Process New Events

To perform comprehensive event analysis by means of the SIEM framework, our first task has been to extend OSSIM with new Source Devices, in particular sensors, control units and security devices. Typically Source Devices generate two kinds of information, namely ”events” and ”indicators”. Events are generated after specific occurrences: for example, SCADA servers and PLCs generate events reporting the issue of control commands or the detection of anomalous parameter profiles (i.e. threshold exceeding); security devices produce evidences of security related events (i.e. access to control station). Indicators are sent to the SIEM framework after a query by the SIEM server: RTUs, Data Loggers and SCADA servers can be in charge of retrieving measures of physical parameters; security devices can provide indicators about specific vulnerabilities (i.e. open ports). Indicators and events can be used to define the correlation rules to detect misuses and malicious activities, as shown in the following lines.

As seen in the previous section, data from ”field” devices are transferred by RTUs with several communication protocols: DNP3, ModBus (TCP/IP), Profibus (DP/PA), Profinet, IEC 60870-5-104, ICCP, OLE for Process Control (OPC), OPC Unified Architecture, just to cite some. Even if OSSIM provides a large number of parsers for the most common log formats or communication protocols, users can provide new plugin modules to make the SIEM able to work with legacy or custom message formats. To integrate new parsers with the OSSIM SIEM, users extend the plugin set within the Collector component. The source type that feeds a plugin can be classified as ”monitor” or ”detector”. Monitors are pull based sources and produce indicators, while detectors are push based and produce events. To feed the Collector agent, transfer methods or protocols must be specified (log, mysql, mssql, wmi): it’s suggested to adopt the Syslog protocol, since it is more suitable to be parsed by the Regular Expression



```
<directive id="50000" name="Unauthorized user command issue from control station" priority="3">
    <rule type="detector" name="RFID_Authentication_not_field_engineer" reliability="2"
    occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
    plugin_id="1001" plugin_sid="1,2">
        <rules>
            <rule type="detector" name="Control command issued" reliability="5"
            occurrence="1" from="1:SRC_IP" to="1:DST_IP"
            port_from="ANY" time_out="600" port_to="ANY"
            plugin_id="1002" plugin_sid="1">
        </rules>
    </rule>
</directive>
```

Fig. 4. Example of OSSIM rule

engine; moreover the Syslog server can be configured to filter events and drop values (as measures) out of valuable ranges.

RegExp (Regular Expression) plugins are in charge of extracting useful information and filling the *Normalized event*. Normalized events contain optional and mandatory fields useful to the correlation process. Each plugin is identified by the Id (unique) and more Sub-Ids (Sids); Sids are useful to create rules and correlation directives. Indeed, rules use Sids to identify different kinds of event messages generated by the data source (for example: plugin Id identifies logs produced by Apache servers in general, Sids identify specific events on the Apache server).

To feed OSSIM with environmental parameters we have adopted a commercial Data Logger. Data loggers can perform measurements and store or forward them to remote servers. The following string contains a sample log of the piezometer measure reporting the seepage or groundwater level.

```
D,088303,"JOB1",2011/03/11,11:27:02,0.016113,1;
A,0,8.621216e-06,-1.4952594;0075;CC8C
```

Normalized events are sent to the SIEM Server. The Server applies a policy to the event (Correlation, Forwarding, Action, Discard), basing on: Time Range, Plugin Group, Source and Destination Addresses, Ports. If not discarded, the event undergoes the *Risk Assessment* process and becomes *Enriched event*. The Enriched event has several metrics: Reliability, that represents how much the reported event is probably a suspect activity; Priority value, that represents the absolute importance of the event with no reference to a specific host or environment; Asset value, that states what is the importance of the assets involved in that event. The Risk is computed by combining metrics in a single value. After Risk Assessment, the event can be processed by the Correlation engine. Correlation produces a new event that, as such, is subjected to new Risk Assessment process. If the Risk is bigger than one, the Alarm event is generated. We give full scale value to Asset and Priority metrics involving events related to physical sensors.

Most interesting Correlation mechanism we considered is the Logical Correlation, implemented by means of directives written in xml syntax or, more easily, by means of visual editors (in the Web Interface). Main objective of the directive is to assess Priority and Risk for a certain number of collected events. Directives specify the Id and Sid of the events involved in the rule: since the Id is unique per event source, we can correlate the Id of physical sensor messages with the Id of security devices, ICT applications, SCADA components and so on. Monitor directives can verify the met of several *conditions* (equal, less than,...) related to the event fields, such as measures; Detector directives are focused on event "occurrence", that is the repetition of the same event. In the latter case, the environmental monitoring units are in charge of transmitting to the SIEM the results of their analysis.

In Figure 4 we show a simple rule of the "Control station hacking" misuse: the first event is produced by RFID device (id=1001), where Sids 1,2 indicate the access by two employees with no authorization to issue commands; the second event is reported by an application on the Control station (id=1002) and is triggered by the execution of a new control command.

6 Conclusion and Future Works

Dams infrastructures are designed to provide services related to the use of water reservoirs (typically in conjunction with different infrastructures, such as hydropower plants). These complex systems are monitored and controlled by several components in charge of providing supervision during the processes. The monitoring and control procedures, orchestrated among several sites, are performed issuing commands and processing data by means of a large number of components (legacy COTS SCADA systems, ICT appliances and applications): typically these components are not designed with security in mind. In such a complex scenario, misuses and malicious activities can represent threats to society, safety and business. Indeed, malicious activities like cyber attacks, can be aimed at changing the automatic control procedures, alter the measures produced by sensor devices, issue control commands.

In this work we propose an extension of the OSSIM SIEM by AlienVault, to perform the analysis of events generated by the security devices (recognition devices, authentication tools,...) and process specific devices (SCADA servers, RTUs, ...) responsible to supervise the operations and the processes of the dam infrastructure. Our objective is to obtain evidences of misuses and malicious activities on the monitoring and control systems, since they can result in issuing hazardous commands to the control devices of the dam infrastructure.

In next works we reserve to perform a more detailed analysis about the safety and cyber security relationship within the systems for CIP and assess the reliability of the reports produced by our prototype.

Acknowledgments. The research leading to these results has received funding from the European Commission within the context of the Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No. 225553 (INSPIRE Project), Grant Agreement No. 248737 (INSPIRE-INCO Project) and Grant Agreement No. 257475 (MAnagement of Security information and events in Service Infrastructures, MASSIF Project). It has been also supported by the Italian

Ministry for Education, University, and Research (MIUR) in the framework of the Project of National Research Interest (PRIN) ”DOTS-LCCI: Dependable Off-The-Shelf based middleware systems for Large-scale Complex Critical Infrastructures”.

References

1. Regan, P.J.: Dams as systems - a holistic approach to dam safety. In: 30th Annual USSD Conference Sacramento, California (2010)
2. White Paper, Global Energy Cyberattacks: “Night Dragon”, McAfee® Foundstone®Professional Services and McAfee Labs (2011)
3. White Paper, Symantec®Intelligence Quarterly Report, Targeted Attacks on Critical Infrastructures, http://bit.ly/g8kpvz (October-December, 2010)
4. Jeon, J., Lee, J., Shin, D., Park, H.: Development of dam safety management system. Advances in Engineering Software 40(8), 554–563 (2009) ISSN 0965-9978
5. Farinha, F., Portela, E., Domingues, C., Sousa, L.: Knowledge-based systems in civil engineering: Three case studies. In: Advances in Engineering Software. Selected papers from Civil-Comp 2003 and AICivil-Comp 2003, vol. 36(11-12), pp. 729–739 (November-December 2005) ISSN 0965-9978
6. Ingelrest, F., Barrenetxea, G., Schaefer, G., Vetterli, M., Couach, O., Parlange, M.: SensorScope: Application-specific sensor network for environmental monitoring. ACM Trans. Sen. Netw. 6(2) Article 17 (2010)
7. Briesemeister, L., Cheung, S., Lindqvist, U., Valdes, A.: Detection, correlation, and visualization of attacks against critical infrastructure systems. In: Eighth Annual International Conference on Privacy Security and Trust (PST), 2010, August 17-19, pp. 15–22 (2010), doi:10.1109/PST.2010.5593242
8. Madrid, J.M., Munera, L.E., Montoya, C.A., Osorio, J.D., Cardenas, L.E., Bedoya, R., Latorre, C.: Functionality, reliability and adaptability improvements to the OSSIM information security console. In: IEEE Latin-American Conference on Communications, LATINCOM 2009, September 10-11, pp. 1–6 (2009)
9. Myers, B.K., Dutson, G.C., Sherman, T.: City of Salem Utilizing Automated Monitoring for the Franzen Reservoir Dam Safety Program. In: 25th USSD Annual Meeting and Conference Proceedings (2005)
10. Parekh, M., Stone, K., Delborne, J.: Coordinating Intelligent and Continuous Performance Monitoring with Dam and Levee Safety Management Policy. In: Association of State Dam Safety Officials Conference Proceedings, at the 2010 Dam Safety Conference (2010)
11. Karg, D., Casal, J.: Ossim: Open source security information management. Tech. report, OSSIM (2008)
12. AlienVault®, http://alienvault.com/
13. AlienVault OSSIM Available Plugins, http://alienvault.com/community/plugins